iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 14 **Issue:** III **Month of publication:** March 2026

**DOI:** https://doi.org/10.22214/ijraset.2026.79180

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue III Mar 2026- Available at www.ijraset.com*

# AI and Blockchain Based eKYC Verification System

Dr. Bharathi[1], V. Harshith[2], Y. Indrajeet[3], S. Omkar[4]
[1]*Assistant Professor, Department of Computer Science and Engineering, Methodist College of Engineering and Technology, Abids, Hyderabad, Telangana, 500001, India*
[2, 3, 4]*Studenent, Department of Computer Science and Engineering, Methodist College of Engineering and Technology, Abids, Hyderabad, Telangana, 500001, India.*

***Abstract:*** ***With the rapid evolution of digital services, the importance of identity verification is paramount. Conventional KYC procedures involve tedious processes, which are prone to fraud and data breaches. This project outlines the design and development of the AI and Blockchain Based eKYC Verification System. It provides the benefits of rapid and accurate identity verification.***
***In the proposed model, the eKYC verification is done using the Artificial Intelligence-based face recognition and liveness detection techniques. It verifies the identity of the user by comparing the live selfie with the ID photograph. Blockchain technology is employed to ensure the security of the data. It stores the identity data in the form of digital hashes, which is immutable and tamper-proof. Smart contracts ensure the rules to be followed, such as one-time user registration.***
***This proposed model is accurate and rapid, making it suitable for various applications. It can be applied to the banking sector, financial institutions, and e-governance.***
***Keywords: eKYC verification, blockchain security, face recognition, liveness detection, smart contracts, blockchain technology, digital identity management***

## I. INTRODUCTION

### *A. Background and Context*

Throughout the last decade, there has been tremendous technological advancement in the country, driven by technologies like UPI, Aadhaar, and online banking platforms. The country has over 900 million internet users, and digital services have become an integral part of life.
However, there has been a tremendous surge in cyber crimes like identity theft, fraud, and illegal access to individual information. It has been reported that financial fraud losses in the country have reached alarming levels.
The conventional Know Your Customer (KYC) process involves manual procedures, which are time-consuming and vulnerable to human error. The conventional KYC system involves storing sensitive end-user data in a centralized manner, which increases the risk of data breaches and illegal usage. With the increasing popularity of digital onboarding, there is an urgent need for an automated and secure identity verification process.

### *B. Need for Secure eKYC Systems*

As online financial services are becoming increasingly popular, electronic KYC systems have become a ne-cessity. The existing systems do not have real-time verification capabilities and are vulnerable to fraud such as fake identity creation, duplicate registrations, and document tampering. The centralized data also increases the risk of sing-le point failures and data tampering.

For an eKYC system to be robust, it needs to:
• Verify the identity of the user correctly
• Prevent spoofing and fraud
• Store the data securely
• Provide a seamless user experience

©IJRASET: All Rights are Reserved 

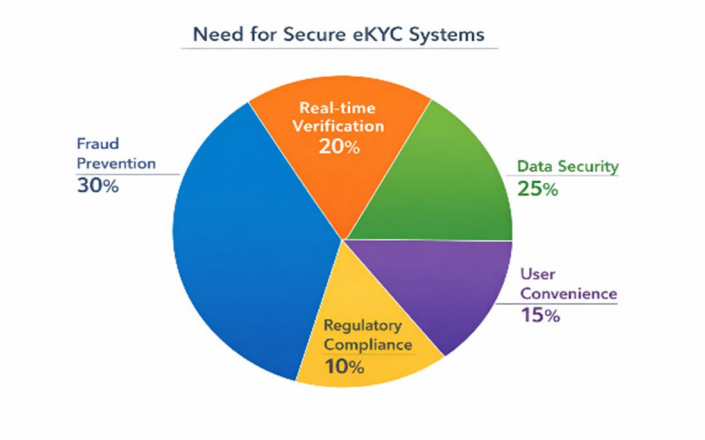



Fig 1.1: Need for Secure eKYC Systems

Furthermore, in India's case, the problem is complicated by the availability of various regional languages like Hindi, Telugu, Tamil, and Bengali, along with code-mixed language varieties like Hinglish and Tanglish. A significant percentage of online users access these facilities in informal forms of communication, which makes it difficult for conventional systems to detect abusive content appropriately.

Furthermore, a lack of digital literacy among some online users is another factor that is allowing harmful content to spread unchecked. They are not able to identify and report cyberbullying appropriately.

### *C. Challenges in Existing Systems*

Even with the progress achieved, the current eKYC technology is still facing the following challenges:Manual Verification Delays: The traditional methods involve human intervention, which is time-consuming.Fraud and Identity Duplication: Counterfeit IDs and duplicated identities are some of the challenges facing the current technology.Lack of Liveness Detection: The current technology is unable to tell the difference between the real user and the one trying to trick the system using images/videos. Data stored in the centralized system is vulnerable to hacking.

Limited Scalability: The current technology is unable to support the high demand for real-time verification

### *D. Motivation for AI & Blockchain-Based eKYC*

To overcome these disadvantages, a solution is offered by using Artificial Intelligence in combination with Blockchain technology. The advantages offered by using Artificial Intelligence are:

*1)* Face recognition for matching
*2)* identityLiveness detection to avoid spoofing
*3)* Real-time verification
*4)* The advantages offered by using Blockchain technology are:
*5)* Secure and tamper-free data storage
*6)* Decentralized system to avoid single-point failure
*7)* Execution of rules such as one user and one identity using smart contracts

### *E. Objectives of the Project*

The key objectives of the proposed AI & Blockchain Based eKYC Verification System are:

*1)* To design a system for identity verification using AI-based face recognition technology
*2)* To incorporate liveness detection in order to avoid any spoofing attacks
*3)* To store identity information in a secure manner using blockchain technology
*4)* To avoid duplication of identity using smart contract logic
*5)* To provide a faster, efficient, and ease-of-use identity verification system
*6)* To ensure data privacy by storing identity information in encrypted or hashed format

## II. LITERATURE SURVEY

This section discusses the existing research on different digital identity verification systems such as traditional KYC systems, machine learning-based systems, biometric systems, blockchain-based systems, and hybrid systems based on AI and blockchain technologies. The focus of these research papers is on security, scalability, and challenges faced by these systems that are relevant to the proposed eKYC system.

### *A. Traditional KYC Systems*

The traditional identity verification systems were simple and based on manual processing of identity proofs. The initial identity verification systems were based on traditional methods of verifying identity proofs such as Aadhaar cards, PAN cards, and passports. The traditional systems are simple but are time-consuming and prone to errors. The traditional systems are also prone to document forgery and manipulation of identity proofs.

The Digital KYC systems are an improvement over traditional systems and are based on online document submission. The Digital KYC systems are also based on traditional identity verification methods and are prone to data breaches and identity duplication due to the centralized nature of these systems.

### *B. Machine Learning-Based Verification*

Machine learning-based identity verification systems have also been explored for identity verification systems. Machine learning-based systems are based on pattern detection of fraudulent activities by the user. The machine learning-based identity verification systems are based on different machine learning algorithms such as Logistic Regression, Random Forest, and Support Vector Machines (SVM), which are based on pattern detection and have shown good results for identity verification systems.

However, machine learning-based systems are also limited in the sense that these systems cannot process visual identity proofs and cannot handle spoofing and impersonation attacks on identity verification systems.

### *C. Biometric Authentication Systems*

The biometric systems such as facial recognition systems and fingerprint scanning systems have shown good results for identity verification systems. The deep learning-based systems such as CNN and FaceNet have shown good results for identity verification systems based on facial recognition systems.

biometric systems have shown high accuracy in identity verification systems and are based on deep learning-based systems such as CNN and FaceNet for facial recognition systems.

Despite high accuracy (above 95%), these systems are also facing challenges such as:

- Spoofing attacks
- High computational requirements
- Privacy issues related to the storage of biometric data

This, in turn, emphasizes the need for implementing more security measures like liveness detection.

### *D. Deep Learning Techniques*

Deep learning techniques, especially Convolutional Neural Networks, have been used to carry out face recognition and identity matching. Deep learning techniques have shown higher accuracy in comparison to other techniques.

Moreover, advanced techniques like liveness detection, blink detection, and facial movement tracking have shown promising results in preventing spoofing attacks. However, these techniques require more computational power and might not be efficient in real-time scenarios.

### *E. Blockchain-Based Identity Management*

The concept of blockchain technology offers decentralization, immutability, and transparency in managing identities. Unlike other techniques, in blockchain-based identity management, sensitive information is not stored in a centralized server.

Moreover, smart contracts have been used to ensure the following:

- One User → One Identity
- Tamper-Proof Data Storage
- Secure Verification Without Any Intermediary

However, there have been issues related to blockchain-based identity management, like scalability and transaction fees.

*F. Hybrid Approach Using AI and Blockchain*

Recent studies have shown promising results in the hybrid approach of AI and blockchain technologies. This approach ensures the efficient use of the benefits offered by both technologies.

The hybrid approach has shown promising results in identity management, like:

•Automated and Real-Time Verification
•Fraud Detection and Prevention
•Decentralized Identity Management

This approach has formed the basis of modern-day eKYC systems.

*G. Deployment and Challenges*

The deployment of eKYC systems in real-world scenarios has shown many challenges, like:

•Scalability Issues: How to handle large numbers of users in real-time scenarios?
•Privacy Issues: How to ensure the security and privacy of sensitive biometric data?
•FALSE POSITIVES/NEGATIVES: How to ensure correct results in identity matching?
• User Experience: The Need for Quick Onboarding
•Integration: Compatibility with banking and government systems

These challenges demonstrate the necessity for an effective, efficient, and easy-to-use system

*H. Dataset and Evaluation Issues*

The performance of AI-based eKYC systems is also dependent on the quality of the datasets used for training the system.
Most datasets used are not effective.
In addition, the use of accuracy, precision, recall, and F1 score as performance metrics is also not effective.
Real-time testing is important in the performance evaluation of the system

*I. Legal and Social Considerations*

The legal considerations for the implementation of the system include:

•KYC/AML guidelines
•Data protection legislation
•Privacy legislation

In India, the legal considerations include:

•Aadhaar-based verification
•RBI guidelines.

*J. Summary and Research Gaps*

The literature has shown a progression of KYC systems, starting with manual systems, then moving to AI-based systems, and finally to blockchain-based systems. Although each system has shown an improvement over the earlier ones, some research gaps still exist, such as:

• The absence of an integrated system of AI and Blockchain
• The lack of liveness detection in some systems
• The centralized storage problem
• The lack of privacy-preserving mechanisms
• Scalability issues in real-time systems

The AI & Blockchain Based eKYC Verification System aims to address these research gaps by incorporating facial recognition, liveness detection, and blockchain-based secure storage, thus providing a reliable, scalable, and secure system to prevent fraudulent activities.and fraud-resistant identity verification solution.

## III. SYSTEM ARCHITECTURE

*A. Architecture Overview*

The architecture of the AI & Blockchain Based eKYC Veri-fication System has been developed to ensure a secure, scalable, and automated system of identity veri-fication. After considering various challenges such as identity fraud, data tampering, and spoofing

attacks, the system has been developed using a layered architecture, where we have integrated Artificial Intelligence for veri-fication purposes and Blockchain for secure data storage.

The system processes various user inputs such as identity information, documents, and facial images through various system modules. All the modules operate independently, such as face veri-fication, liveness, and blockchain, and then provide a combined output to determine the veri-fication status.

The architecture of the system has been divided into four phases: user registration, data processing, AI-based veri-fication, and blockchain-based decision-making.

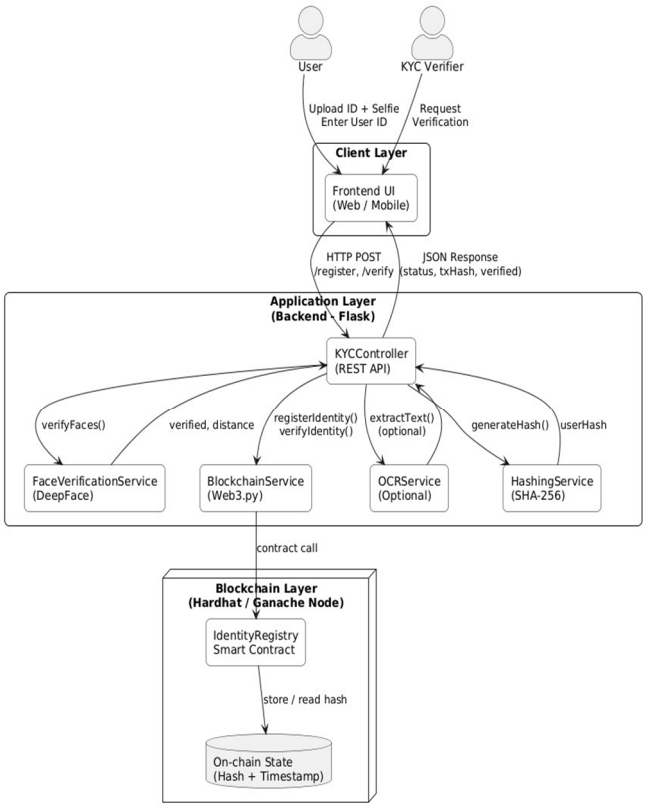



Fig 3.1: System Architecture

*B. Detailed Explanation of the Phases*

*1) User Registration & Input Collection*

The verification process commences when a user initiates registration by interacting with the application interface. The user is required to submit information such as:

•Username / Unique ID

•Government ID (Aadhaar / PAN / etc.)

•Live Photo / Selfie

This phase ensures that users are not registered more than once by checking existing records in the system.

*2) Data Preprocessing & Validation*

This phase involves processing and preparing the collected data for analysis:

Image Processing

• Data Cleaning

• Feature Preparation

This phase ensures that the collected data is in a suitable format for accurate verification.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue III Mar 2026- Available at www.ijraset.com*

*3) AI-Based Identity Verification*

This phase is responsible for verifying user identity using AI models:
Face Recognition Model
• Liveness Detection
• Duplicate Detection
This phase uses AI models to verify user identity by comparing the selfie image with the ID image and checking whether the user is real (not a photograph/video) and whether the identity is duplicated.

*4) Blockchain Storage & Decision Making*

This phase is responsible for processing AI results:
Smart Contract Validation
• Data Hashing
• Blockchain Storage
• Decision Making
This phase ensures that one user corresponds to one identity; data is hashed into a secure format; and records are stored securely in a blockchain system

## IV. IMPLEMENTATION

### *A. Development Environment and Technology Stack*

The implementation of the AI & Blockchain Based eKYC Verification System can be divided into three major phases: AI Model Development, Backend Integration, and Frontend Interface Design.
For the development of the AI Model, the programming languages used are Python, OpenCV, DeepFace, TensorFlow, and PyTorch. The models are trained to compare the selfie images of users with ID images and detect spoofing.
For the backend development of the system, Flask is used to create REST APIs for handling user requests. Web3.py is used to connect the backend of the system with the Ethereum Blockchain.
For the frontend development of the system, a user-friendly interface is designed using HTML, CSS, JavaScript, or Streamlit to allow users to register, upload ID proofs, and perform verification in real-time.

*1) User Interaction and Input Handling*

The first phase of the system involves user interaction through the web interface. Users need to provide the following information:
• Username/Unique ID
• Government ID (Aadhaar/PAN Card)
• Live selfie image
The system follows an event-driven approach in which the verification process starts only after the user has submitted the required information.

*2) Data Preprocessing and Validation*

The data provided by the user is then sent for data preprocessing before sending it for the verification process:
• Image preprocessing
• Face detection
Validation of the user information and ID format
This phase ensures that the data sent for the verification process is consistent.

*3) AI-Based Verification Pipeline*

Pipeline 1: Face Recognition
The comparison is done by matching the user's live selfie with the up-loaded ID image. The process is done by DeepFace and other similar models. A similarity score is generated for the purpose of verifying identity.
Pipeline 2: Liveness Detection
Spoofing attacks are prevented by implementing liveness detection methods such as
- Facial movements
- Eye blink detection

©IJRASET: All Rights are Reserved 

- Real-time detection

The process is carried out to ensure that the user is physically present and not a fake identity.

Pipeline 3: Duplicate Identity Check

The process is carried out by checking if the user or ID already exists:

- Username uniqueness
- ID uniqueness
- Face embedding uniqueness

The process is carried out to ensure that a user is equal to an identity.

*4) Blockchain Integration and Storage*

The process is carried out by integrating the data into the blockchain after the AI verification process:

- User data is converted into a cryptographic hash
- Smart contracts are created to validate the uniqueness
- The data is stored on the blockchain
- The process is carried out to ensure:
- Tamper-proof data
- Transparency
- Decentralization

### *B. Fusion and Decision Module*

The outputs of all the pipelines are fused to obtain the final output:

- Face matching score
- Liveness detection
- Duplicate identity detection

The outputs are based on which the final output is provided:

- Verified
- Rejected

### *C. Deployment and System Integration*

*1)* The process is carried out by integrating the following:
*2)* Flask for the backend
*3)* AI models for inference
*4)* Blockchain for storing data
*5)* Frontend for user interaction
*6)* The process is carried out to ensure scalability and integration into:
*7)* Banking systems
*8)* Fintech systems
*9)* Government eKYC systems

### *D. Key Implementation Features*

*1)* Real-time AI verification
*2)* Secure data storage using blockchain
*3)* Fraud prevention
*4)* One user – one identity
*5)* Development Environment and Technology Stack

## V. METHODOLOGY

The methodology of the proposed AI & Blockchain Based eKYC Verification System is developed to overcome the challenges of identity frauds, spoofing attacks, and data security by implementing the concepts of Artificial Intelligence and Blockchain Technologies.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue III Mar 2026- Available at www.ijraset.com*

The proposed system is different from existing systems that only use document verification for identity verification by implementing multiple facets of identity verification such as biometric information, user presence, and decentralized data storage.

### *A. Multi-Module Verification Approach*

The proposed system is based on a multi-layered verification approach:

• Face Recognition Module:

The proposed system will use a deep learning algorithm such as DeepFace to compare the user's real-time selfie and the ID image uploaded by the user. This will ensure that the user is the actual owner of the identity.

• Liveness Detection Module:

The proposed system will also use a liveness detection approach to prevent spoofing attacks by taking a photo or video of the user's identity. The user presence will be validated by checking the facial movements and blinking of the user.

• Identity Validation Module:

The information provided by the user will be validated and checked for duplication in the system.

### *B. Decision Fusion Logic*

The proposed system will not rely on a single approach for identity verification. Instead, it will use a combination of multiple modules for identity verification by implementing a weighted decision approach:

The weights will be assigned based on the importance of each module:

• Face Recognition → 50%
• Liveness Detection → 30%
• Identity Validation → 20%

The final decision for verification is made by calculating these scores. This is a rational decision process, similar to how humans make decisions based on facial similarity being the most important factor and supported by real-time presence and identity validation checks.

### *C. Blockchain-Based Security Mechanism*

Once the verification process is completed, the data integrity is ensured by implementing a blockchain-based mechanism:

• The user data is converted into a cryptographic hash value
• Smart contracts are used to implement the rule of one user to one identity
• The data is stored in a decentralized and tamper-proof manner

This removes any risk of data breaches and data tampering that may happen due to a centralized data storage mechanism.

### *D. System Performance and Efficiency*

The proposed system is efficient and performs in real time:

• The verification process is completed in 2-5 seconds for a user
• The accuracy of the face recognition process is ~90-95%
• The use of Flask and Web3 for efficient backend processing
• The use of lightweight AI models for efficient processing

The output of the system is clear and indicates:

• Verified
• Rejected

Additionally, the output may also include confidence levels for better transparency.

### *E. User-Centric Approach*

The proposed system is user-centric and provides a simple and efficient user experience:

• The system provides a simple interface for uploading the ID and selfie
• The process is completed in real time and provides feedback to the user
• The process is secure and ensures data privacy
• The process is simple and does not require significant effort from the user

©IJRASET: All Rights are Reserved 

### *F. Methodology Summary*

The proposed methodology is a combination of:

- AI-based biometric verification
- Liveness detection for anti-spoofing attacks
- Blockchain-based data storage
- Weighted decision-making for better accuracy

## VI. RESULTS

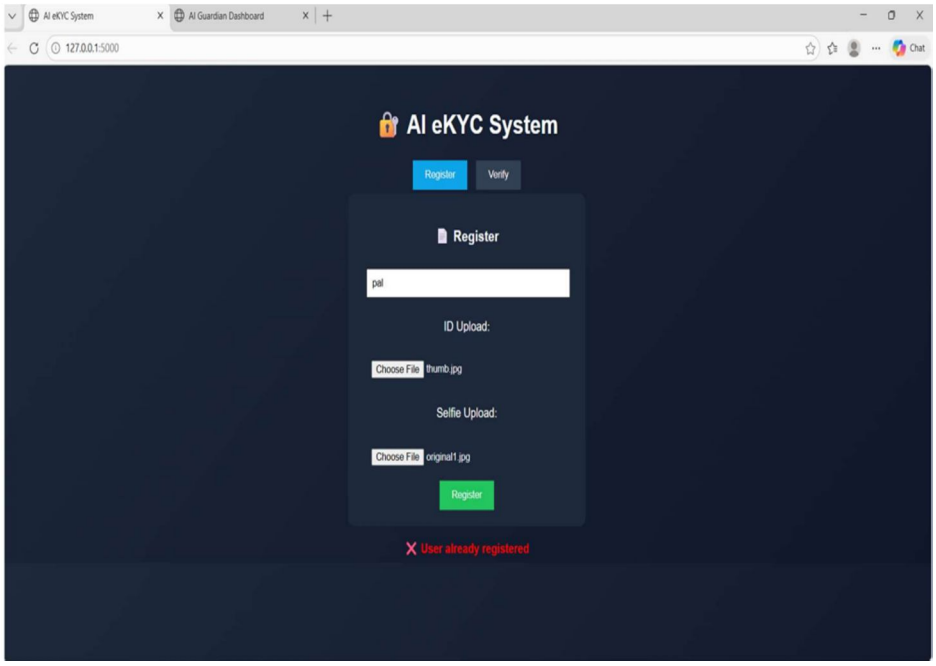



Fig 6.1: Dashboard of Ai eKYC System

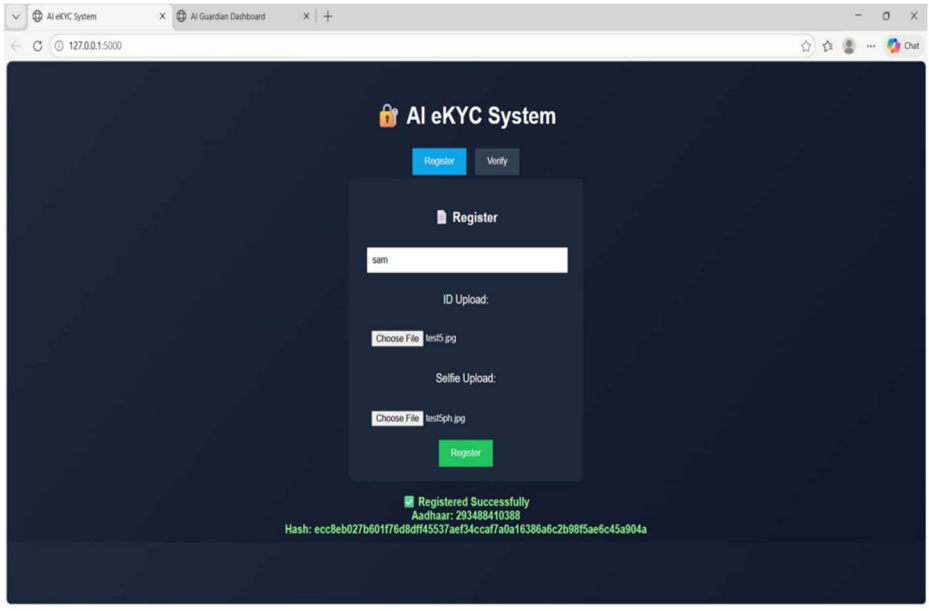



Fig 6.2: Registration of Ai eKYC System

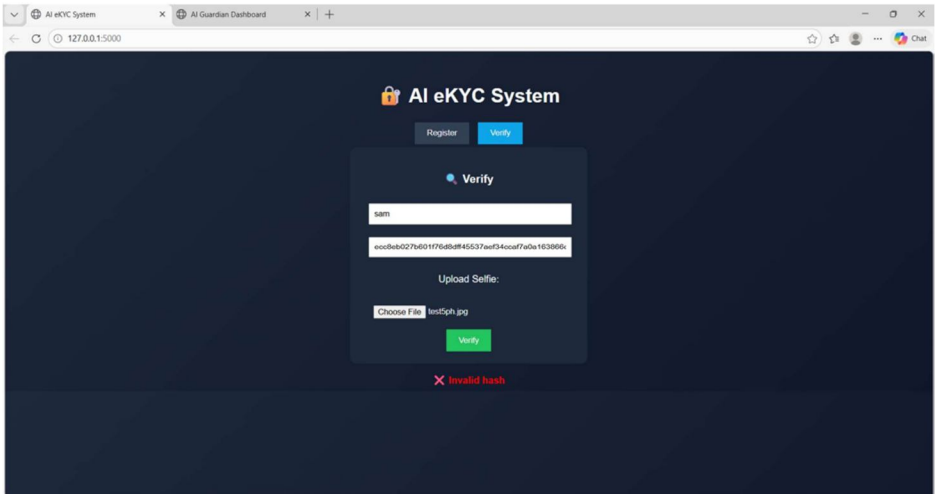



Fig 6.3: verifying of user in Ai eKYC System

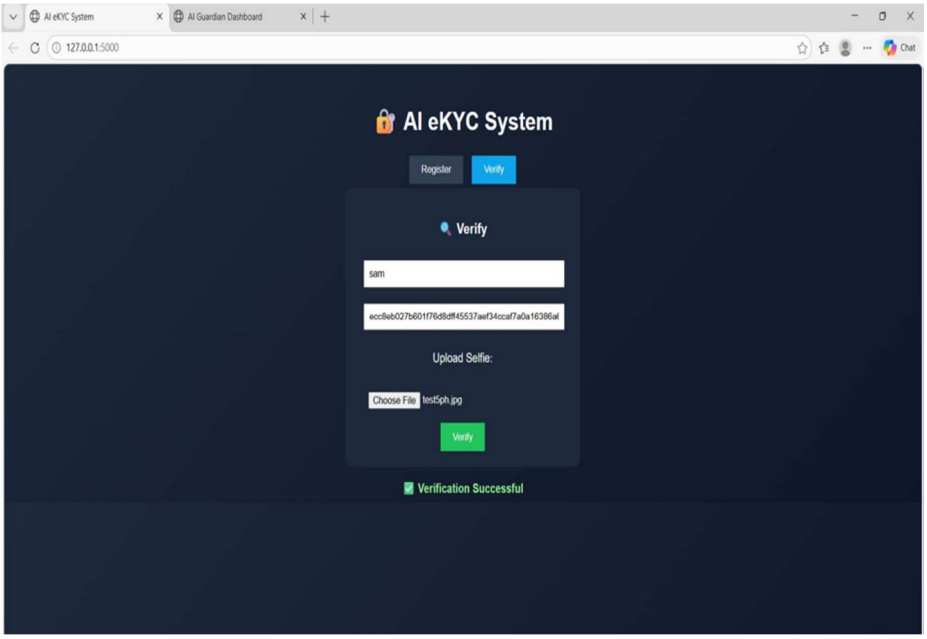


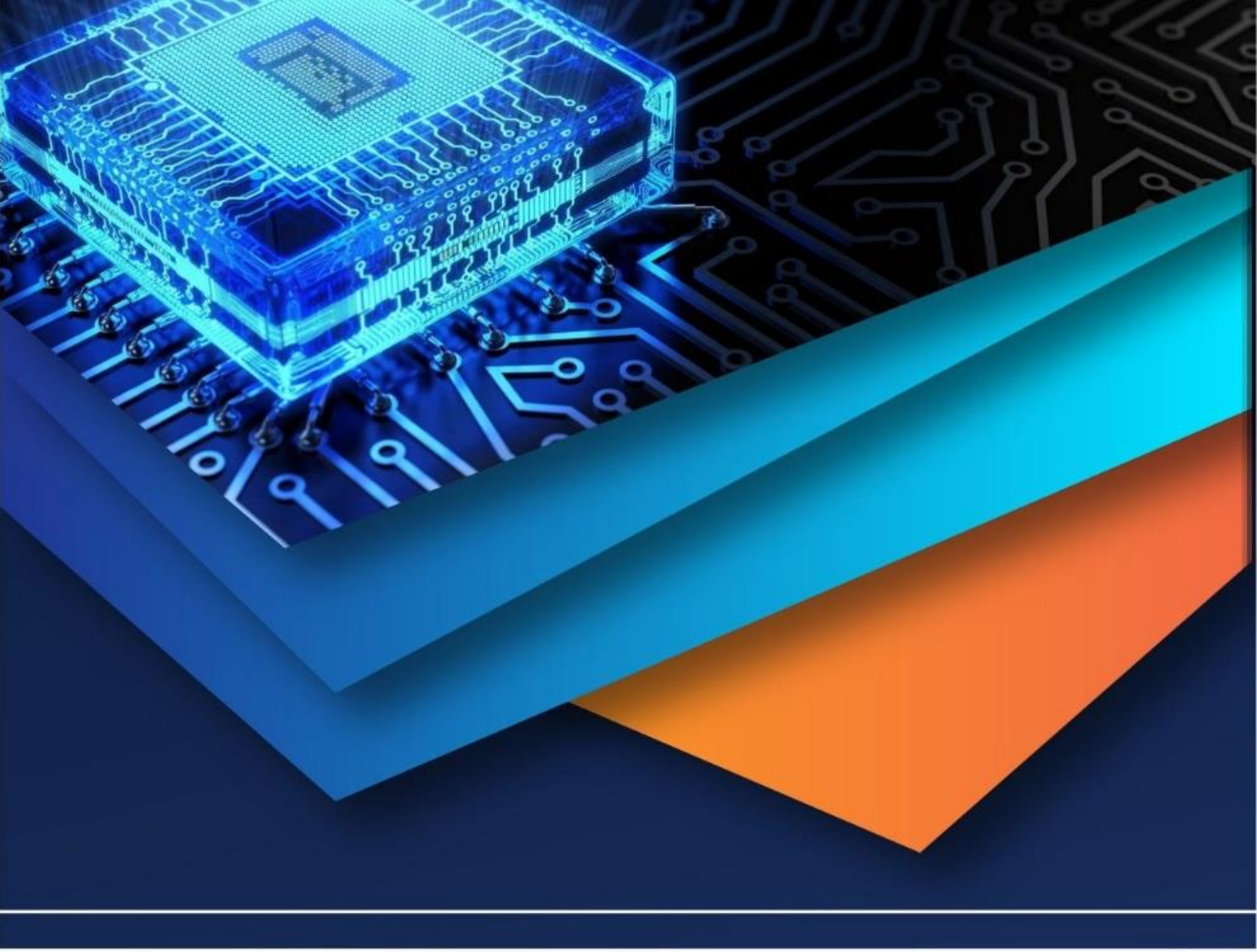

Fig 6.4: Completed Verification of User in AI eKYC System

## VII. CONCLUSION

The AI & Blockchain Based eKYC Verification System is an efficient, effective, and safe system for the verification of digital identities. The system utilizes various artificial intelligence technologies such as face recognition and liveness detection, along with the power of blockchain technology, to provide the best possible experience in the verification of user identities. The system is effective in the verification process as compared to traditional KYC systems, which often result in various issues such as the risk of identity theft, data tampering, and the registration of duplicate identities. The system is effective in the verification process as compared to traditional KYC systems, which often result in various issues such as the risk of identity theft, data tampering, and the registration of duplicate identities. The system is effective in the verification process as compared to traditional KYC systems, which often result in various issues such as the risk of identity theft, data tampering, and the registration of duplicate identities. The system is effective in the verification process as compared to traditional KYC systems, which often result in various issues such as the risk of identity theft, data tampering, and the registration of duplicate identities. The system is effective in the verification process as compared to traditional KYC systems, which often result in various issues such as the risk of identity theft, data tampering, and the registration of duplicate identities. The system is effective in the verification process as compared to traditional KYC systems, which often

## REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[2] V. Buterin, “Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform,” 2014.
[3] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” Ethereum Project Yellow Paper, 2014.
[4] DeepFace, “Deep Learning Face Recognition Library,” GitHub Repository, 2020.
[5] F. Schroff et al., “FaceNet: A Unified Embedding for Face Recognition and Clustering,” CVPR, 2015.
[6] J. Deng et al., “ArcFace: Additive Angular Margin Loss for Deep Face Recognition,” CVPR, 2019.
[7] A. Rosebrock, “Face Detection with OpenCV,” PyImageSearch, 2020.
[8] Ethereum Foundation, “Solidity Documentation,” https://soliditylang.org
[9] Nomic Foundation, “Hardhat Development Environment,” https://hardhat.org
[10] G. Wood et al., “Web3.js and Web3.py Documentation,” Ethereum Developer Resources, 2021.
[11] M. Swan, “Blockchain: Blueprint for a New Economy,” O’Reilly Media, 2015.
[12] A. Mosenia and N. Jha, “A Comprehensive Study of Security of Internet-of-Things,” IEEE Transactions, 2017.
[13] R. Lu et al., “E-Healthcare Information Security Using Blockchain,” IEEE Access, 2019.
[14] K. Krombholz et al., “Security and Usability of Blockchain Wallets,” IEEE Symposium, 2018.
[15] S. Singh and N. Singh, “Blockchain: Future of Financial and Cyber Security,” ICACCI, 2016.
[16] Python Software Foundation, “Python Documentation,” https://www.python.org
[17] Flask Documentation, “Flask Web Framework,” https://flask.palletsprojects.com
[18] OpenCV, “Open Source Computer Vision Library,” https://opencv.org
[19] Web3.py Documentation, “Ethereum Interaction using Python,” https://web3py.readthedocs.io
[20] NIST, “Digital Identity Guidelines (eKYC Standards),” National Institute of Standards and Technology, 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)