Journal of Analysis and Computation (JAC)
(An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861
Volume XVIII, Issue II, July-December 2024

DOCUMENT VERIFICATION USING COMPUTER VISION (EKYC)

Lokesh Chavan[1], Sanskruti Dumbre[1], Vedanti Wandile[1], Sana Sayyed[1], Aparitosh Gahankari[2]

1Student, Department of Artificial Intelligence, St. Vincent Pallotti College of Engineering and Technology Nagpur, India

2Assistant Professor, Department of Artificial Intelligence, St. Vincent Pallotti College of Engineering and Technology, Nagpur, India

ABSTRACT

The aim of this project is to design an end-to-end eKYC verification system using face recognition and OCR techniques. The system allows the users to take a webcam shot of their ID proof and capture their face for identity verification And, it uses Tesseract OCR to recognize the name, address, and contact that are included in ID proof and utilizes regular expression for converting the ID in containing structured text. At the same time a face verification process is performed to ensure the face of the user is the same as that on the ID. Once verification is successful, the next step displays an auto-fill form that contains the data retrieved from the previous steps and required for user confirmation. Flask, JavaScript and HTML/CSS are the technologies used in the project which creates a highly efficient application that is easy to use while being accurate and secure in eKYC procedures.

Keywords: E-KYC, Identity Verification, OCR, Face Verification, Flask Framework, Text Extraction, Autofill Form, Image Processing.

[1] INTRODUCTION

In the present-day digital ecosystem, identity verification has become the bulwark for secure entry into such services as banking and government benefits. Traditional KYC (Know Your Customer) processes are never straightforward; they involve tiresome long queues, errors, and human interference. Thus, to deal with these problems, this project sets up an eKYC (electronic

Know Your Customer) system that runs on advanced technologies to assist in raising the pace and efficiency of the verification process. The tool allows users to upload valid identification documents and a live facial image through the webcam. The Optical Character Recognition (OCR) would extract name, address, and contact information from the ID proof. The recognition of the individual's face would also be involved in the identity verification system. The information processed in different steps will later be automatically populated within a digital file, thus alleviating the workload of manual work and intervention decisions in problems where blood relations exist. Not only would this solution accelerate user convenience and operational efficiency, but it would also ensure accuracy and security in sensitive data management. Subsequently, with the assistance of intelligent algorithms and user-friendly interfaces, the project has thus proved to showcase a practical method for bringing identity verification to a quicker, more reliable, and adaptable scale in real-life scenarios.

[2] RELATED WORK

As digital transformation accelerates, the need for robust, efficient identity verification systems has become crucial across industries such as finance and healthcare. This review explores the latest advancements in document verification and electronic Know Your Customer (eKYC) technologies, focusing on the integration of computer vision, biometric authentication, and blockchain for enhanced security and operational efficiency. By analysing various research findings, the review highlights the advantages of these technologies, including improved data integrity, user experience, and regulatory compliance, while also discussing challenges like high implementation costs, data privacy issues, and integration complexity. Additionally, the review identifies emerging trends such as artificial intelligence (AI) and the Internet of Things (IoT) in eKYC systems, which promise further advancements in identity verification. This review aims to provide insights into the current landscape of eKYC technologies and to outline future directions for secure, scalable digital identity solutions.

The paper [1] addresses the challenge that deepfake technology poses to electronic Know Your Customer (eKYC) systems, which are vulnerable to sophisticated fake videos used for identity fraud. To address the lack of suitable datasets for developing eKYC defenses, the authors created eKYC-DF, a large-scale dataset of over 228,000 videos with realistic facial movements and diverse demographics tailored to eKYC needs. Built using face-swapping technologies like SimSwap, FaceDancer, and SberSwap, the dataset improves model training for liveness detection and deepfake resistance in eKYC systems. Although it lacks audio-visual deepfakes, the dataset serves as a foundational resource, with future work suggested for expanding multimodal deepfake detection and enhancing generalisation to other datasets.

The paper [2] presents an advanced, efficient KYC (Know Your Customer) authentication system designed for digital banking environments. It highlights the growing need for robust customer verification methods, particularly in an era of increasing cybersecurity threats and regulatory demands. The proposed system integrates modern technologies to streamline

customer onboarding while ensuring secure verification. By leveraging electronic KYC (eKYC) procedures, the system aims to enhance security measures and user experience, reducing the reliance on traditional, time-consuming methods. The solution also addresses scalability concerns, enabling financial institutions to handle larger customer bases with minimal risk and greater efficiency. This innovation supports regulatory compliance while providing a more user-centric and secure banking experience.

The paper [3] presents a decentralized solution for enhancing KYC processes and microfinance using blockchain technology. It addresses key issues such as multiple KYC verifications, security vulnerabilities, and high costs due to intermediaries. By leveraging blockchain's transparency and immutability, the system securely centralizes KYC data, reducing data breaches and fraud. Smart contracts automate KYC verification and peer-topeer lending, eliminating the need for intermediaries and lowering transaction costs. The use of Polygon blockchain further reduces costs, making the system more efficient. While the approach improves security and transparency, challenges include the complexity of implementation and scalability concerns. The authors propose further development toward a fully decentralized KYC model with broader applications in finance.

The [4] examines the challenges of using face recognition technology on historical photographs from a Theatre Museum, where actors are depicted in various angles, poses, ages, and costumes. It highlights issues such as significant intra-class variations and image decay, which complicate accurate identification. The study specifically evaluates Elastic Face, a face recognition model trained with a novel learning loss strategy, which successfully addresses these problems, achieving an accuracy of 79.6%. This performance indicates that face recognition can provide meaningful insights for historians analysing complex historical image collections.

The paper [5] processes face significant challenges, including inefficiencies, security vulnerabilities, and difficulties in verifying individuals without formal documentation. While e-KYC has improved authentication by incorporating AI and other digital technologies, vulnerabilities such as susceptibility to deepfake attacks remain a concern. Existing methods like Haar-cascade for face detection and Deep Face for image recognition offer accurate results but struggle with issues like complex lighting conditions and demographic diversity. Additionally, datasets such as eKYC-DF, which consist of over 228,000 high-quality deepfake videos, have been developed to improve model training for liveness detection and deepfake resistance. However, the dataset's limitation to visual deep fakes and lack of multimodal integration highlight gaps in current solutions.

The Paper [6] has emerged as a transformative solution for addressing critical challenges in healthcare data management, including security, privacy, and interoperability. Traditional healthcare systems often rely on centralized databases, making them vulnerable to breaches and unauthorized access. Blockchain's decentralized architecture ensures data integrity and tamper resistance through immutable ledgers and smart contracts, offering robust access control

mechanisms. Furthermore, it empowers patients by granting them ownership and control over their health information while ensuring confidentiality and compliance with regulatory standards. The technology also enhances interoperability, enabling seamless data sharing across healthcare providers, streamlining processes, and ultimately improving patient outcomes. Real world case studies have demonstrated how blockchain can transform healthcare operations by enhancing efficiency and accuracy.

The paper [7] has become a cornerstone of the banking sector's transformation, particularly in enhancing Know Your Customer (KYC) processes. This article explores the integration of cutting-edge technologies like machine learning, blockchain, and 5G communication in shaping modern identity verification systems. Machine learning facilitates the detection of fraudulent activities through advanced anomaly detection algorithms, while blockchain ensures the immutability and integrity of identity data. Additionally, 5G communication enables real time identity verification, enhancing the efficiency of financial transactions. Case studies demonstrate how these technologies streamline operations, improve customer experiences, and bolster security, offering a promising pathway for secure and efficient banking practices in the digital era.

[3] METHODOLOGY

Methodology To carry out this project a systematic approach is adopted such as image processing, text extraction and facial recognition techniques. The methodology is as follows: Data Collection: Users inquire, upload their identity documents and take a real-time image of their face using a webcam connected in the application itself.

Optical Character Recognition (OCR): The uploaded ID proof is subjected to OCR to retrieve text - for example the name, address, and contact details of the user. Development and use of advanced text processing techniques to retrieve relevant information from unstructured texts. Facial Recognition: The system does a recognition by matching the captured image's output to the image extracted from the provided ID proof. Secure and Reliable Matching Powered by Machine Learning Facial Comparison Autofill Form Generation: The validated information is used. Data Collection: Users upload their identity documents and capture a live facial image using a webcam integrated with the application.

Facial Recognition: The system compares the live captured facial image with the photo extracted from the uploaded ID proof to verify the identity. Machine learning-based facial matching ensures reliable and secure comparisons.

Autofill Form Generation: The extracted information, once validated, is used to pre-fill a digital form with user details. This eliminates manual entry and streamlines the process. Verification Result: The system displays the verification outcome, allowing users to proceed with further steps only if their identity is successfully confirmed.

Integration and Output: The application consolidates the processed data and presents it in a user-friendly format for further use, ensuring efficiency, accuracy, and security throughout the workflow.

[4] ARCHITECTURE

The Engineering of the Project: The design of this venture points to streamline the method of confirmation of character and extraction of information employing a web-based stage, taking after a client-server show that includes a client (client) collaboration with the browser interface and the server carrying out diverse functions. Client-side The UI of the application is built utilizing HTML, CSS, and JavaScript. The clients transfer the checked duplicates of their ID and snap a picture of their confrontation utilizing the webcam. The picture capturing is done through JavaScript, which changes over the captured confront picture into base64 organize and sends it to the server for processing. Server-side Flask System: The server is built on Carafe, a web system based on Python. Carafe gets demands and conveys reactions, rendering a web page to the user. OCR for Content Extraction: The transferred ID picture is filtered for Optical Character Acknowledgment (OCR), for the most part by Tesseract, to drag out the content for pertinent areas required such as title, address, and date of birth. Face Confirmation: The captured confront picture is compared and confirmed against ID verification through facial acknowledgment methods. This makes a difference in verifying that the individual uploading the archive is really the same individual as the one within the photo. (Optional) Database A database can be utilized to store client information or to confirm against already transferred qualifications. In any case, in this plan, the extricated information is given for seeing after the completion of verification. Verification and Result Display The backend forms the extricated information and the confront confirmation comes about. If the confrontation matches, at that point the essential client subtle elements are auto filled into a shape, permitting the method to proceed. Something else, the complete preparation of confirmation is hailed as failed. This design guarantees a secure, robotized, and immaculate handling of confirmation of character, extraction of data from archives and auto filling shapes in a web environment.

Journal of Analysis and Computation (JAC)
(An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861
Volume XVIII, Issue II, July-December 2024

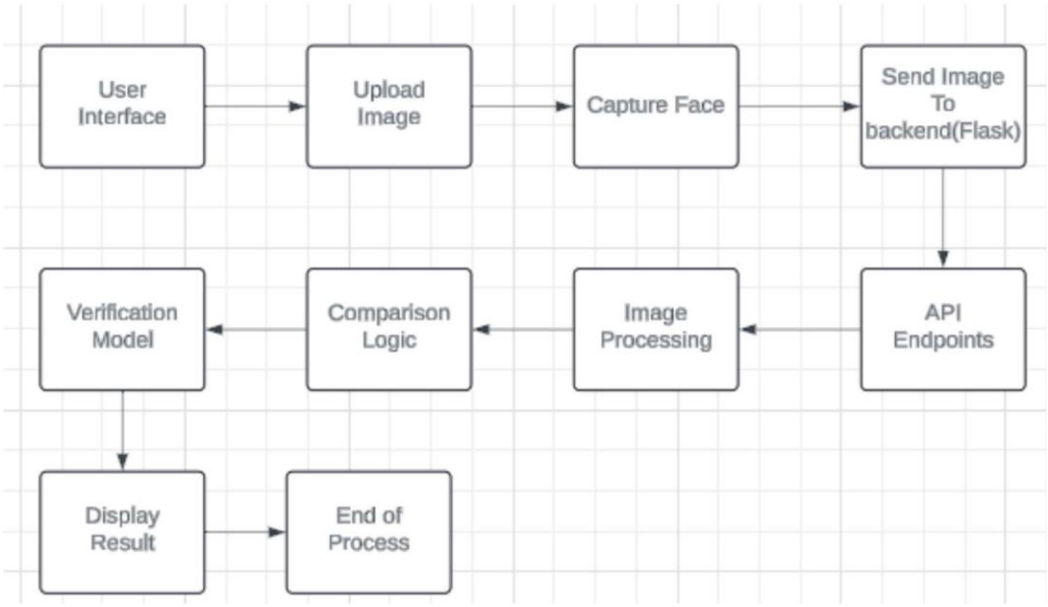

Fig. 1 System Architecture

[5] PROPOSED WORK

In today's advanced world, character confirmation and information extraction from official records have become progressively basic, particularly for online administrations that require verification. The proposed work points to streamline the method of confirming a user's personality by leveraging advances like Optical Character Acknowledgement (OCR) and facial acknowledgment to extricate and compare information from government-issued character archives such as Aadhaar cards. The framework will work by permitting clients to transfer their character verification pictures and capture a live picture of their confrontation by means of a webcam for comparison. The centre of this framework rotates around two key functionalities: content extraction and confront confirmation. The content extraction component will utilize OCR to extricate key data from the transferred ID, such as the user's title, date of birth, address, and other important subtle elements. This extricated data will be utilized to autofill a client shape that demands extra points of interest for Proposed Work. In today's advanced world, character confirmation and information extraction from official records have become progressively basic, particularly for online administrations that require verification. The proposed work points to streamline the method of confirming a user's personality by leveraging advances like Optical Character Acknowledgement (OCR) and facial acknowledgment to extricate and compare information from government-issued character archives such as Aadhaar cards.

The framework will work by permitting clients to transfer their character verification pictures and capture a live picture of their confrontation by means of a webcam for comparison. The centre of this framework rotates around two key functionalities: content extraction and confront confirmation. The content extraction component will utilize OCR to extricate key data from the transferred ID, such as the users title, date of birth, address, and other important subtle elements. This extricated data will be utilized to autofill a client shape that demands extra points of interest for assist handling. In expansion, the confront confirmation module will compare the confront from the transferred ID to the confront captured through the webcam, guaranteeing that the individual submitting the archive is undoubtedly the legitimate owner.

The proposed framework is planned to be profoundly user-friendly, with a straightforward interface where clients can transfer their ID verification and capture their confrontation in realtime. Once the information is extricated and confront confirmation is performed, the framework will autofill the frame areas with the pertinent data, decreasing the required for manual input and minimizing errors. The design will comprise of a web-based frontend built utilizing HTML, CSS, and JavaScript, giving a consistent client involvement. The backend will be actualized utilizing Carafe, a lightweight Python system, which can handle all the preparing, counting OCR for content extraction and integration with facial acknowledgment calculations. Besides, the framework will consolidate security measures to guarantee the security of touchy client information and anticipate misuse.

The extend will permit for adaptability and versatility, as the strategies utilized for content extraction and confront confirmation can be adjusted to handle a wide assortment of identity reports and client scenarios. Through this framework, we aim to supply a secure, productive, and computerized arrangement for personality confirmation, making a difference to diminish extortion and progress the effectiveness of online administrations that require client confirmation.st handling. In expansion, the confront confirmation module will compare the confront from the transferred ID to the confront captured through the webcam, guaranteeing that the individual submitting the archive is undoubtedly the legitimate owner. The proposed framework is planned to be profoundly user-friendly, with a straightforward interface where clients can transfer their ID verification and capture their confrontation in real-time. Once the information is extricated and confront confirmation is performed, the framework will autofill the frame areas with the pertinent data, decreasing the required for manual input and minimizing errors. The design will comprise of a web-based frontend built utilizing HTML, CSS, and JavaScript, giving a consistent client involvement.

The backend will be actualized utilizing Carafe, a lightweight Python system, which can handle all the preparing, counting OCR for content extraction and integration with facial acknowledgment calculations. Besides, the framework will consolidate security measures to guarantee the security of touchy client information and anticipate misuse. The extend will too permit for adaptability and versatility, as the strategies utilized for content extraction and confront confirmation can be adjusted to handle a wide assortment of identity reports and client scenarios. Through this framework, we point to supply a secure, productive, and computerized

arrangement for personality confirmation, making a difference to diminish extortion and progress the effectiveness of online administrations that require client confirmation.

[6] RESULTS AND ANALYSIS

The framework created for character confirmation and information extraction from Aadhaar cards has been effectively executed and tried. The centre functionalities, counting Optical Character Acknowledgement (OCR) for extricating client subtle elements from the transferred ID verification and confront confirmation through a webcam, have been coordinated successfully. The OCR module precisely extricates basic information such as title, date of birth, address, and other significant data from the ID verification. The confront confirmation module compares the captured confront with the one on the ID and gives a match/non-match result. Also, the framework can autofill the extricated subtle elements into a client frame, altogether lessening manual information passage blunders and speeding up the confirmation process. The general client encounter is natural and user-friendly, with clear information for uploading reports and capturing the confront. The system's execution in terms of information extraction precision and confront confirmation unwavering quality has met the extend objectives, with negligible mistakes in extraction and tall exactness in confront comparison. The integration of these innovations has demonstrated to be an compelling arrangement for confirming character in real-time.

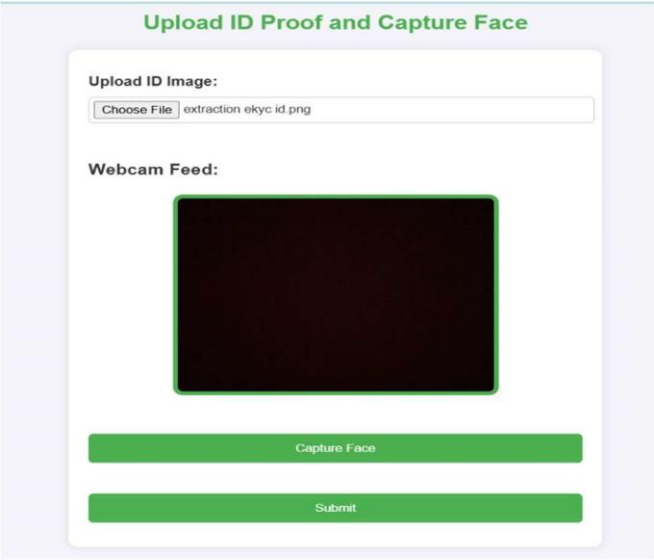

Fig. 2 Final Predicted Output

[7] FUTURE SCOPE

While the current execution serves as a solid establishment for personality confirmation, there are a few openings for future upgrades and advancements. A few of the potential zones for advancement include: 1. Bolster for Numerous Personality Records: The framework can be expanded to bolster an assortment of government-issued reports (e.g., identifications, driver licenses, voter ID cards) for broader applicability. 2.Progressed Confront Acknowledgement Calculation: By coordinating more progressed machine learning models for confront confirmation, the framework seems accomplish higher exactness and strength, indeed in challenging lighting conditions or with minor varieties in facial features. 3.Real-time Video Gushing for Confront Capture: Rather than capturing a single outline, the framework can be overhauled to handle real-time video gushing for confront capture, guaranteeing the confirmation prepare is more energetic and flexible. 4. Improved Information Security: With the expanding significance of information security, extra security conventions such as encryption, secure capacity, and multi-factor confirmation can be executed to secure delicate client information. 5.Portable App Integration: Creating a portable adaptation of the application seems to make it more open for clients who prefer to perform character confirmation on their smartphones, upgrading the system convenience over diverse platforms. 6.AI-based Mistake Taking care of and Information Redress: Actualizing machine learning calculations to identify and redress common OCR extraction blunders (such as misinterpret names or addresses) might assist move forward the exactness of information extraction. 7. Adaptability and Cloud Integration: Moving the backend to the cloud can move forward the system's adaptability, making it competent of dealing with expansive volumes of information and numerous concurrent clients, which is basic for arrangement in commercial or government applications. By tending to these ranges, the framework can be assist optimized for a wide run of real-world applications, from monetary administrations to government forms, making character confirmation speedier, more secure, and user-friendly.

[8] CONCLUSION

This venture illustrates the effective integration of Optical Character Acknowledgement (OCR) and confront confirmation advances to make an effective personality confirmation framework. The framework successfully extricates key subtle elements from Aadhaar cards and compares the captured confront with the one on the ID, guaranteeing precise personality approval. The auto-filling of extricated data into a shape streamlines information section, diminishing human blunders and moving forward in general effectiveness. While the current framework has appeared promising comes about in its capacity to confirm identities and extricate fundamental data, there's plentiful scope for assist upgrade. Future enhancements, such as bolster for extra character reports, way better confront acknowledgment models, and progressed security measures, can extend the system’s usefulness and pertinence. Eventually, the venture lays a

solid establishment for robotized personality confirmation arrangements, with the potential for wide selection in different divisions requiring secure and proficient client confirmation.

REFERENCES

[1] Hichem Felouat, Huy H. Nguyen, Trung-Nghia Le, Junichi Yamagishi, and Isao Echizen: eKYC-DF: A Large-Scale Deepfake Dataset for Developing and Evaluating eKYC Systems. IEEE Access, Volume 12 (2024). Digital Object Identifier: 10.1109/ACCESS.2024.3369187.
[2] Nor Izham Subri, Abdul Ghafur Hanafi, and Mohd Affendi Ahmad Pozin: Comparative Analysis of eKYC and 2FA in Implementing PADU Database System to Strengthen Digital Identity Security.
[3] Sri Sai, Ramisetty Nikhil, Shivangini Prasad, and Nenavath Srinivas Naik: A Decentralised KYCBased Approach for Microfinance Using Blockchain Technology. Volume 1 (December 2023), 100009.
[4] Khan, M., et al.: Secure and Efficient Electronic Know Your Customer (e-KYC) System Based on Blockchain Technology. IEEE Transactions on Services Computing (2023).
[5] Pranav Khare and Shristi Srivastava: Transforming KYC with AI: A Comprehensive Review of Artificial Intelligence-Based Identity Verification. JETIR, Volume 10, Issue 12 (December 2023).
[6] Hizogie Paul Adeghe, Chioma Anthonia Okolo, and Olumuyiwa Tolulope Ojeyinka: Evaluating the Impact of Blockchain Technology in Healthcare Data Management: A Review of Security, Privacy, and Patient Outcomes. Open Access Research Journal of Science and Technology, Volume 10, Issue 2 (March 30, 2024), pp. 013–020.
[7] Sachin Parate, Hari Prasad Josyula, and Latha Thamma Reddi: Digital Identity Verification: Transforming KYC Processes in Banking Through Advanced Technology and Enhanced Security Measures. Volume 5, Issue 9 (September 2023).
[8] Dr. Manoj Kumar, Nikhil, and Parina Anand: A Blockchain-Based Approach for an Efficient Secure KYC Process with Data Sovereignty. International Journal of Scientific & Technology Research, Volume 9, Issue 1 (January 2020).
[9] Anuraj Soni and Reena Dugga: Reducing Risk in KYC (Know Your Customer) for Large Indian Banks Using Big Data Analytics. International Journal of Computer Applications, Volume 97, Issue 9 (July 2014).
[10] Sri Sai, Ramisetty Nikhil, Shivangini Prasad, and Nenavath Srinivas Naik: A Decentralised KYCBased Approach for Microfinance Using Blockchain Technology. Volume 1 (December 2023), 100009.