

Transforming KYC with AI: A Comprehensive Review of Artificial Intelligence-Based Identity Verification

Pranav Khare
Independent Researcher
Woodinville, WA, USA
khare.pranav@gmail.com

Shristi Srivastava
School of Science, Technology, Engineering & Mathematics
University of Washington Bothell
Woodinville, WA, USA
shristisrivastava14@yahoo.com

Abstract— In the context of business operations, it is imperative for service providers to engage in the identification and evaluation of clients, as well as the assessment of the risks associated with them, before proceeding with the delivery of services. Providers have challenges in verifying the identities or completing due diligence of potential customers who do not possess formal documentation or whose identity verification is problematic. The process of e-KYC entails authorized organizations accessing a digital identification system in order to identify and validate the identities of clients, occasionally extracting necessary information. This study presents an advanced E-KYC (Know Your Customer) authentication system that leverages blockchain technology and AI-driven face recognition to address the inefficiencies and security vulnerabilities of traditional KYC processes. In addition, the proposed system contains data storage using encrypted blocks and users' consent-based data sharing for privacy. Some of the causal attributes that make identification and recognition accurate are Haar-cascade for face detection, Deep Face for image comparison, and others give this project an accuracy rate of 92%. It provides an intuitive graphical user interface to ease the process of using the system and uses OTP for further user authentication. Administrators are able to increase efficiency through the utilization of efficient fast search and date wise sorting for subsequent user interaction tracking.

Keywords— KYC, E-KYC, AI-driven, DNN, Haar-cascade, Deep Face.

I. INTRODUCTION

The Know Your Customer (KYC) procedure is one that banks apply to obtain information on the name and address of customers as well as the buyers and debtors. To ensure that the abuse of financial services is prevented, the procedure requires that authorities oversee it and complete checks to verify the identity of the customers. Banks are required to maintain their KYC records and to follow the process of KYC while opening accounts. The KYC procedure, however, was slightly cumbersome, time-consuming, and specific to some institutions. Every enterprise needs to identify its clients, but it is especially necessary in the sphere of financial services and products. KYC procedures are used to assist businesses make sure they are aware of who they are doing business with in order to accomplish this. This procedure provides the banking industry and financial institutions with a background check and a feeling of security. The KYC procedure is often a laborious and drawn-out procedure where customers must provide certain documentation, submit to background checks, and go through verification [1]. Figure 1 illustrates the increased cost, delay, and redundancy associated with the banks' existing manual KYC procedure. However, automating the KYC process might lead to an upsurge in criminality and compromise client privacy via system exploits. Because of its decentralized, immutable, and trustless nature, the newly developing Blockchain Technology may provide a means to safeguard the KYC procedure.

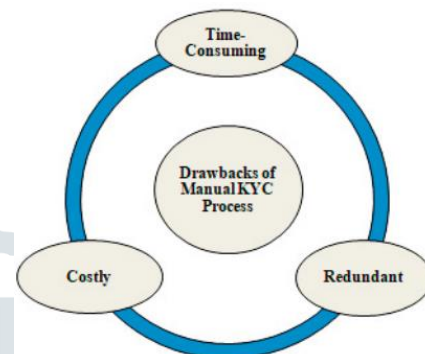


Fig.1. Drawbacks of Manual KYC

Financial institutions' primary goal in implementing KYC is to help them stop money laundering, identity theft, terrorist funding, and profiling. Eliminating rogue creditors is another benefit. Traditionally, each bank or other institution uses a government framework or a stand-alone organization to carry out its own KYC procedure for every customer. This is a time waster since it implies that if someone wants to create a new bank account, they have to go through the same KYC procedure all over again. In addition, KYC data must be updated often, requiring a lot of human labor and duplication when changing an address or phone number [2] [3].

Financial institutions and service providers are investigating the use of next-generation technologies like AI and cognitive technologies to solve these issues. Blockchain is one technology that has the potential to completely transform the cumbersome KYC procedure. We may more fully grasp the need for blockchain technology for KYC by being aware of the flaws of the present approach [4]. The inefficiencies annoying are the centralized KYC processing that is not standardized across different bank or service providers. Again, customers have to repeat the KYC process every time they engage with an institution and this is very unnecessary, creating work and leaving incomplete data sets. This fragmented structure poses a problem when financial institutions are to integrate their clients' spending across different platforms because it leads to inefficiency of the KYC process. It also creates the risk of flagging false values, low customer profiling, clients providing fake information, and long processing time. These make the KYC expensive and contribute to the general expansion in cases of money laundering[5].

The need to combat the inefficiencies and security risk of conventional KYC processes underlines the motivation behind this work. In the proposed e-KYC model, the use of blockchain and artificial intelligence should make e-KYC transactions secure, efficient, and user-friendly. The importance of decentralization can be seen in the areas of privacy, decreased verifying time, and lastly, reduced operational costs to the banking institutions. These are the main contributions of the work, which include the application

of blockchain for achieving the secure storage of data and management of user consent and the identification of new AI algorithms for enhanced and accurate face recognition and OCR-based document validation leading to much efficient identity validation process. The key contribution of this paper as:

- **Enhanced Security and Privacy:** The incorporation of blockchain helps in secure storage of the user data and restricts the data to be accessed without the user permission drastically reducing risk of data leak and unauthorized access.
- **Improved Verification Accuracy:** Sophisticated AI algorithms, namely Haar-cascade to recognize faces and Deep Face for comparing images, ensure high accuracy when it comes to the identification of a person and has a 92% accuracy rate.
- **Streamlined User Experience:** The e-KYC system provides the feasibility of conducting identity verification in a shorter amount of time, and with less effort, while integrating OTP-based authentication mechanism for enhanced security.
- **Efficient Data Management:** The admin interface provides tools for targeted searches and date-wise filtering, allowing for effective monitoring, evaluation, and management of user activities, thus improving overall administrative efficiency.
- **Reduction in Operational Costs:** By digitizing and automating the KYC process, the system reduces the need for manual intervention and paperwork, leading to lower operational costs and increased efficiency for financial institutions.

A. Organization of paper

The remainder of the document is arranged as follows. Section 2 provides an overview of the relevant research work in the field. Section 3 describes the methodology with steps, flowchart, and performance evaluation criteria. The findings and discussion are presented in Section 4. The study is concluded with suggested future work in Section 5.

II. LITERATURE REVIEW

The main goal of this procedure is to detect and stop fraudulent actions such as money laundering, identity theft, funding of terrorism, etc. However, the cost of handling KYC per client may be high because to a lack of transparency, distrust, and data duplication. Blockchain technology holds a self-sovereign and Decentralised Know Your Customer (DKYC) structure which aids the process of establishing trust. Due to the benefits of regulator supervision, consent-based access, and lower customer acquisition cost, this approach enables banks to use trustworthy and rightful customer information that enhances consumer privacy as well.

In [6], exhibits experiments using several neural networks taking into account a publicly available database of actual camera photos and identification papers. Using the ID picture database images and a deep neural network trained with an Arc Face loss function, the findings demonstrate a recognition rate of more than 94%. We also validate this method with a small sample of Chilean individuals and find that they achieve a comparable rate. Our recommendation for future research is to make use of bigger databases that contain document data from Chile.

In[7], to design and implement an ML-based verification portal for the users where they can update and verify their credentials as and when required for banking

purpose, for opening new Bank accounts, applying for Loan and other Business requirements with the comfort of time. It entails gathering the client's basic address and identification data. This would not only greatly expedite the KYC procedure but also ensure error-free execution. Customers may snap pictures of their AADHAR credentials using our mobile application to update their KYC. The application will make advantage of OCR to reduce typing mistakes, resulting in error-free form completion and time savings.

In[5], to identify a way to solve the issue of user authentication in a car-sharing system that relies on the KYC procedure by combining DL techniques with OCR approaches. They researched and used deep learning algorithms and the fast Hog approach to extract the client's face from the picture and compare it to others. Results obtained by applying these techniques to a test dataset consisting of document photos from 2,000 customers demonstrated a 91% recognition accuracy as measured by Jaccard's score. In comparison to 3.3 seconds when using trained models, the average time it took to separate faces using the Hog technique was 0.2 seconds. Combining ROI and ORC separation techniques allows for a substantial improvement in verification accuracy.

In [8], have suggested a decentralized KYC verification procedure based on the Ethereum Blockchain. All banks connected to the Blockchain network would be able to confirm and cast votes about the authenticity of the information that customers provide. The KYC status of a consumer is recorded on the Blockchain based on the number of votes they get. A significant improvement to our suggested approach is that banks will be able to vote for other banks to be removed from the network if they are found to be manipulating KYC data. With its unique characteristics, Blockchain may be used in this manner to increase the effectiveness of the KYC procedure.

In[9], in order to address this problem. They proposed a blockchain-based approach that eliminates the need for numerous KYC checks by performing a single KYC verification and maintaining a single safe database. The user's consent is required before any of the participating financial institutions on the blockchain may access their KYC data. Even without the need for intermediaries, the user retains full authority over their data. The customer might choose to let the bank see their KYC information or not. Sharing KYC data on Blockchain will help financial organizations improve compliance, efficiency, and customer experience.

In[10], the proposed system, each client only has to go through the essential KYC verification procedure once, regardless of how many financial institutions they want to operate with. Through the use of DLT, users may safely communicate the outcome of their basic KYC verification with all the financial institutions they choose to collaborate with. Efficiency improvements, cost savings, an enhanced client experience, and more transparency throughout the onboarding process are all made possible by this technology.

Despite advancements highlighted in the integration of blockchain and machine learning technologies for KYC processes, several research gaps remain. One significant gap is the scalability and interoperability of decentralized KYC systems across different regulatory environments and financial institutions. To promote the use of such solutions across the banking industry, guidelines and frameworks must be created that could be easily implemented into existing systems. Moreover, despite increased effectiveness of identity verification through the use of OCR and deep learning, more studies should be conducted to reduce the impact of bias and increase the efficiency of these

technologies. Another important aspect of the system is connected to the issues of KYC data storage on the blockchain and possible ways of their leakage and unauthorized access. Similarly, these radical changes in terms of the distribution of KYC methodologies require procedural analyses based on cost-benefit ratios because, essentially, the adjustment will affect the financial institutions' economics. Finally, the rules and regulations concerning the implementation of KYC through blockchain have to be analyzed deeply in order to determine their compliance with the state and international legislation as well as to gain the confidence of the state authorities and users. It is therefore evident that developing research focusing on these gaps will go a long way in improving the effectiveness and adoption of decentralized KYC solutions.

III. METHODOLOGY

KYC thus stands as a major step forward as towards providing clients with an option to complete the on-boarding process online, thus rejecting the limitations of traditional model of KYC. This paper aims at discussing the applicability of blockchain technology in enhancing the safety and privacy facets in the e-KYC and outline some of the modern-day issues in customer identification processes. Thus, using artificial intelligence algorithms to detect the face and verify and use OCR the proposed e-KYC has the potential to become the efficient tool to achieve identity validation in shortest possible time. There are two key part in this module:

3.1 E-KYC authentication system

A. User End

The proposed website offers users the choice to either sign up or log into their accounts upon visiting. To register as a first-time visitor, you need to provide your name, phone number, and create a username and password. Returning users can easily log in using their username and password. After logging in successfully, users can access the home page, which includes a KYC tab for completing a form. The user is directed to a new page where they can enter their mobile number to receive an OTP. Users can fill out the form after entering the correct OTP. The user enters personal details such as their first and last name, contact number, and either Aadhaar card or PAN card number. To complete the process, users must upload a scanned image of the card and use a working webcam for live video recording. To submit the uploaded video and card image, simply click the designated button.

The technologies and algorithms used include Python, HTML, CSS, Haar-cascade, and Deep Face (VGG Face model). The system uses Haar-cascade to detect faces in live videos and card images [11]. It also utilizes Deep Face for image comparison to verify identity. The user's details are verified by comparing them with the information on their Aadhaar card or PAN card. The Python Tesseract OCR tool is used for extracting text from documents[12][13]. Verification success leads to a confirmation message. User data and outcomes are securely stored in the database.

B. Admin End

The admin needs to log in to their designated account to access the admin homepage and start performing administrative functions. Several tools and functions are assigned to the admin control allowing them to manage users and their operations securely. On the admin homepage, there is an option for listing all the users who have used the service. The user roster within this context is a source for reference regarding platform usage. The search engines within the

program can be utilized to search for specific users, allowing admins to easily find information. This has made it easier for the admin to scrutinize or manage specific user by use of the search bar that is provided.

Furthermore, the admin can filter data according to different periods next to the capabilities focused on users. More specifically, the date-wise filtering mechanism brings effectiveness into the picture regarding the time intervals the admin look for the user information. The feature can be used to obtain additional information about the tendencies, patterns, and activity of the users in certain periods of time by the admin. Many options are provided in the admin interface, which contributes to the proper assessment and management of user interactions. The admin has all the options needed to track and manage the platform activities via lists of users and filters based on search results and date.

3.2 AI and Deep Learning

Some of the latest innovations include self-driving cars that move on the tarmac, recommendation of products by online selling firms, and voice recognition in smartphones, all of which are facilitated by AI [14]. The applicability of ML and DL—a subfield of AI—to solve issues with superior performance has been proved.

DL algorithms are designed to function similarly to how the human brain does. Importantly, DL can learn from massive datasets. A hierarchical approach to learning is used by deep learning[15]. The term "deep" refers to a multi-stage process that involves learning and analyzing data in order to get the desired result. A DL neural network is shown schematically in Figure 2.

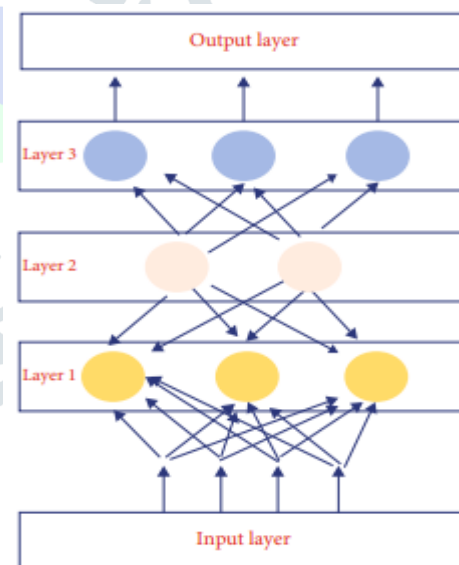


Figure 2: Deep learning neural network.

Neural networks, as seen in Figure 2, are networks of neurons that resemble human brains. The components of an AI architecture include an input layer, an output layer, and many hidden levels, including layers 1, 2, and 3 [16]. The intended usage determines the optimal number of hidden layers. A model for an AI-powered autonomous car, for instance, may have millions of hidden layers. Typically, a DNN will include several hidden layers. Compared to other methods, DNN is much better at face recognition because it allows users to focus on a specific area of an image for exploration rather than assessing the whole image. Most people know convolution as the method for DNN-centric identification. DNNs outperform competing algorithms when it comes to the recognition of certain face features, including moles.

Using DNN extensively is a common practice in several research fields related to image recognition systems. Utilization in face detection, feature extraction, and segmentation are all components of face recognition.

3.3 Face Recognition Using AI

The introduction of deep learning-based AI for facial recognition was motivated by Project Gurukul [17][18]. A human face may be detected in a live video with the addition of the algorithm. A face recognition network in Python's Dlib is used to do this. You may think of Dlib as a software library that can do it everything. Images are processed using common Python Dlib methods like preprocess image (input path, output path, crop dim) for analysis 1. The system must invoke the appropriate function and provide the necessary parameters to perform the image analysis, which includes preprocessing, segmentation, and feature extraction. To commence, we have established a link list of KYC numbers and image numbers, as illustrated in Table 1. This is necessary in order to link each picture to its corresponding Know Your Customer data in the CRM system. Consequently, the system can track the associated KYC whenever a DNN identifies a person in a video feed. To train DNN, a total of 2 pictures were used, as shown in Table 2. Instead of a name, each picture is given a no for security reasons.

Table 1: Image link list table format.

No.	1	2	3
Images	01	02	03
KYC	2020_05_20_01	2018_07_10_04	2019_06_04_03

Table 2: Image classifications.

No.	1	2
Classification Images	KYC images	Non-KYC images
Count	80	20

Images from the KYC are used to train the proposed AI system. The ability to identify a registered user via camera is the primary benefit of integrating AI with Python Dlib's face recognition network. The user's KYC photos provided upon registration are utilized to train the AI system. The need for a person to verify the identity of a registered user is thus eliminated. The processing models provided by the AI-based method are superior and more efficient. Consistently better results and accuracy are driven by its capacity to learn unattended. Anomaly detection and impersonation alarms are also included in the suggested AI method.

3.4 Proposed Algorithm

Proposed Algorithm for Know Your Customer (KYC) Identity Verification using Artificial Intelligence-based Techniques:

User Registration and Authentication:

- Users visit the website and are presented with options to sign up or log in.
- New users provide personal details such as name, phone number, and create a username and password.
- Returning users log in using their credentials.
- Upon successful login, users access the home page and proceed to the KYC tab.

KYC Form Submission:

- Users enter their mobile number to receive an OTP for authentication.

- After OTP verification, users fill out a KYC form with personal information, including first and last name, contact number, and either Aadhaar card or PAN card number.
- Users upload scanned images of the identity documents and use a working webcam for live video recording to further verify their identity.
- The submitted information and documents are securely stored in the database.

Admin Oversight and Management:

- Admins log in to their designated account to access the admin homepage.
- Managers get privileges of working with tools and functionalities to monitor and control users' actions.
- The admin homepage displays all the users who have used the service, giving the possibility of typing searches as well as filtering the results with the help of time search boxes.
- Date-wise data analysis and some other additional features in the admin interface help to discover more detailed information about users' tendencies, actions, and activities.

AI-based Face Recognition:

- Programs like deep Face and Python Dlib's facial recognition network are used for detecting facial features and identification.
- It uses Haar-cascade for face recognition in live videos and card images while the Python Tesseract OCR for identity documents.
- Authentication involves comparing the details that the users have entered with the Aadhaar or PAN card.
- The AI system is updated with KYC images for the system's training in improving accuracy and the results it delivers, further enhancing features of impersonation and anomaly detection.

Performance Analysis:

- Performance of the AI models is evaluated employing metrics like precision, accuracy, and sensitivity.
- Comparative analysis is conducted between extracted images from identity documents and live video recordings, utilizing the VGG face model for face recognition tasks.
- The efficiency of the classifier is assessed using a confusion matrix, providing insights into the model's performance in KYC image recognition tasks.

In general, the suggested algorithm uses AI-related methods combined with easy-to-use interfaces and administrative options, providing an exhaustive and safe platform for KYC identity verification and meeting modern tendencies in customer identification and onboarding.

IV. RESULTS ANALYSIS AND DISCUSSION

The e-KYC authentication system work of task initiation entails making a form using HTML, with a CSS form for styling the appearance. The implementation uses the web application service provider called Fast2SMS for the sending of OTP to mobile phones belonging to the users. The text

from both Aadhaar and Pan cards are parsed by using Python Tesseract. The Haar Cascade algorithm is used to detect and localize image in videos. Besides, images are taken from Aadhaar and PAN cards which are further stored and used whenever required. The next step involves comparing the image extracted from Aadhaar or Pan card with the image from the recorded video. This comparison is performed with the help of the deep Face package. During installation followed by library importation, a pair of images retrieved from the video along with the Aadhaar card is as input. The comparison process uses a pre-design neural network architecture known as the VGG face model which is aimed at facial recognition tasks.

The e-KYC process can be divided into several phases, which allow users to undergo several stages of identification and service. Each of them emerges for the user while the respective output of each stage is shown in Fig. 5. Here it means the user is talking of a login page. A user usually needs to send his or her username and password at a login page or over a network connection. The result of this stage is to successfully log the user into the system, thus enabling them to proceed into the subsequent stages of e-KYC. The user is actually pointing to a signup page. For the new users, the first-time entry can be done on the signup page. This entails having the users input details such as name, phone number, username and password. The output is the creation of a new user 'John. 'After login or registration, the users are capable of viewing and altering the information they provided. The output enables the users to retrieve as well as update the information they require. Mobile OTP provides an extra layer of security for the system and allows its users to authenticate the system. The users are expected to enter the OTP generated and sent to the mobile number registered with them. Conclusively, entry and verification of the OTP mark the end of this security-enhancing stage.

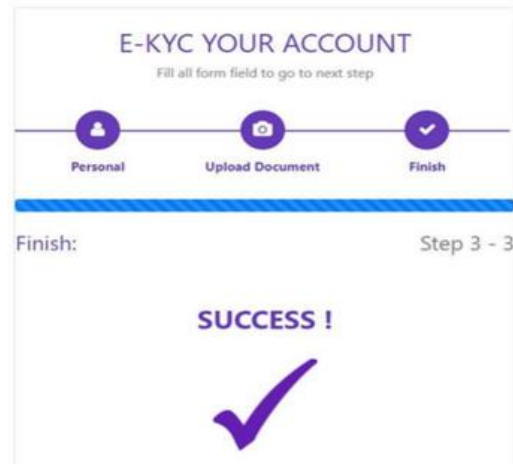


Figure 3: Whole process of e-KYC system

Fig. 3. Stage wise process output: (a) Login Page, (b) Signup Page, (c) User information, (d) User authentication through mobile OTP, (e) e-KYC Form personal information page, (f) document upload page, and (g) e-KYC Form final page.

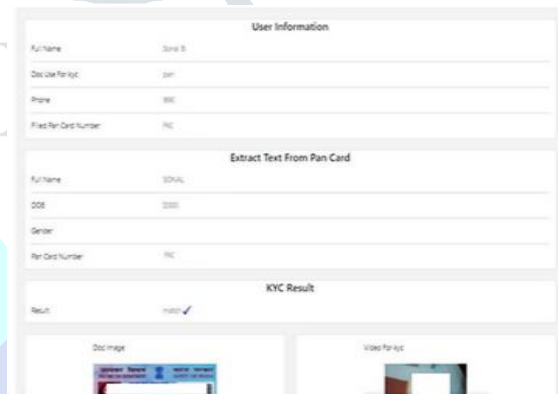
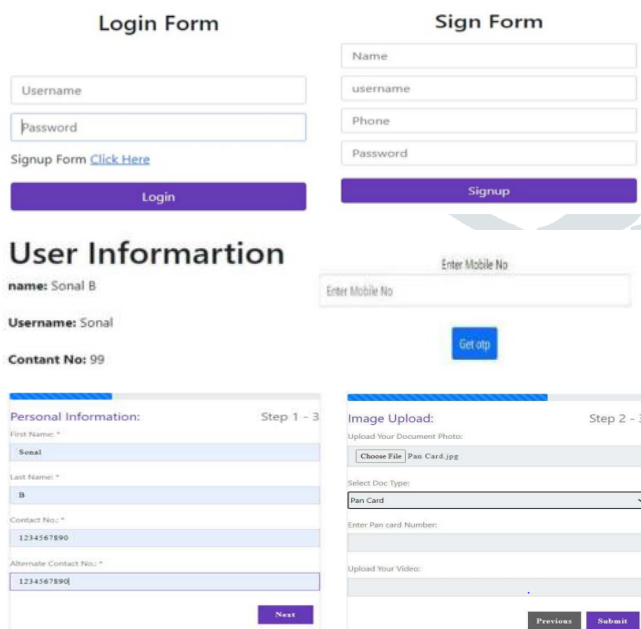


Fig. 4. Final validation stage response of e-KYC authentication system.



Information collected on the Personal Information page of e-KYC includes first name, last name, contact number, Aadhaar card or PAN card number on a special form filled by the users. We are providing this information for the purpose of confirmation and validation. Specifically on the document upload page, the users are expected to pass through the upload of scanned copies of the Aadhaar card or PAN card for identification. Finally, when the user goes through the preceding stages, they are navigated to the last page of the e-KYC form. Here, users may use a functioning webcam for live video recording to further verify their identity. After successfully recording and uploading the video and documents, users can finalize the process by clicking the "Submit" button. This marks the completion of the e-KYC process and a successful submission. The final validation stage response of e-KYC authentication system is depicted in Fig.4. User interactions and inputs are pivotal in the e-KYC process, contributing to information accumulation and verification steps, ensuring a comprehensive and secure procedure.

4.1 Analysis of Results of AI models

Equations (1), (3), and (equation. 2) may be used to determine the effectiveness of the categorization approach. Based on an element from a matrix called the confusion matrix or contingency table 3, these metrics are useful for assessing the effectiveness of supervised machine learning algorithms [32].

Table 3: Contingency Table of confusion matrix

		Predicted class	
		Positive	Negative
Actual class	Positive	True Positive (TP)	False Positive (FP)
	Negative	False Negative (FN)	True Negative (TN)

Accuracy: This is the proportion of reviews that have been accurately categorized to the total number of properly predicted images.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FN + FP} \dots (1)$$

Precision: A key indicator of accuracy is precision, which predicts the number of times the prediction is accurately connected to real KYC.

$$\text{Precision} = \frac{TP}{TP + FN} \dots (2)$$

Recall: The definition of this ratio is the proportion of properly categorized positive photos to all favorably classified images.

$$\text{Recall} = \frac{TP}{TP + FP} \dots (3)$$

Comparing the labels of the classes in this matrix, as seen in Table 3, is done from a classification perspective using terminology like "True Positive (TP)," "False Positive (FP)," "True Negative (TN)," and "False Negative (FN)." False Positive reviews are projected to be negative but are really classed as negative, whereas True Positive reviews are positive evaluations that the classifier incorrectly classified as positive. On the other hand, False Negative is a prediction of good reviews that were mistakenly categorized as negative, while True Negative illustrates negative reviews that the classifier identified as negative.

Figure 5's confusion matrix is utilized as an analytical tool to evaluate the experiment's results. This is employed to determine the classifier's efficiency.

		Matched No	Matched Yes	
Actual No		TN = 20	FP = 3	23
Actual Yes		FN = 5	TP = 72	77
		25	75	

KYC image recognition confusion matrix, shown in Figure 5.

"Matched" indicates that a picture has been recognized by the DNN's training algorithm, according to the confusion matrix. "Actual" refers to the KYCs that are known and are included in Table 4. The parameters for True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) are averaged in Figure 7. [19] The results are shown in Table 4, which reveals that the accuracy was 92% and the precision was 96%, with an FP rate of 13%.

Table 4: Classification results of model

Parameters (%)	AI Model
Accuracy	92
Precision	87
Sensitivity	94
Known KYC	80

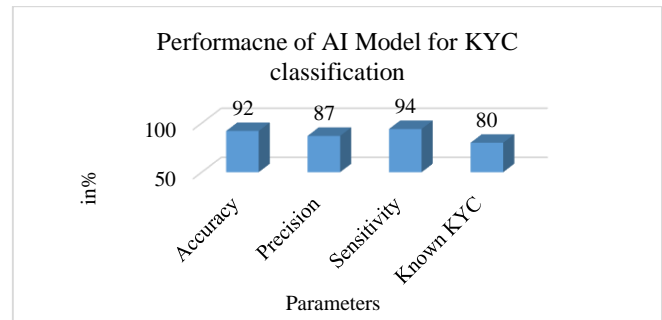


Figure 6: Parameter performance of AI-based model for KYC image recognition.

Figure 6 presents the performance metrics of an AI-based model designed for Know Your Customer (KYC) image recognition. The model demonstrates high accuracy at 92%, indicating that it correctly identifies KYC images in most cases. With a precision of 87%, the model has a relatively low false positive rate, meaning it is effective at correctly identifying relevant KYC images over irrelevant ones. The sensitivity, or recall, is 94%, showing the model's ability to correctly identify a high proportion of actual KYC images, minimizing false negatives. However, known KYC parameter stands at 80%, suggesting that while the model is generally reliable, there is room for improvement in recognizing all variations within the KYC dataset. Overall, these metrics highlight model's robust performance, particularly in accurately and sensitively recognizing KYC images, though enhancement in its comprehensive identification capabilities could further boost its effectiveness.

V. CONCLUSION AND FUTURE WORK

This study showcases a significant advancement in digital identity verification by integrating blockchain technology with AI-driven face recognition for an efficient and secure e-KYC authentication system. The methodology focuses on leveraging AI algorithms, particularly for face detection and verification, as well as OCR for text extraction from identification documents, to streamline the KYC process. The findings reveal enhanced security and privacy through blockchain, ensuring data is securely stored and accessible only with user consent. AI algorithms such as Haar-cascade and Deep Face significantly improve verification accuracy, achieving a 92% accuracy rate, 87% precision, and 94% sensitivity. The streamlined process enhances user experience by reducing verification time and effort, with OTP-based authentication adding an extra layer of security. The admin interface facilitates efficient user data management through targeted searches and date-wise filtering. Future work should focus on scalability, interoperability, minimizing AI biases, enhancing security measures, ensuring regulatory compliance, and conducting cost-benefit analyses to promote widespread adoption. Addressing these areas will enable the e-KYC system to offer a robust, efficient, and secure solution for digital identity verification. Additionally, continued efforts are required to refine AI models to minimize biases and errors in face recognition and text extraction, ensuring fair and accurate verification for all users.

VI. REFERENCES

[1] P. J. Burke and J. E. Stets, "Identity Verification," in *Identity Theory*, 2022.

[2] R. Fries, "Software Verification and Validation," *Reliab. Des. Med. Devices, Third Ed.*, pp. 401-410, 2012, doi: 10.1201/b12511-35.

[3] et al., "A SURVEY PAPER ON SMART AUTHENTICATION

- SYSTEM FOR IDENTITY VERIFICATION,” *Int. J. Eng. Appl. Sci. Technol.*, 2022, doi: 10.33564/ijeast.2022.v07i07.023.
- [4] A. Satybaldy, A. Subedi, and M. Nowostawski, “A Framework for Online Document Verification Using Self-Sovereign Identity Technology,” *Sensors*, 2022, doi: 10.3390/s22218408.
- [5] B. Amirgaliyev, G. Yegemberdiyeva, A. Kuchansky, Y. Andrashko, and I. Korol, “Automating the Customer Verification Process in a Car Sharing System Based on Machine Learning Methods,” *Eastern-European J. Enterp. Technol.*, vol. 4, no. 2–118, pp. 59–66, 2022, doi: 10.15587/1729-4061.2022.263571.
- [6] R. Reyes, B. Peralta, O. Nicolis, and L. Caro, “A Proposal for Deep Online Facial Verification using Selfies and Id document,” 2022, doi: 10.1109/ICA-ACCA56767.2022.10006244.
- [7] R. Waghchaure, D. Chavan, S. Shinde, R. Patil, and S. Singhania, “E-KYC Verification Portal Using ML,” vol. 10, no. 10, pp. 546–549, 2022.
- [8] P. Patil and M. Sangeetha, “Blockchain-based Decentralized KYC Verification Framework for Banks,” 2022, doi: 10.1016/j.procs.2022.12.055.
- [9] S. N V, “KYC Verification Using Blockchain,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 7, pp. 861–865, 2022, doi: 10.22214/ijraset.2022.45156.
- [10] R. Paper, “Blockchain-Based KYC Implementation : Enhancing Identity Verification and Compliance I Abstract : II Introduction,” 2013.
- [11] C. H. Choi, J. Kim, J. Hyun, Y. Kim, and B. Moon, “Face Detection Using Haar Cascade Classifiers Based on Vertical Component Calibration,” *Human-centric Comput. Inf. Sci.*, 2022, doi: 10.22967/HGIS.2022.12.011.
- [12] S. Mandava, J. S. Pereira, and S. Janagiraman, “Know Your Customer Verification using Blockchain and CPABE Algorithm,” *3rd Int. Conf. Innov. Mech. Ind. Appl. ICIMIA 2023 - Proc.*, no. Icimia, pp. 262–266, 2023, doi: 10.1109/ICIMIA60377.2023.10426480.
- [13] S. Kumar Garai, O. Paul, U. Dey, S. Ghoshal, N. Biswas, and S. Mondal, “A Novel Method for Image to Text Extraction Using Tesseract-OCR,” *Am. J. Electron. Commun.*, 2022, doi: 10.15864/ajec.3202.
- [14] M. Buyukyilmaz and A. O. Cibikdiken, “Voice Gender Recognition Using Deep Learning,” 2016, doi: 10.2991/msota-16.2016.90.
- [15] M. Akhtaruzzaman, M. K. Hasan, S. R. Kabir, S. N. H. S. Abdullah, M. J. Sadeq, and E. Hossain, “HSIC Bottleneck Based Distributed Deep Learning Model for Load Forecasting in Smart Grid with a Comprehensive Survey,” *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3040083.
- [16] S. Y. Siddiqui *et al.*, “IoT Cloud-Based Intelligent Prediction of Breast Cancer Stages Empowered with Deep Learning,” *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3123472.
- [17] N. I. Vivian and O. Anderson Ise, “Face Recognition Service Model for Student Identity Verification Using Deep Neural Network and Support Vector Machine (SVM),” *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 3307, pp. 11–20, 2020, doi: 10.32628/cseit2063225.
- [18] D. Estrada, L. Tawalbeh, and R. Vinaja, “How Secure Having IoT Devices in Our Homes?,” *J. Inf. Secur.*, 2020, doi: 10.4236/jis.2020.112005.
- [19] A. S. Sohal, R. Sandhu, S. K. Sood, and V. Chang, “A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments,” *Comput. Secur.*, 2018, doi: 10.1016/j.cose.2017.08.016.

