IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

KYC THROUGH FACE DETECTION

Abhijeet.S Chavan [1], Anoop.A Nanekar[2], KailashNath Tripathi[3]

[*1, *2] Student, Department of Artificial Intelligence and Machine Learning, ISBM College of Engineering, Pune, Maharashtra, India

[*3] Professor, Department of Artificial Intelligence and Machine Learning, ISBM College of Engineering, Pune, Maharashtra, India

ABSTRACT

Know your customer (KYC) is a set of guidelines used by banks to verify a customer's identification. In the current scenario, an e-KYC collects and stores an individual's information, as well as photocopies of valid government identity certificates, in a central database. We suggest a real-time Face KYC mechanism using authorization and authentication in this paper. Web-based platform for the banking sector that uses real-time KYC with face recognition is available. With photocopies of all legal official documents, such as Aadhar cards, passports, and so on, this technology recognize live faces.

Keywords: Face Detection, Authorization, Authentication, Facial Database, Biometric Verification.

I. INTRODUCTION

KYC (Know Your Customer) through face detection, authorization, and authentication is a modern and technology-driven approach to verifying the identity of individuals. It involves the use of facial recognition technology to establish and confirm a person's identity for various purposes, such as on boarding new customers, enhancing access control, and bolstering security measures. [1]

KYC is used to verify a customer's credentials and prove his or her identification. The process of electronically validating a customer's credentials, also known as paperless KYC, is known as e-KYC. You're probably curious about the KYC verification process on the internet right now. When opening an account and on a regular basis, KYC (Know Your Customer) is an essential process for identifying and validating a client's identification.

The know-your-customer (KYC) process that financial institutions (FIs) are obliged to follow whenever they establish a financial relationship with a new customer represents a significant financial burden for FIs but creates no productive added value. [3]

II. FACE RECOGNITION

Face recognition is the process of identifying or verifying a person's face from photos and videos. Face recognizers generally take face images from photos or videos. Cv2, NumPy, and face recognition libraries were used in this project. The face-recognition library contains the implementation of the various utilities that help with the process. The face recognition library provides a useful method called face locations (), which locates the coordinates of every face detected in the images. [2]

By detecting the face using libraries we can able to connect with the system in the various industries. It authorize and authenticate the image.

III. BACKGROUND TECHNOLOGIES

1. **Two Factor Authentication:**

   To enhance security, KYC systems often employ 2FA, combining facial recognition with another authentication factor, such as a password, PIN, or token. This dual-layer security approach adds an extra level of protection.

2. **Databases:**

   MySQL is an open-source relational database management system (RDBMS) that allows users to store, manage, and retrieve structured data. It's based on structured query language (SQL), the most common standardized language used to access databases.

3. **Flask:**

   Flask is a micro web framework written in Python. It is classified as a micro framework because it does not require particular tools or libraries. It has no database abstraction layer, form validation, or any other components where pre-existing third-party libraries provide common functions.

IV. CHARACTERISTICS

1. **Real-Time Verification:**

   It providing quick results and enabling immediate access to services or resources once the user's identity is confirmed.

2. **Data Security:**

   Protecting biometric data is paramount. Robust encryption and secure storage mechanisms are employed to safest facial recognition data against leakiness and unauthorized access.

3. **Database Integration:**

   KYC systems may integrate with databases and records to cross-verify an individual's identity, making it suitable for applications that require background checks.

4. Remote Authentication:

This method enables remote identity verification, which is particularly valuable in applications like online account creation, e-commerce, and remote access to secure systems.

5. Continuous Authentication:

Some implementations incorporate continuous authentication, periodically re-verifying a user's identity during an ongoing session to ensure that the same person remains present.

V. BLOCK DIAGRAM

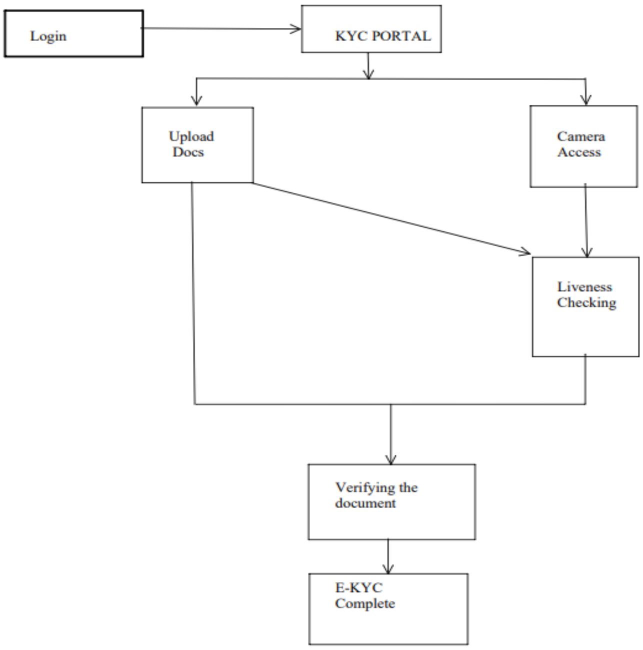

Fig.1 Block Diagram

In block diagram first block is a login block when user can login through its ID and password then user going to KYC portal. KYC portal has basically to section in section 1 is to upload documents in this user can upload documents like Aadhar card, pan card, passbook, driving license, passport, etc. in second section user has to give a camera access to the system upload a document then authenticate the document from the database and using live image it accessed camera and verify the document and finally the Face KYC will be complete and connect main account.

VII. CHALLENGES IN PROJECT

1. **Privacy Concern:**

   Collecting and storing biometric data, such as facial features, raises significant privacy concerns. Individuals worry about the potential misuse of their data and may be hesitant to provide consent for its use.

2. **Bias and Fairness:**

   Facial recognition systems have faced criticism for potential bias, as they may be less accurate for certain demographic groups. Addressing and mitigating bias in these systems is a significant challenge.

3. **Legal Liabilities:**

   Organizations implementing KYC through face detection may face legal liabilities in cases of data breaches or unauthorized use of biometric data. Legal precautions and liability management are essential.

4. **Public Perception:**

   The general public's perception of facial recognition is often negative due to concerns about privacy and surveillance. Managing public perception and building trust is a significant challenge.

5. **Cost:**

   Implementing and maintaining facial recognition systems, along with compliance measures, can be costly. Organizations need to allocate resources for technology, security, and compliance.

VII. FLOWCHART

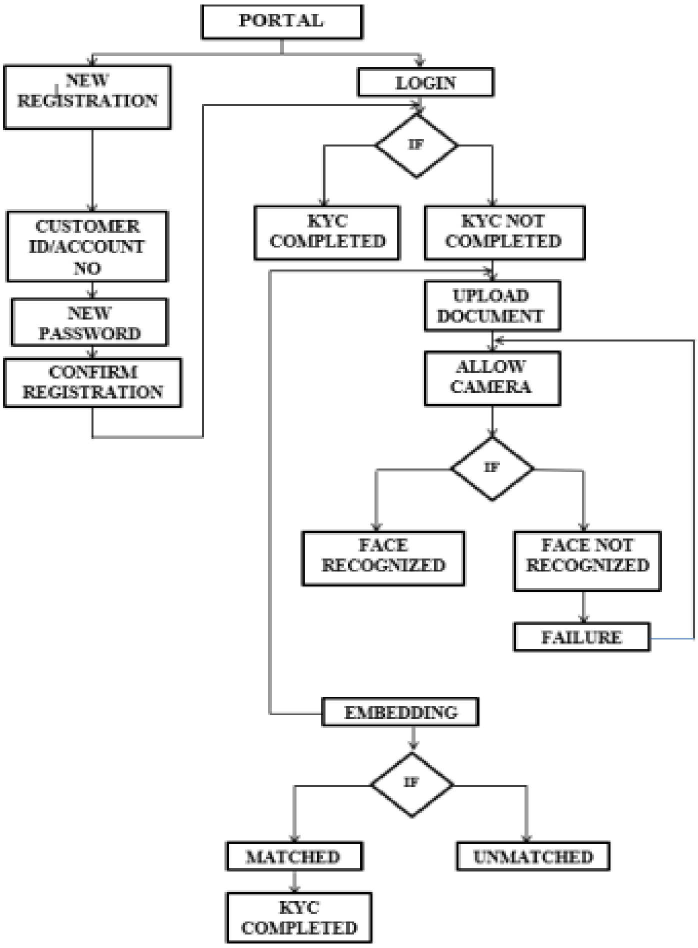

Figure 1 Architecture (Reference 1)

Once a customer visits the portal, there are two options. Under the New Registration process customer need to fill mandatory information about bank details. After set the password and once password get confirm then customer registration process is successfully done. Registered customers go through the login process to do KYC. The customer must upload a document (validate their ID) and grant access to the camera. If the customer's face is not properly recognized, the KYC process fails.

VIII. CONCLUSION

The paper tried to implement a platform for easy KYC document verification through a TensorFlow which check user's liveliness in few seconds. We make a web-based platform for the various sector that uses real-time KYC with face recognition using database of our documents. This technology recognize live faces in photocopies of all legal documents, when the KYC process is completed, the customer is redirected to the account page.

IX. SUMMERY

Know your customer (KYC) is a set of guidelines used by banks to verify a customer's identification. In the current scenario, an e-KYC collects and stores an individual's information, as well as photocopies of valid government identity certificates, in a central database. We suggest a real-time Face KYC mechanism using authorization and authentication in this paper. Web-based platform for the banking sector that uses real-time KYC with face recognition is available. With photocopies of all legal official documents, such as Aadhar cards, passports, and so on, this technology recognize live faces.

KYC (Know Your Customer) through face detection, authorization, and authentication is a modern and technology-driven approach to verifying the identity of individuals. It involves the use of facial recognition technology to establish and confirm a person's identity for various purposes, such as on boarding new customers, enhancing access control, and bolstering security measures. KYC is used to verify a customer's credentials and prove his or her identification. The process of electronically validating a customer's credentials, also known as paperless KYC, is known as e-KYC. You're probably curious about the KYC verification process on the internet right now. When opening an account and on a regular basis, KYC (Know Your Customer) is an essential process for identifying and validating a client's identification.

Face recognition is the process of identifying or verifying a person's face from photos and videos. Face recognizers generally take face images from photos or videos. Cv2, NumPy, and face recognition libraries were used in this project. The face-recognition library contains the implementation of the various utilities that help with the process. The face recognition library provides a useful method called face locations (), which locates the coordinates of every face detected in the images. By detecting the face using libraries we can able to connect with the system in the various industries. It authorize and authenticate the image. To enhance security, KYC systems often employ 2FA, combining facial recognition with another authentication factor, such as a password, PIN, or token. This dual-layer security approach adds an extra level of protection.

MySQL is an open-source relational database management system (RDBMS) that allows users to store, manage, and retrieve structured data. It's based on structured query language (SQL), the most common standardized language used to access databases. Flask is a micro web framework written in Python. It is classified as a micro framework because it does not require particular tools or libraries. It has no database abstraction layer, form validation, or any other components where pre-existing third-party libraries provide common functions.

It providing quick results and enabling immediate access to services or resources once the user's identity is confirmed. Protecting biometric data is paramount. Robust encryption and secure storage mechanisms are employed to safest facial recognition data against leakiness and unauthorized access. KYC systems may integrate with databases and records to cross-verify an individual's identity, making it suitable for applications that require background checks. This method enables remote identity verification, which is particularly valuable in applications like online account creation, e-commerce, and remote access to secure systems.

Some implementations incorporate continuous authentication, periodically re-verifying a user's identity during an ongoing session to ensure that the same person remains present. In block diagram first block is a login block when user can login through its ID and password then user going to KYC portal. KYC portal has basically to section in section 1 is to upload documents in this user can upload documents like Aadhar card, pan card, passbook, driving license, passport, etc. in second section user has to give a camera access to the system upload a document then authenticate the document from the database and using live image it accessed camera and verify the document and finally the Face KYC will be complete and connect main account.

Collecting and storing biometric data, such as facial features, raises significant privacy concerns. Individuals worry about the potential misuse of their data and may be hesitant to provide consent for its use. Facial recognition systems have faced criticism for potential bias, as they may be less accurate for certain demographic groups. Addressing and mitigating bias in these systems is a significant challenge. Organizations implementing KYC through face detection may face legal liabilities in cases of data breaches or unauthorized use of biometric data. Legal precautions and liability management are essential.

The general public's perception of facial recognition is often negative due to concerns about privacy and surveillance. Managing public perception and building trust is a significant challenge. Implementing and maintaining facial recognition systems, along with compliance measures, can be costly. Organizations need to allocate resources for technology, security, and compliance. Once a customer visits the portal, there are two options. Under the New Registration process customer need to fill mandatory information about bank details. After set the password and once password get confirm then customer registration process is successfully done. Registered customers go through the login process to do KYC. The customer must upload a document (validate their ID) and grant access to the camera. If the customer's face is not properly recognized, the KYC process fails.

The paper tried to implement a platform for easy KYC document verification through a TensorFlow which check user's liveliness in few seconds. We make a web-based platform for the various sector that uses real-time KYC with face recognition using database of our documents. This technology recognize live faces in photocopies of all legal documents, when the KYC process is completed, the customer is redirected to the account page.

X. REFERENCES

1. https://ijirt.org/master/publishedpaper/IJIRT153783_PAPER.pdf.

2. https://www.researchgate.net/publication/344390086_Secure_and_Transparent_KYC_for_Banking_System_Using_IPFS_and_Blockchain_Technology#:~:text=The%20proposed%20system%20allows%20a,it%20using%20the%20blockchain%20technique

3. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248913

4. https://figi.itu.int/wp-content/uploads/2021/05/e-KYC-innovations-use-cases-in-digital-financial-services.pdf

5. https://ieeexplore.ieee.org/document/9770032

6. https://www.researchgate.net/publication/333129124_Focus_Note_The_Use_of_eKYC_for_Customer_Identity_and_Verification_and_AML

7. https://www.google.com/search?q=ekyc+research+paper&oq=ekyc+research+paper&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIJCAEQABgNGIAEMgoIAhAAGAgYDRgeMg0IAxAAGIYDGIAEGIoFMg0IBBAAGIYDGIAEGIoFMg0IBRAAGIYDGIAEGIoFMg0IBhAAGIYDGIAEGIoF0gEJMTQ4NDhqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8#ip=1

8. https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/customer-cases/id-verification-digitalization

9. https://www.adb.org/sites/default/files/linked-documents/56037-001-tor.pdf

10. Al Mamun, Abdullah, Sheikh Riad Hasan, Md Salahuddin Bhuiyan, M. Shamim Kaiser, and Mohammad Abu Yousuf. "Secure and transparent KYC for banking system using IPFS and

blockchain technology." In 2020 IEEE region 10 symposium (TENSYMP), pp. 348-351. IEEE, 2020.

11. S. Chaubey, S. Bhalerao and N. Mangaonkar, "AutoKYC: Automation of Identity establishment and authentication in KYC process using Text extraction and face recognition," 2022 2nd Asian Conference on Innovation in Technology (ASIANCON), Ravet, India, 2022, pp. 1-6, doi: 10.1109/ASIANCON55314.2022.9909442.