Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 4, 2026

AUTOMATED CUSTOMER ACCOUNT OPENING USING AGENTIC AI

Dr. Noman Hasany[*1], Arshan Nasir[2], Dr. Khalid Rasheed[3]

[*1]*CCSIS, Institute of Business Management, Karachi*
[2]*Department of Computer Science, SZABIST University, Karachi*
[3]*Associate Professor, Denning Institute of Technology and Entrepreneurship*

[*1]noman.hasany@iobm.edu.pk, [2]mscs2473106@szabist.pk, [3]khalid.rasheed@denning.edu.pk

DOI: https://doi.org/10.5281/zenodo.19492388

Keywords
Chatbot, Digital Onboarding, QR Verification, Face Recognition, Biometric Authentication, Speech Recognition, NADRA API, Remote Account Opening, WebRTC, Tensor- Flow.js, FinTech

Article History
Received: 12 February 2026
Accepted: 22 March 2026
Published: 10 April 2026

Corresponding Author: *
Dr. Noman Hasany

Abstract
It takes a lot of paperwork and a physical visit to the branches to open a bank account. These documents are examined and validated by people after submission, which causes an excruciatingly drawn-out procedure. Digital banking has made an effort to provide answers over the years, but many businesses continue to rely on manual identity approvals and validation submission processes. Furthermore, these procedures lack robotic technology and intelligent automation, which restricts accessibility and ease. In order to automate every step of the process—from user interaction and identity verification to document authentication and account creation—this study presents an AI-based approach. The primary goal is to create a smart AI agent that enables consumers to safely open accounts without ever leaving their home. Uneducated or physically handicapped users can also benefit from a voice-based interface. Customers typically use traditional techniques for 180 minutes, but the suggested Chabot-based system cuts this time down to 30 minutes.

I. INTRODUCTION

Customers interactions with banks are changing as a result of the financial industry's digital revolution. The ability to open an account remotely using contemporary AI-powered onboarding technologies is one noteworthy development. Customers used to go to bank branches, fill out long forms, and personally turn in identity and address verification paperwork. The suggested solution incorporates an intelligent agent that provides real-time user data verification while helping users select their chosen language, submit personal information, and upload CNIC photos and photos. In order to provide a quick, inclusive, and AI-assisted banking experience, the system also provides a voice-based option for users who are unable to write.

II. LITERATURE REVIEW

Customer onboarding has altered dramatically as a result of the banking industry's digital transformation. In the past, opening an account needed in-person visits, paperwork, and manual verification, which made the process cumbersome and unavailable to people with physical disabilities or those living in remote locations. A shift toward automated onboarding systems that use biometrics and artificial intelligence for safe and effective account creation is seen in recent developments. Studies already conducted show that chatbots with

AI capabilities are becoming more and more common in banking. These chatbots improve client interaction, lighten the strain for employees, and offer round-the-clock assistance. But many still utilize strict menu-driven processes, which makes digital banking more complicated for people who are not accustomed with it [1]. Munira [2] contends that natural input should be permitted by chatbots in order to provide more seamless en- counters and expedite the gathering of information. A helpful technique for streamlining user options is gesture recognition. Research demonstrates that Media Pipe and Transtion [3]. G Hilario-Acuapan [4] also proved that gesture systems function dependably in a variety of camera and illumination scenarios. Because of its tamper-resistant design, identity verification via QR-based document checks has proven successful. Previous research demonstrates that cross-verification of QR-embedded personal information with government databases can minimize manual errors and delays. [5]. Verification is further strengthened by biometric authentication. Validation accuracy is greatly increased when biometric checks are combined with document data. But earlier systems frequently handled these phases separately, which led to inconsistencies and slower processing Othayoth and Khanna [6] examined FinTech AI applications, highlighting chatbots as a major force behind digital transformation. Similarly, Garg [7] offered a thorough analysis of the literature on AI in banking, emphasizing its application to fraud prevention and customer onboarding Patil et al. [8] and Nosrati et al. [9] examined the application of facial recognition technology to safe financial transactions. Their research supports the proposed system's facial recognition module by demonstrating that AI-based face matching increases accuracy and decreases human verification errors. Kumar [10] talked about cutting-edge approaches to financial security, such as facial recognition for walk-in clients. This highlights how crucial biometric verification is to contemporary banking systems. The integration of conversational AI, gesture recognition, document verification, and biometrics into a unified onboarding pipeline represents a research gap. By offering a single, automated procedure for creating accounts, this study fills that gap.

III. METHODOLOGY

Manual verification at physical branches is a major component of traditional bank account opening processes [1]. Mobile banking apps do exist, however they usually only offer a portion of digital onboarding [2] and do not incorporate multimodal chatbot interaction [3]. Facial recognition, biometric validation, and QR-based CNIC verification are rarely combined in a single automated workflow by current systems [4]. In order to close this gap and improve accessibility, this project suggests a chatbot-based solution that allows clients to open accounts remotely using both speaking and typing modes. The suggested system is built as a multi-stage pipeline for verification that is managed using a chatbot interface. The following modules make up the architecture:

*1) **User Interaction Layer:***

- Offers two modes: speech and typing.
- Responses are manually entered by the user in typing mode.
- Speech recognition translates spoken input into text when the chatbot is in speaking mode.

*2) **Data Collection Module:***

- Gathers information on the user, such as name, account type, address, CNIC, and father's name.
- keeps transient session data so that it can be compared to official records.

*3) **QR Verification Module:***

- The CNIC QR code is scanned with Instascan.js [11].
- The NADRA API is used to get data, which is then compared with information submitted by the user [12].
- If mismatch occurs, the process terminates with an error message.

4) Face Verification Module:

- Captures a selfie using the device camera.
- Compares the selfie with CNIC photo using FaceAPI.js [13].
- Employs TensorFlow.js for enhanced

image matching accuracy [14].

5) Biometric Verification Module:

- Captures fingerprint data through biometric sensors.
- Validates against NADRA records using secure API calls [15].
- Failure results in termination of the process

6) KYC Submission Module:

- Prompts the user to upload a PDF form.
- Stores the document for backend verification. [16]

7) Account Activation Module:

- Upon successful completion of all verification steps, the chatbot generates an account number.
- User is informed that activation will occur within 24 hours after backend validation. [17]

A. Tools and Libraries

- **Instascan.js** – QR code scanning [11].
- **FaceAPI.js** – facial recognition and comparison [12].
- **WebRTC** – real-time camera and microphone access [18].
- **TensorFlow.js** – advanced biometric and image matching [14].
- **Dialogflow / Rasa** – natural language understanding for chatbot [19].
- **Speech Recognition API** – speech to text conversion in speaking mode.

B. Validation Process

- **Data Matching** – User input compared with NADRA QR data.
- **Image Correspondence** – Selfie and CNIC photo comparison.
- **Matching Biometrics** – NADRA records and fingerprints were compared.
- **Handling Errors** – The process is stopped and error messages are displayed if there is a mismatch [20].

C. Ethical and Security Considerations

- **Every crucial piece of information** – sent over encrypted channels. [21]
- **No CNIC or biometric information** – saved locally; only the NADRA API is used for verification [22].
- **Privacy of users** – preserved by restricting data retention to storage that is session-based [23].

D. Comparative Analysis

Category	Chosen Library	Alternatives	Reason for Choice
QR Code Scanning	Instascan.js: - Lightweight - Real-time webcam scanning - Smooth NADRA API integration	ZXing: - Complex setup - Browser latency - Inconsistent results	Faster & reliable for pure web usage
Facial Recognition	FaceAPI.js: - Built on TF.js - Easy webcam use - Good accuracy	OpenCV.js: - Complex config - Lower accuracy - Slower processing	Best balance of accuracy & browser support
Speech Recognition	Speech Recognition API: - Native support - Reliable speech-to-text	CMU Sphinx: - Server required - Poor multilingual accuracy	Lightweight & sufficient for chatbot input
Biometric Verification	NADRA API: - Official fingerprint validation - Govt compliant	Local SDKs: - No NADRA link - Not valid for banking	Mandatory for regulated verification

Fig. 1. Comparison Table

IV. System Design

The suggested chatbot system combines several verification modules into a single automated workflow through its web-based application

design. The Front End Interface, Application Logic Layer, and Backend Integration Layer comprise the three layers of the system architecture.

A. Front End Interface

- **Languages Employed** – The user interface was designed using HTML, CSS, and JavaScript.
- **Adaptive Design** – To guarantee device compatibility, CSS frameworks like Bootstrap were used.
- **User Communication** – Allows for data entry in both speech and typing modes.
- **Access to a camera and microphone** – Built utilizing the WebRTC API to allow voice input and the taking of selfies.

B. Application Logic Layer

- **Engine for Chatbots** – created in JavaScript with Di- alogflow's assistance for natural language comprehen- sion.
- **QR Code Validation** – Instascan.js was used to implement real-time CNIC QR code scanning.
- **Recognition of faces** – FaceAPI.js is integrated, and TensorFlow.js is used to improve the accuracy of image comparison.
- **Speech Recognition** – Utilized the Web Speech API for converting spoken input into text.
- **Biometric Verification** – Fingerprint data captured through compatible biometric devices and processed via secure API calls.
- **Error Handling** – Each module includes validation checks; mismatches halt the process with error messages.

C. Backend Integration Layer

- **Server Framework** – Node.js with Express.js was used to handle API requests and manage communication between modules.
- **Database** – MongoDB was employed to store temporary session data, KYC forms, and logs of verification attempts.
- **NADRA API Integration** – Secure RESTful API calls were made to NADRA servers for QR, biometric, and identity verification.
- **Security** – All communication channels were encrypted using HTTPS/TLS to protect sensitive data.

D. Workflow Description

- User selects interaction mode (typing or speaking).
- Personal details are collected and stored.
- CNIC QR code is scanned and verified against NADRA records.
- Selfie is captured and matched with CNIC photo.
- Biometric fingerprint verification is performed.
- KYC form is uploaded and stored.
- Account number is generated, and user is notified of activation within 24 hours after document verification.

E. Flowchart Diagram

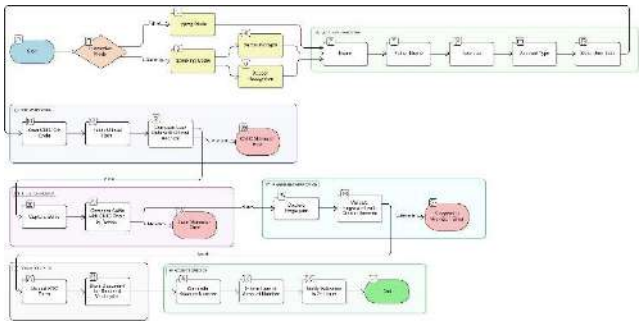

Fig. 2. Agentic AI Flowchart Diagram

The suggested Chabot system's general workflow is depicted in Fig. 2. The flow chart shows the processes that must be followed in order: mode selection (speaking or typing), gathering of personal information, CNIC QR verification, facial recognition, biometric validation, KYC

submission, and account activation. Fault management is a part of each verification phase; if a discrepancy occurs, the technique is finished.

F. Use Case Diagram

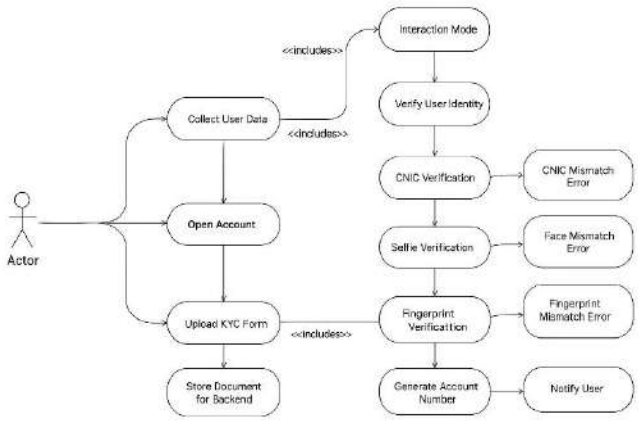

Fig. 3. Use Case Diagram for Agentic AI

The use case illustration in Fig. 3 demonstrates in what way the key actor (user) interrelates with other structures like the bank server and the NADRA API. The user contributes in numerous use cases, such as entering individual information, captivating an image, skimming the CNIC QR code, finishing biometric confirmation, submitting the KYC procedure, and receiving the account number. The practical needs of the Chabot structure are decorated in this figure.

G. Comparison Graph

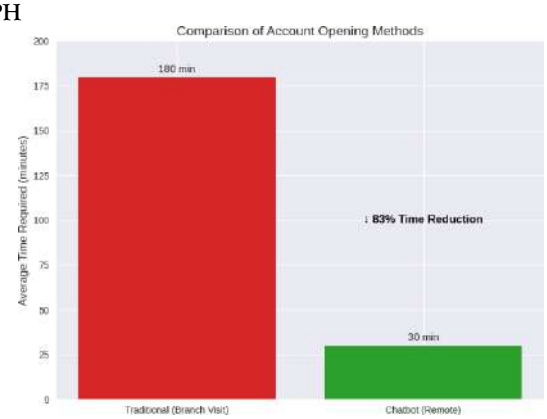

Fig. 4. Relating Outdated and Chatbot Account Opening in a Bar Diagram

Fig. 4 displays a assessment among Chabot-based remote account opening and old-fashioned branch visits. The bar diagram explains how fewer time is necessary when applying the chatbot structure.

- **Outdated Theoretical Branch Visit** – Counting travel, waiting, and papers, consumers expend a usual of 180 minutes (3 hours).
- **A inaccessible chatbot** – Cheers to automatic QR, facial, and biometric confirmation, the similar process just takings 30 minutes at home.
- **Effects** – This results in an 83% reduction in time, making opening an account quicker, easier, and more accessible.

The average daily visitor difference between chatbot-based remote account opening and regular branch visits is depicted in the line graph.

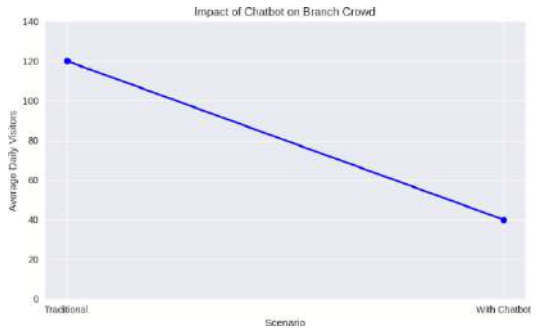

Fig. 5. Line Chart Comparison of Branch Visitors

- **Hypothetical Traditional (Branch Visit)** – Average daily visitors ≈ 120.
- **With Chatbot** – Average daily visitors ≈ 40.
- **Impact** – This shows a ~67% reduction in branch crowd, meaning fewer queues, less waiting time, and more convenience for customers.

V. RESULTS

Experimental results demonstrate successful account creation in both typing and speaking modes. The chat bot reduces on boarding time by approximately $(180-30)/180 \times 100 \approx 83\%$

The mode selection interface allows the user to choose between typing or speaking to interact with the chatbot system. In Type Mode, the user enters details manually, while in Speak Mode, the chatbot listens and transcribes spoken input.

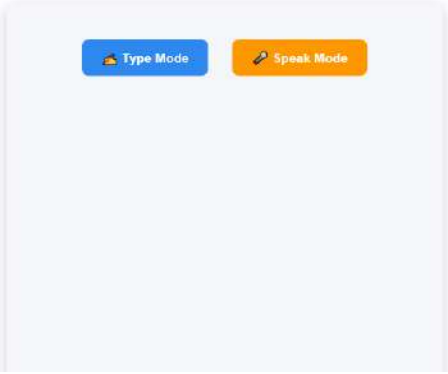

Fig. 6. Figure 3: Mode Selection "Type" Or "Speak"

Fig. 7. Type Mode - Welcome and Name

Fig. 8. Type Mode - Father Name

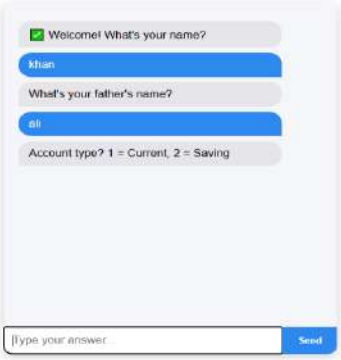

Fig. 9. Type Mode - Account Type Selection

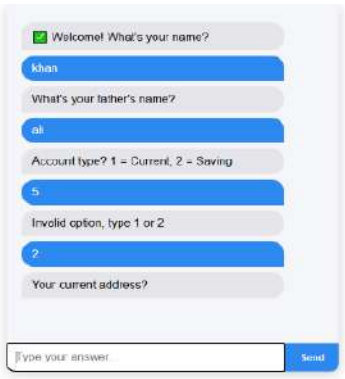

Fig. 10. Type Mode - Enter Address

Fig. 11. Type Mode - Camera Open For QR Scan

Fig. 12. Type Mode - CNIC Data Verify Screen

Fig. 13. Type Mode - Camera Open For Take Selfie

Fig. 14. Biometric Verification in Type Mode

Fig. 15. Type Mode - Upload KYC Form

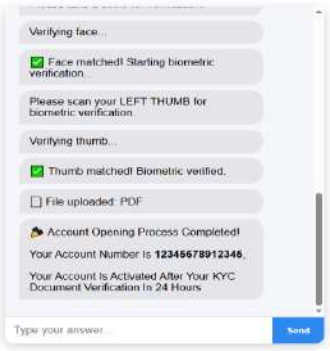

Fig. 16. Type Mode - Process Completed Screen

Fig. 17. Speak Mode - User Will Speak and Give the Answer

Fig. 18. Speak Mode - Chatbot Listen and Write the Answer

VI. CONCLUSION

This paper presented a Chabot-based system for creating accounts that incorporates several steps of verification, such as biometric authentication, facial recognition, CNIC QR scanning, and KYC filing. Because the system can function in both speaking and typing modes, it is more accessible to a wider range of users. The suggested approach minimizes processing time, increases client convenience, and eliminates the need for in-person branch visits by automating the verification process via NADRA API integration and lightweight web technologies. A comparative analysis of libraries showed that browser-based solutions, such Instascan.js and FaceAPI.js, were more accurate and efficient than heavier

equivalents. Overall, by providing a safe, scalable, and user-friendly method of opening accounts remotely, the system aids in the digital transition of banking.

VII. Future Work

Even if the suggested chatbot system met its goals, there are a few improvements that should be investigated in subsequent studies:

- **Innovative Security Contrivances** – Using dispersed record or blockchain expertise to assurance identity confirmation that cannot be changed.
- **Gesture-Based Communique´** – n gesture acknowledgement—such as hand signs or facial expressions—will allow users to connect through the Chabot in an extra available and usual way, particularly for those who have trouble talking or typing.
- **Multilingual Support** – Increasing chatbot answers and language recognition to several local languages, permit- ting for better inclusivity.
- **Deployment of Mobile Applications** – Making native iOS and Android apps to increase usability and interest.
- **AI-Powered Scam Identification** – Knocking machine learning models into preparation to spot questionable behaviors throughout onboarding.
- **Testing for Scalability** – Measuring system performance in the face of weighty contemporaneous user loads to guarantee reliability.
- **Improvements to User Familiarity** – To improve suability, flexible interfaces and customized guidance are being presented.
- **Financial Network Integration** – To surge functionality, connect the chatbot to e-wallets, payment gateways, and extra banking facilities.

Acknowledgment

I want to express my gratitude to the instructor for all of their support and guidance throughout this research. Their insightful advice, constructive criticism, and steadfast support were essential to the accomplishment of this study. I genuinely appreciate the time and effort they invest in assessing my work and offering insightful suggestions. It has been an honor to learn under their direction, and I am immensely grateful for the opportunity to benefit from their expertise.

References

[1] W. H. Chou, Y. Wu, and L. Zhang, "A study on chatbot adoption in leading banks," *Issues in Information Systems (IACIS)*, vol. 26, no. 1,
pp. 446–457, 2025. [Online]. Available: iacis.org

[2] M. S. K. Munira, "A systematic review of AI-driven strategies in banking," *Asian Journal of Applied Technology and Engineering Sciences (AJATES)*, vol. 12, no. 2, pp. 55–68, 2025. [Online]. Available: abacademies.org

[3] H. H. Li and C. Hsieh, "Dynamic hand gesture recognition using MediaPipe and Transformer," *Engineering Proceedings (MDPI)*, vol. 108, no. 1, pp. 22–29, 2025. [Online]. Available: mdpi.com

[4] M. Gil-Mart´ın, J. D´ıaz, and R. Rodr´ıguez, "Hand gesture recognition using MediaPipe landmarks," in *Proc. 17th Int. Conf. on Computer Vision Theory and Applications (SCITEPRESS)*, pp. 312–320, 2025. [Online]. Available: scitepress.org

[5] S. S. Sambare, A. Patil, and R. Kulkarni, "Document verification system and validation against QR codes," in *Proc. Int. Conf. on Computing, Communication, Control and Automation (ICCUBEA)*, IEEE, pp. 1–6, 2023. [Online]. Available: ieeexplore.ieee.org

[6] P. Othayoth and S. Khanna, "Implementation of artificial intelligence and chatbot for the enhancement of new age banking systems: A systematic review," in *Generative AI in FinTech: Revolutionizing Finance Through Intelligent Algorithms*, Springer, pp. 1–19, Mar. 2025. [Online]. Available: springer.com

[7] N. Garg, "A systematic literature review on artificial intelligence technology in banking," *Academy of Banking Studies Journal*, vol. 24, no. 3, pp. 45–60, 2025. [Online]. Available: abacademies.org

[8] H. Patil, D. Agrawal, and S. Solanki, "Advancing banking system using face recognition," *International Journal of Scientific Research in Engineering and Technology (IJSRET)*, vol. 11, no. 6, pp. 106–112, 2025. [Online]. Available: ijsret.com

[9] L. Nosrati, A. M. Bidgoli, and H. H. Seyyed Javadi, "Identifying people's faces in smart banking systems using artificial neural networks," *Int. J. of Computational Intelligence Systems*, vol. 17, no. 9, pp. 1–12, Jan. 2024. [Online]. Available: atlantis-press.com

[10] V. R. R. Kumar, "Innovative solutions for financial security: Implementing facial recognition to identify walk-in customers in banking centers," *International Journal of Computer Engineering and Technology (IJCET)*, vol. 16, no. 1, pp. 1594–1608, 2025. [Online]. Available: iaeme.com

[11] S. Schmich, "Instascan.js: Real-time webcam QR code scanner library," GitHub, 2017. [Online]. Available: github.com

[12] National Database & Registration Authority (NADRA), "NADRA official services and APIs," Government of Pakistan, 2025. [Online]. Available: nadra.gov.pk

[13] V. Justadude, "FaceAPI.js: JavaScript API for face recognition in the browser," GitHub, 2018. [Online]. Available: github.com

[14] Google, "TensorFlow.js: Machine learning for JavaScript developers," TensorFlow, 2025. [Online]. Available: tensorflow.org

[15] National Database & Registration Authority (NADRA), "Biometric verification services," Government of Pakistan, 2025. [Online]. Available: nadra.gov.pk

[16] State Bank of Pakistan, "Anti-Money Laundering and KYC Guidelines, "SBP, 2025. [Online]. Available: sbp.org.pk

[17] State Bank of Pakistan, "Customer onboarding and account activation framework," SBP, 2025. [Online]. Available: sbp.org.pk

[18] WebRTC Project, "WebRTC: Real-time communication for the web," Google, 2025. [Online]. Available: webrtc.org

[19] Google Cloud, "Dialog flow: Natural language understanding for conversational interfaces," Google, 2025. [Online]. Available: cloud.google.com

[20] Rasa Technologies, "Rasa: Open-source conversational AI framework, "Rasa, 2025. [Online]. Available: rasa.com

[21] National Institute of Standards and Technology (NIST), "Block cipher techniques and encryption standards," NIST, 2025. [Online]. Available: csrc.nist.gov

[22] IEEE, "Privacy in biometric systems: Challenges and solutions," IEEE Xplore, 2020. [Online]. Available: ieeexplore.ieee.org

[23] OWASP Foundation, "Session management cheat sheet," OWASP, 2025. [Online]. Available: owasp.org