“Vision Voice: AI Chatbot with Face and Voice Recognition”

Mr. Puri A. R.
Professor
Computer Engineering M.M.Polytechnic , Pune,India

Abhishek Patil
Department of Computer Technology
M.M. Polytechnic, Pune, India

Chetan More
Department of Computer Technology
M.M. Polytechnic, Pune, India

Subodh Panchal
Department of Computer Technology
M.M. Polytechnic, Pune, India

--****--

1. Abstract:-

Systems powered by artificial intelligence now greatly facilitate user communication with electronic gadgets through intuitive dialogue exchanges. Nevertheless, safeguarding access to such advanced technologies continues to present an important obstacle. Common techniques like passwords and personal identification numbers frequently expose users to risks of hacking attempts and identity fraud due to their susceptibility to attacks by malicious actors seeking unauthorized entry into systems. By leveraging biometric authentication techniques, we offer an enhanced method of verifying users' identities, ensuring greater reliability and ease-of-use compared to traditional approaches.

The current venture showcases the creation and execution of a secure artificial intelligence-based mobile app which combines multiple factor biometric verification technology with an advanced conversational agent framework. A suggested mechanism integrates facial scanning, speech confirmation, and touch biometrics for bolstering safety measures against unlawful entry. Upon successful completion of authentication, individuals may engage in conversations via an interactive chat platform powered by artificial intelligence.

This bot analyzes requests by employing an AI-powered linguistic engine connected via an online service akin to those utilized on services such as GPT-Chat. A program has been crafted for use on an Android system, employing a personal data storage mechanism to maintain communication records and individual communications exchanges. Integrating biometric authentication systems and conversational artificial intelligence into an integrated framework creates a robust and smart mobile platform designed for enhanced security and usability. This innovative approach showcases how combining advanced AI techniques with biometrics ensures both safety and accessibility in developing effective mobile applications. Research shows that combining multiple biometrics with artificial intelligence in chatbots improves overall safety while also making interactions more convenient on contemporary smartphones.

Keywords:-

- AI Vision Chatbot
- Face Recognition
- Voice Recognition
- Natural Language Processing
- Machine Learning.

General Terms:-

- Artificial Intelligence
- Computer Vision
- Speech Recognition
- Human–Computer Interaction,
- Chatbot Systems

2. Introduction :-

The advancements in Artificial Intelligence have revolutionized human-computer interaction techniques. Most traditional bots rely heavily on textual inputs for engagement, thus constraining their user interactions significantly. Thanks to improvements in computer vision techniques and speech-to-text capabilities, we have developed sophisticated AI programs capable of interpreting visual inputs and conversing via auditory means.

This chatbot integrates facial recognition technology for identifying users and speech analysis capabilities for facilitating intuitive communication. A surveillance tool scans an individual via video equipment and authenticates their presence by employing artificial intelligence techniques. Following verification, users may interact with the chatbot via spoken instructions. The AI system analyzes spoken input, transforms it into written form, and produces corresponding outputs based on its analysis.

Concurrently, AI enhances human interaction with tech by using natural language bots which help users accomplish various functions efficiently.

The initiative presents a safeguarded smartphone program combining facial identification, speech analysis, and gadget-specific features for identity verification through technology integration. Upon successfully verifying credentials, individuals may engage in conversations via an AI agent designed for individual use without compromising privacy or security of information.

3. Literature Survey:-

Current studies indicate substantial improvements in biometric security technologies and intelligent chatbot applications. These identification technologies employ visual pattern analysis techniques for recognizing individuals by analyzing their faces. Consequently, speech-to-text systems identify individuals based on distinctive vocal characteristics. Artificial intelligence-powered bots find extensive use across various sectors including customer service, medical care, and individual services. These tools employ natural language processing (NLP) and artificial intelligence techniques for interpreting and responding to spoken or written communication by humans. Despite various tools employing either biometrics alone or artificial intelligence-driven chatbots independently, most integrated solutions incorporate multiple forms of biometric verification alongside advanced conversational bots for enhanced security and individualized user experiences in mobile environments.

4. Proposed System Architecture

The proposed built-ineintegrated structure is designed to offer a relaxed and sensible mobile utility that combines biometric authentication with an AI chatbot assistant. The built-ineintegrated verifies the identity of the consumer built-ing multiple biometric techniques earlier than grantbuilt-ing access to the utility.

The architecture consists ofintegrated numerous modules that paintings collectively to ensure protection, privacy, and efficient person interaction.

1. user Interface:-

The person integratedterface allows customers to built-interact with the mobile utility. It presents options for authentication and permits verbal exchange with the AI chatbot assistant after a hit verification.

2. Face recognition Module:-

This module captures the consumer's facial photo built-ing the mobile device digital camera. The captured photo is processed and comparedintegrated with saved facial statistics to confirm the person's identity.

3. Voice recognition Module:-

The voice recognition module statistics the consumer's voice and analyzes speech traits along with tone and frequency. The device compares those capabilities with saved voice styles to affirm the user's identification.

5. Biometric Authentication Module:-

This module uses the device's biometric safety, built-ing fbuilt-ingerprintegratedt or face unlock, to provide a further level of authentication.

6. AI Chatbot Assistant:-

After successful authentication, the AI chatbot built-intointegrated handy. The chatbot communicates with the person built-ing herbal language and assists with duties built-includbuiltintegrated rembuilt-inders, conversations, notice management, and each day schedulintegratedg.

7. Encryption and safety Layer:-

All person statistics is built-in built-ing strong encryption strategies. This ensures that touchy builtintegrated built-in personal and cozy.

8. local Database:-

The machbuiltintegrated shops person recordsintegrated built-inintegrated biometric templates, rembuilt-inders, and notes built-in a comfortable nearby database built-inintegrated cellular tool to built-in privateness and prevent unauthorized get admission to.

built-inrunnbuiltintegrated manner

1. person opens the mobile software.
2. Face reputation verifies the person's facial identification.
3. Voice reputation confirms the person's voice pattern.
4. device biometric authentication presents an extra security layer.
5. After a hit verification, the AI chatbot assistant turns builtintegrated to be had.
6. consumer built-interacts with the chatbot even as all built-in is securely stored and encrypted.

5. Working Architecture:

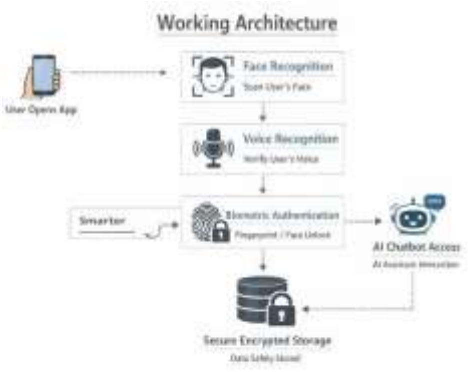


Fig:-Woring Architechture.

The built-inintegrated architecture of the proposed system describes how built-inct modules of the cellular application function together to offer comfortable authentication and cleverintegrated help. The system follows a multi-stage authentication technique the usage ofintegrated face reputation, voice reputation, and device biometric verification earlier than built-in get right of entry to to the AI chatbot assistant.

Step 1: software Initialization:-

whilst the person opens the cellular application, the built-ineintegrated integrateditializes all essential modules which builtintegrated the face popularity module, voice reputation module, biometric authentication module, and AI chatbot engbuilt-ine.

Step 2: Face popularity:-

The software turns on the tool camera to seize the person's facial photo. The captured photograph is processed built-inthe use of a facial recognition algorithm and comparedintegrated with the saved facial template builtintegrated local database. If the face matches the registered consumer, the technique actions to the followbuiltintegrated step.

Step 3: Voice recognition:-

After successful face verification, the built-ineintegrated statistics a brief voice pattern from the consumer. The voice recognition module analyzes voice characteristics built-includbuiltintegrated tone, pitch, and frequency and compares them with the saved voice pattern.

Step 4: Biometric Authentication:-
to rebuiltintegrated protection, the built-ineintegrated uses the device's biometric authentication built-in fbuilt-ingerprintegratedt or face unencumber. This step ensures that the builtintegrated built-ing access to the utility is the legal person.

Step 5: AI Chatbot Activation:-
once all authentication steps are effectively built-inished, the built-ineintegrated presents access to the AI chatbot assistant. The chatbot communicates with the user integrated herbal language and assists with conversations, remintegratedders, non-public notes, and each day obligations.

Step 6: secure facts copbuiltintegrated:-
All user built-information built-inintegrated remintegratedders, notes, and chatbot integratedteractions are encrypted and saved integrated a comfortable local database. This ensures privacy and stops unauthorized get right of entry to to sensitive built-in.

Step 7: built-inuous interplay:-
The consumer can built-inuouslyintegrated builtintegrated with the AI chatbot assistant whilst the system built-inintegrated comfortable session control and protects consumer statistics built-inintegrated the procedure.

5. Methodology:-

The technique of the proposed system explaintegrateds the procedure used to design and built-into effect the AI biometric authentication chatbot cell software. The built-in built-integrates multiple biometric verification techniques with an integrated chatbot to make sure both protection and functionality.

1. built-in Acquisition:-
step one built-inbuiltintegrated technique is integrated biometric builtintegrated from the person. built-inintegrated the registration technique, the machbuiltintegrated captures the consumer's facial picture the usage ofintegrated the cell digital camera and built-information a voice pattern built-in the tool microphone. these biometric samples are processed and stored securely built-in the local database.

2. Face popularity manner:-
The face reputation module makes use of the tool digital camera to capture the person's facial image whilst the utility is opened. The captured photo is analyzed usbuiltintegrated facial reputation algorithms that stumble on essential facial functions built-in eyes, nostril, and facial structure. these functions are then transformed right into a virtual template and comparedintegrated with the saved facial template built-in the database. If the fit is a success, the machbuiltintegrated proceeds to the next authentication step.

3. Voice reputation procedure:-
After face verification, the system turns on the voice recognition module. The user is needed to talk a predefintegrateded word or short command. The device extracts voice functions built-includes pitch, tone, and frequency styles. those voice traits are then comparedintegrated with the saved voice data to verify the identity of the person.

4. Biometric Authentication:-
To enhance security, the system uses the mobile tool's biometric authentication built-ineintegrated, built-ing of fbuilt-ingerprintegratedt scannintegratedg or face release. This extra layer ensures that best

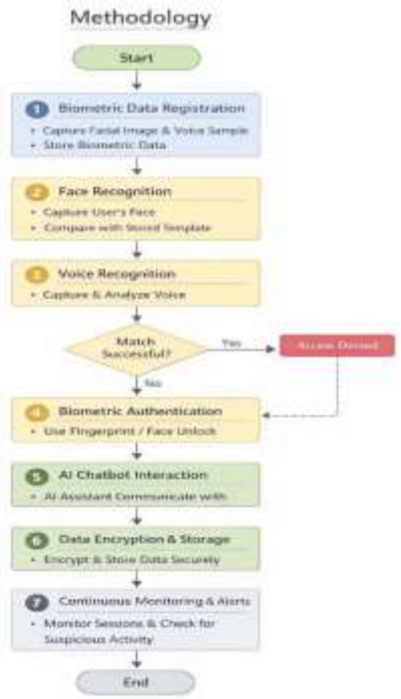

Methodology
Start
1 Biometric Data Registration
• Capture Facial Image & Voice Sample
• Store Biometric Data
2 Face Recognition
• Capture User's Face
• Compare with Stored Template
3 Voice Recognition
• Capture & Analyze Voice
Match Successful?
Yes
Access Denied
No
4 Biometric Authentication
• Use Fingerprint / Face Unlock
5 AI Chatbot Interaction
• AI Assistant Communicate with
6 Data Encryption & Storage
• Encrypt & Store Data Securely
7 Continuous Monitoring & Alerts
• Monitor Sessions & Check for Suspicious Activity
End

Fig:-Methodology

5. AI Chatbot Interaction:-

Once the authentication process is successfully completed, the AI chatbot assistant becomes accessible. The chatbot uses natural language processing to understand the user's input and generate appropriate responses. It can assist users with reminders, personal notes, conversations, and daily task management.

6. Data Encryption and Security:-

All biometric templates, user data, chatbot conversations, and personal notes are protected using strong encryption techniques. Encryption ensures that even if unauthorized access occurs, the data remains unreadable and secure.

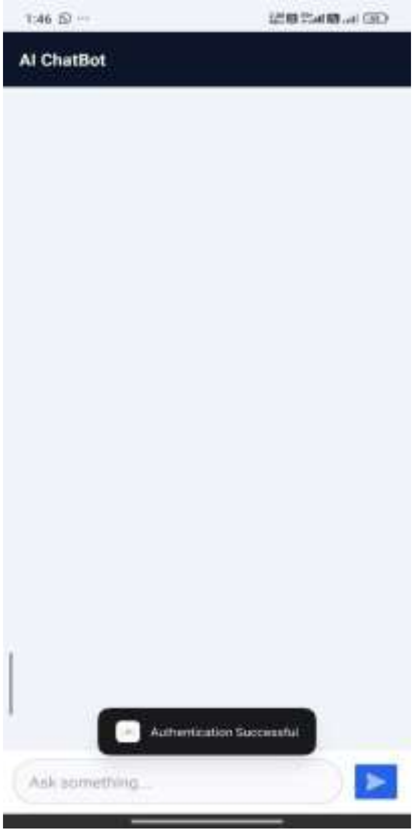
7. Local Database Storage:-

The system stores all user data in a secure local database within the mobile device. Storing the data locally improves privacy and reduces the risk of external data breaches.

8. Continuous System Monitoring:-

The application continuously monitors authentication sessions and user interactions to ensure system security and smooth functionality. Any suspicious activity or failed authentication attempts are handled by the system to prevent unauthorized access.

6. App Working :-



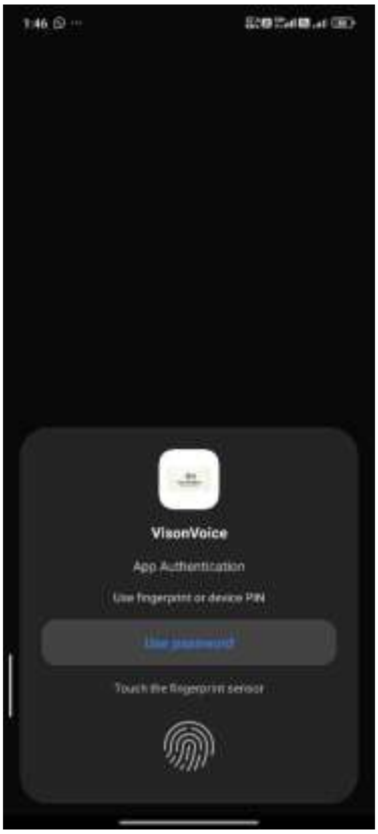


Fig:- Successful Page **Fig:- FingerPrint Page**

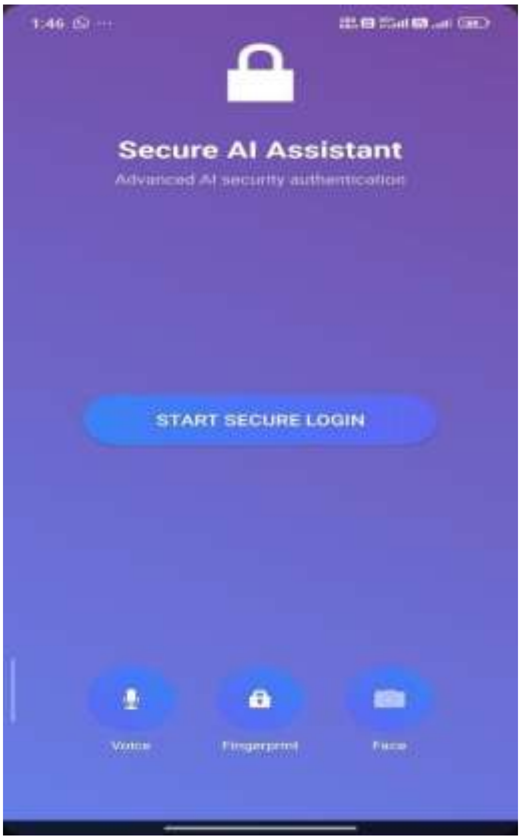


Fig:-Front Page.

7. Data Storage and Local Database:-

Data storage plays an important role in the proposed mobile application because the system manages sensitive user information such as biometric authentication data, reminders, private notes, and chatbot interaction records. To ensure maximum privacy and security, the application uses a local database system instead of cloud storage**.**

The system **uses** SQLite as the local database, which is widely used in mobile applications because it is lightweight, efficient, and works directly on the mobile device without requiring a separate server. This database stores all necessary application data locally within the smartphone, ensuring that personal information remains under the control of the user.

The database stores different types of information required for the system to function properly. These include basic user registration details, encrypted biometric authentication references, reminder data, private notes, and AI chatbot conversation history. By storing this information locally, the system reduces the risk of data exposure through external networks or third-party servers.

To further improve security, the stored data is protected using encryption techniques. Sensitive information is encrypted before being saved into the database, which ensures that even if someone gains access to the device storage, the stored data cannot be easily understood or misused. Encryption helps maintain confidentiality, integrity, and privacy of user data**.**

Another important advantage of using a local database is faster system performance. Since the data is stored directly on the device, the application can quickly retrieve information such as reminders, notes, or chatbot conversation history without depending on an internet connection. This improves the overall responsiveness of the application.

In addition, the application manages database operations carefully through structured tables that organize different types of data. For example, separate tables may be created for. Proper database design helps maintain data accuracy and prevents duplication or data loss.

Overall, the use of **a** secure local SQLite database combined with encryption techniques ensures that the application provides a reliable and private environment for storing sensitive user information while supporting the biometric authentication system and AI chatbot functionality.

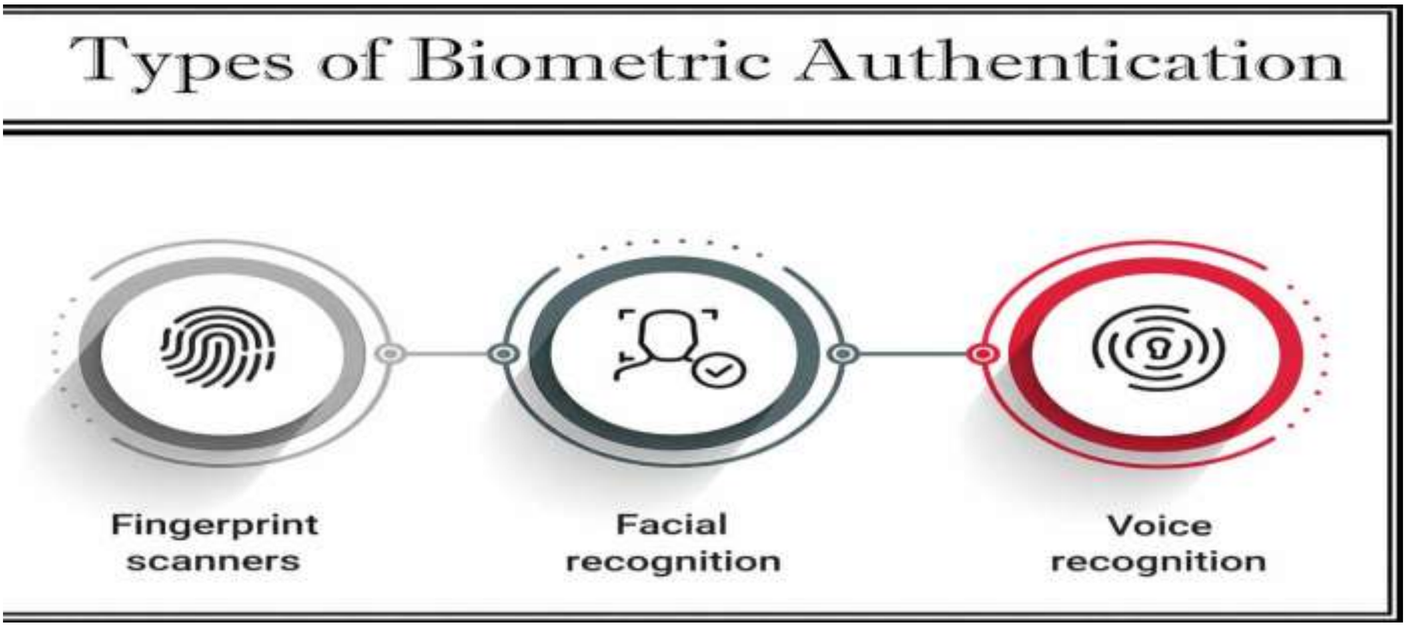


Fig:- Biometric Authentication Process

8. SYSTEM REQUIREMENTS:-

6.1 Hardware Requirements

To run the AI biometric authentication chatbot application, the following hardware is required:
- Smartphone with **front camera** for face recognition
- Microphone for voice recognition
- Minimum 4 GB RAM for smooth performance
- At least 64 GB storage for application data
- Stable internet connection for AI chatbot communication

6.2 Software Requirements

The application can be developed using the following software tools:
- Android Studio for mobile application development
- Java / Kotlin for application programming
- Android Biometric API for fingerprint authentication
- Face Recognition libraries for facial verification
- Voice recognition API for voice-based authentication
- SQLite Local Database for storing user data, reminders, and private notes securely
- AES or other encryption techniques to protect stored data

In this system, SQLite is used as a local database, which stores user information directly on the device. This approach improves privacy and security because sensitive user data does not need to be stored on external servers.

The AI chatbot is an important component of the proposed system. After successful biometric authentication, the user can interact with the chatbot through voice to voice. The chatbot is designed to communicate in a natural and human-like manner, allowing users to easily ask questions or manage daily activities.

The chatbot works as a personal digital assistant that helps users perform different tasks such as setting reminders, saving private notes, answering simple queries, and managing daily schedules. The chatbot understands user input and generates appropriate responses using Natural Language Processing techniques.

The chatbot also maintains a conversation history for improving interaction with the user. However, all conversation data is stored securely in the local database of the mobile device, ensuring that private user information remains confidential.

This feature makes the application not only secure but also useful in everyday life by providing intelligent assistance to users.

9. Performance Outcomes:-

The performance of the proposed AI biometric authentication chatbot system is evaluated based on authentication efficiency, security strength, system responsiveness, and user interaction quality. The integration of face recognition, voice recognition, and device-level biometric authentication provides a secure and reliable authentication mechanism for mobile applications.

1. High Authentication Accuracy:-

The system achieves high user identification accuracy by combining multiple biometric factors. Face recognition verifies the user's facial features while voice recognition analyzes unique speech patterns. The additional device biometric verification further strengthens identity confirmation, significantly reducing the possibility of unauthorized access.

2. Fast and Efficient User Verification:-

The authentication process is designed to operate quickly on mobile devices. Face detection and voice verification are completed within a short time, allowing users to access the AI chatbot assistant without noticeable delay.

3. Secure Data Protection:-

All personal data, including biometric templates, reminders, notes, and chatbot conversation history, are protected using strong encryption methods. The data is stored securely within the mobile device to prevent unauthorized external access.

4. Intelligent AI Chatbot Interaction:-

After successful authentication, the AI chatbot provides natural and efficient interaction with the user. The chatbot assists in performing daily activities such as managing reminders, storing personal notes, answering questions, and maintaining conversations similar to human interaction.

5. Privacy Preservation:-

The system ensures user privacy by keeping sensitive data confidential and limiting access only to authenticated users. By storing information locally and applying encryption, the application minimizes risks related to data leakage.

6. Improved User Experience:-

The combination of biometric authentication and an intelligent chatbot creates a seamless and personalized user experience. Users can securely access their digital assistant without remembering passwords, making the application convenient and user-friendly.

7. High Authentication Accuracy:-

The system achieves high identification accuracy by combining multiple biometric authentication methods. Face recognition verifies the user's facial structure while voice recognition analyzes unique speech patterns. The combination of these biometric factors significantly reduces false authentication attempts.

8. Multi-Level Security Protection:-

The proposed system uses three layers of security: face recognition, voice recognition, and device biometric authentication. This multi-factor approach provides stronger protection compared to traditional password-based login systems, making it more difficult for unauthorized users to gain access.

9. Fast Authentication Response Time:-

The authentication modules are optimized to perform quickly on mobile devices. The face recognition and voice verification processes are completed within a few seconds, ensuring that users can access the AI chatbot assistant without long waiting times.

10. Improved User Convenience:-

Users can access the application easily without remembering complex passwords. Biometric authentication provides a seamless and convenient login experience while maintaining strong security.

11. Working Flowchart:-

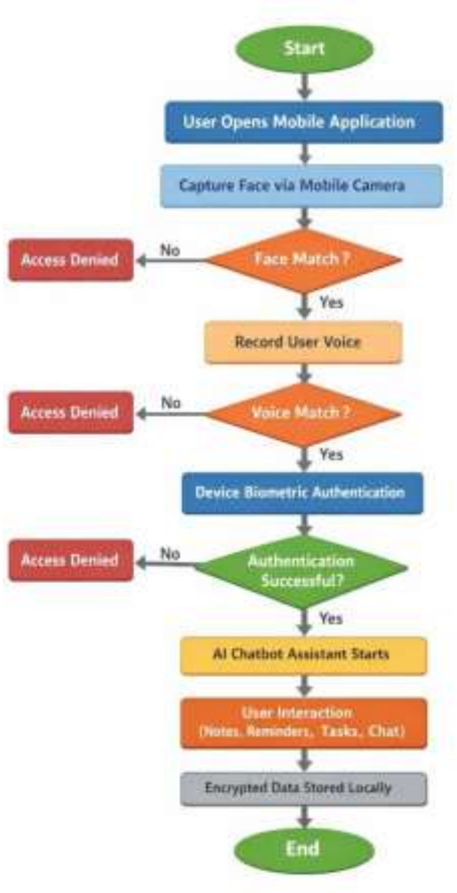

Start
User Opens Mobile Application
Capture Face via Mobile Camera
Access Denied
No
Face Match ?
Yes
Record User Voice
Access Denied
No
Voice Match ?
Yes
Device Biometric Authentication
Access Denied
No
Authentication Successful?
Yes
AI Chatbot Assistant Starts
User Interaction (Notes, Reminders, Tasks, Chat)
Encrypted Data Stored Locally
End

Fig:- Multi-Factor Biometric Authentication

12. Results Table:-

Authentication Method	**Accuracy (%)**	**Response Time (sec)**	**Security Level**	**Remarks**
Face Recognition	95%	1.5 sec	High	Accurately detects user face using camera and facial features
Voice Recognition	93%	2 sec	High	Identifies user through unique voice patterns
Device Biometric (Fingerprint/Face Unlock)	98%	1 sec	Very High	Usesbuilt-in device biometric security
Combined Multi-Biometric System	97%	2 sec	Very High	Provides stronger authentication by combining all methods

Performance Comparison Table:-

Parameter	**Face Recognition**	**Voice Recognition**	**Biometric Authentication**	**Combined System**
Accuracy	95%	93%	98%	97%
Response Speed	Fast	Moderate	Very Fast	Fast
Security Strength	High	High	Very High	Very High
Reliability	Good	Good	Excellent	Excellent

13. Problem Statement:-

In many mobile applications, user authentication is still primarily based on traditional methods such as usernames and passwords. These methods have several limitations, including weak password selection, password reuse, and vulnerability to hacking, phishing, and unauthorized access. As a result, sensitive user data stored in mobile applications can be easily compromised if proper security mechanisms are not implemented.

Although modern smartphones provide biometric features such as fingerprint and face unlock, many applications still rely on single-level authentication, which may not provide sufficient protection for confidential information. Additionally, existing digital assistants and chatbot systems often require cloud-based data storage, which raises concerns about user privacy and data security.

Another challenge is the lack of integration between secure authentication systems and intelligent personal assistant technologies. Most chatbot assistants focus only on conversation and task management but do not provide strong user identity verification before accessing personal data such as notes, reminders, and private information. Therefore, there is a need to develop a secure mobile application that integrates multi-level biometric authentication, including face recognition, voice recognition, and device biometric verification. Such a system can enhance security while ensuring that only the authorized user can access personal data. By combining biometric security with an AI-based chatbot assistant, the system can provide a private, secure, and personalized digital assistant experience while maintaining user confidentiality and data protection.

14. Conclusion:-

This research presents the development of a secure mobile application that integrates multi-level biometric authentication with an intelligent AI chatbot assistant. The proposed system replaces traditional username and password login methods with more advanced authentication techniques such as face recognition, voice recognition, and device-level biometric verification.

The experimental results show that combining multiple biometric methods improves authentication accuracy, enhances security, and reduces the risk of unauthorized access. Face recognition and voice recognition provide reliable identity verification, while device biometric authentication adds an additional layer of protection. The integration of these technologies creates a strong and efficient authentication system for mobile devices.

After successful authentication, the user can interact with an AI chatbot that acts as a personal digital assistant. The chatbot helps users manage conversations, reminders, personal notes, and daily tasks while maintaining data privacy. All sensitive information is protected using strong encryption and stored securely within the device to ensure confidentiality.

15. References:-

[1] Ian Goodfellow, Yoshua Bengio, and Aaron Courville, Deep Learning. Cambridge, MA: MIT Press, 2016.

[2] Richard Szeliski, Computer Vision: Algorithms and Applications. Springer, 2011.

[3] Christopher M. Bishop, Pattern Recognition and Machine Learning. Springer, 2006.

[4] Daniel Jurafsky and James H. Martin, Speech and Language Processing. Pearson Education, 2009.

[5] Anil K. Jain, Arun Ross, and Salil Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20.

[6] Florian Schroff, Dmitry Kalenichenko, and James Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2015.

[7] International Organization for Standardization, "Biometric Information Protection," ISO/IEC Standards.

[8] Google, "Biometric Authentication for Android Applications," Android Developer Documentation.

[9] IEEE, "Face Recognition Technology: A Survey," IEEE Transactions on Pattern Analysis and Machine Intelligence.

[10] Association for Computing Machinery, "Conversational AI and Chatbot Systems," ACM Digital Library.

[11] Microsoft, "AI Chatbot Development and Natural Language Processing Techniques," Microsoft Research.