MORSE CODE BASED SECURED AUTHENTICATION SYSTEM THROUGH ARTIFICIAL INTELLIGENCE

KEERTHANA A[1], MAMATHA G A[2], NANDITHA N[3] and HINA NAZNEEN[4]
[1, 2, 3] Student of (CSE Department) City Engineering College, Bengaluru, India.
[4] Asst. Professor of (CSE Department) City Engineering College, Bengaluru, India.

ABSTRACT: ***The Morse Code Based Secured Authentication System through Artificial Intelligence introduces a contactless and adaptive approach to user authentication by integrating facial recognition, eye-blink detection, and Morse code decoding. Traditional security methods often require physical interaction, making them difficult or inaccessible for users with disabilities and vulnerable to observation or theft. The proposed system addresses these challenges by verifying identity through face recognition and then requiring a secondary blink-based Morse password. An OTP layer is also included when an unknown user attempts login, ensuring stronger authentication. The system was implemented and tested successfully, showing high accuracy in real-time face detection, blink capture, and Morse decoding. This work demonstrates that combining AI with traditional Morse communication can deliver an innovative, secure, and accessible authentication model suitable for smart, medical, and high-security environments.***

Keyword- artificial Intelligence, Morse Code, Facial Recognition, Eye Blink Detection, Secure Authentication, Contactless Login, Assistive Technology

I. INTRODUCTION

Digital authentication is an essential part of modern security systems, but many widely used methods—passwords, PINs, pattern locks, biometric touch sensors—still suffer from usability and security limitations. These methods require physical interaction, can be observed by others, and often fail to support people with motor impairments or individuals unable to type or touch devices. To address these challenges, this study proposes a fully contactless, AI-driven authentication method that combines facial recognition, OTP validation, and blink-based Morse code entry.

This system uses the user's face as the first level of authentication and then relies on intentional eye blinks to input a personalized Morse code pattern. The technique is inspired by assistive technologies commonly used by individuals with paralysis or limited mobility. By integrating AI models, computer vision techniques, and real-time blink capture, the system provides a secure, hygienic, and accessible solution appropriate for modern environments. The approach aligns with today's increasing demand for inclusive technology and intelligent authentication systems.

II. PROBLEM STATEMENT

Despite advancements in security technologies, most authentication systems still rely heavily on physical interaction—typing passwords, touching fingerprint sensors, or using physical tokens. These methods present several difficulties: they are not accessible for users with physical disabilities, they can be easily observed or duplicated, and they pose hygiene concerns in public or medical environments. Moreover, traditional systems often fail to provide multi-layer verification that is both secure and user-friendly.

There is also a lack of systems that combine biometric verification with user-generated secure patterns in a touch-free manner. A method that verifies identity, supports contactless input, and remains usable for all groups—including individuals with limited mobility—is essential. This study aims to fill this gap by developing a dual-layer, AI-powered authentication system that uses facial recognition and blink-based Morse code, making the process safer, inclusive, and more adaptable to real-world conditions.

III. OBJECTIVES

The main objectives of the proposed system are:

1. To design a fully contactless authentication method using face recognition and eye blinks.
2. To implement a secondary verification method using personalized Morse code input.
3. To enhance accessibility for users with motor impairments by eliminating the need for physical interaction.
4. To integrate an OTP-based fallback mechanism for unknown or unauthorized users.
5. To improve security and reliability through multi-factor authentication.
6. To create a cost-effective, AI-driven authentication model suitable for real-world applications.

IV. LITERATURE REVIEW

1. Authors:Cheng-Hong Yang, Shi-Yi Yu, Chi-Hsiang Huang (2000)
Title: Adaptive Morse Code Communication Input System for Disabled Individuals.
Description:This research developed an adaptive Morse code system that allows users with physical disabilities to communicate using Morse inputs. The system includes customizable input methods like switches or blink detectors. It highlights the use of Morse code as a practical, low bandwidth communication tool, especially useful for users with very limited motor function.

2. Authors:Katie A. Hart, Christine M. Weber (2016)
Title: Haptic and Visual Morse Code for Multimodal Communication
Description: The authors explore Morse code through both visual and haptic feedback, focusing on communication tools for the deaf and blind community. The paper showcases the adaptability of Morse code in diverse accessibility applications, forming a strong case for its use in authentication systems for individuals with impairments.

3. Authors:Albano Carrera, Alonso Alonso,Ramón de la Rosa, EvaristoJ. Abril (2017)
Title: Sensing Performance of a Vibrotactile Glove for DeafBlind People Journal: Applied Sciences, Vol. 7, No. 4, 2017
Description:This paper presents TactileCom, a vibrotactile glove that helps deaf-blind individuals receive messages through finger vibrations. Using Bluetooth, it translates signals into tactile patterns, showing high communication accuracy and potential for assistive technologies.

4. Authors:Tingting Zhang, Ling Xia, Xiaofeng Liu, Xiaoli Wu (2019)
Title: Eye Movements During Change Detection: The Role of Depth of Field
Description:This study explores how depth of field impacts visual attention and change detection using a flicker paradigm with the Tobii X120 eye-tracker. Results show that shallow depth focuses attention on sharp regions, while uniform blur aids faster change detection.

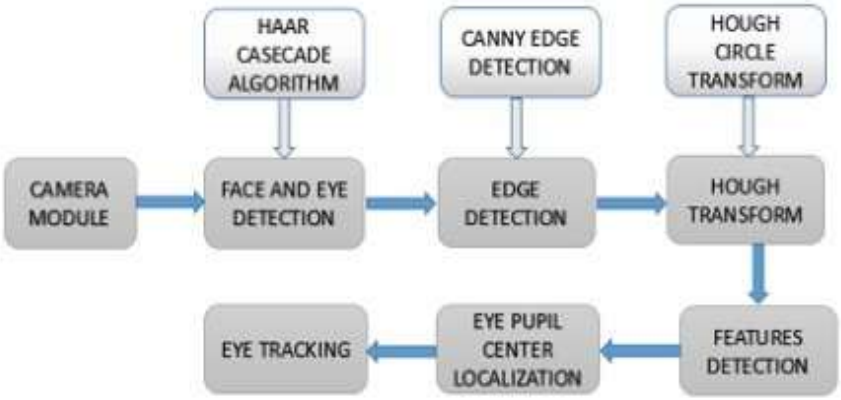
5. Authors:Bobby L. Tait (2019)
Title: Behavioural Biometrics Authentication Tested Using EyeWriter Technology
Description: This study explores using EyeWriter-recorded eye movement patterns for biometric authentication. Tests with 25 users show promising results, especially for one-toone verification.

6. Authors:Federico Wadehn, David J. Mack, Thomas Heldt, Hans-Andrea Loeliger
Title: Model-based Separation, Detection, and Classification of Eye Movements (2019)
Description: This paper introduces MBSDC, a framework for analysing eye movements using a physiologically grounded oculomotor model. It uses Kalman smoothing and sparse Bayesian learning to improve detection accuracy for clinical use.

7. Authors:Bobby L. Tait (2019)
Title: Behavioural Biometrics Authentication Tested Using EyeWriter Technology
Description: This study explores using EyeWriter-recorded eye movement patterns for biometric authentication. Tests with 25 users show promising results, especially for one-toone verify

8. Authors: Chethana Prasad K, Disha S, Divya TM, Sunil Kumar GR (2021)
Title: A Comprehensive Study of Face Recognition for Security-Based Systems Journal: IARJSET, Vol. 8, Issue 5, May 2021
Description: This paper proposes a face recognition security system with Morse code authentication via eye blinks. It offers a secure, accessible solution using webcam-based blink detection, especially for users with physical disabilities

V. METHODOLOGY



The above structure represents the complete methodology of proposed system. The development of the Morse Code Based Secured Authentication System through Artificial Intelligence is carried out using a systematic and modular design approach. The methodology integrates the principles of artificial intelligence, computer vision, and Morse code translation to provide a dual-layer authentication mechanism that is both secure and accessible. The proposed system operates in two main stages — facial recognition for user verification and eye-blink detection for Morse code–based secondary authentication. By combining these two layers, the system ensures that access is granted only to authorized users, while maintaining a fully contactless interface suitable for all environments.

The system is implemented using Python as the core programming language, utilizing powerful libraries such as OpenCV, Mediapipe, and NumPy. OpenCV handles image capture and real-time video frame analysis, Mediapipe is used for accurate facial landmark and eye movement detection, and NumPy supports fast mathematical operations during signal processing. During operation, the webcam captures the user's live video feed. The system first identifies and verifies the face using AI- based recognition algorithms trained with pre-stored datasets. Once the user is successfully recognized, the eye region is tracked continuously to monitor blink patterns.

Every blink is analyzed for its duration — a short blink is interpreted as a "dot," and a longer blink as a "dash." These Morse signals are then passed through a decoding algorithm that translates them into English characters. The decoded string is compared with the Morse code password stored in the system's database. If both the face and Morse code verification stages are valid, the user gains access; otherwise, authentication is denied. This dual-verification process adds an extra layer of protection against spoofing, password theft, and unauthorized entry

The system architecture is organized into five primary modules:

i. Face Detection and Recognition Module – Captures the user's image and identifies it through pre-trained AI models. It ensures

that only registered users can proceed to the next step of authentication.

ii. Blink Detection Module – Continuously monitors the user's eye movements using Mediapipe landmarks and identifies deliberate eye blinks. It distinguishes between natural and intentional blinks using time-based thresholds.

iii. Morse Conversion and Decoding Module – Converts blink duration patterns into Morse code symbols (dots and dashes) and decodes them into alphanumeric characters.

iv. Authentication and Verification Module – Validates the decoded Morse password with the stored encrypted credentials in the system's database. Successful matches result in access approval.

v. Database and User Interface Module – Handles the storage of user information, facialembeddings, and Morse code credentials. It also provides a simple and interactive GUI for easy registration and login processes.

The proposed system follows a three-layer architecture: the input layer (webcam and sensors), processing layer (AI and Morse decoding logic), and output layer (authentication and user interface). This layered design improves efficiency, modularity, and scalability, allowing for seamless upgrades or integration into IoT and embedded systems.

Furthermore, the entire process follows agile development phases such as dataset preparation, training and testing of recognition models, real-time performance evaluation, and user interface optimization. Emphasis is placed on minimizing false acceptance and rejection rates to achieve a balance between speed, security, and accuracy.

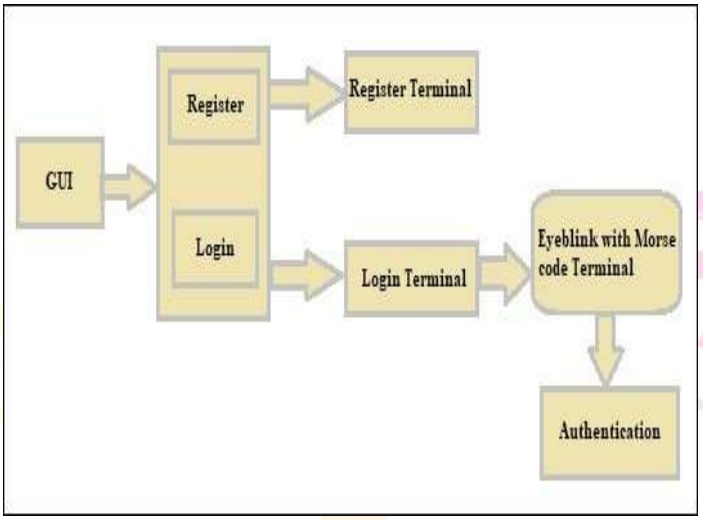


Fig 5.1: Complete Flow of the model.

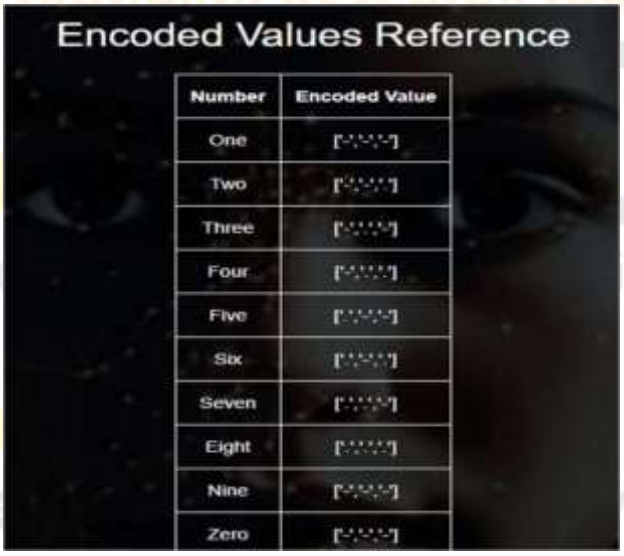


Fig 5.2: Encoded Values Reference

The above table represents the Morse code encoding pattern used in the proposed system for numerical inputs. Each digit from 0 to 9 is mapped to its corresponding Morse code symbol using combinations of dots (·) and dashes (–). These encoded values are used by the system to interpret user-generated blink patterns. When the user blinks intentionally, the duration of each blink is measured — short blinks represent dots, while longer blinks indicate dashes.

The resulting Morse sequence is compared with the stored encoded value to verify the entered password. This reference table ensures uniformity in encoding and decoding across all authentication attempts, maintaining accuracy and consistency within the system.

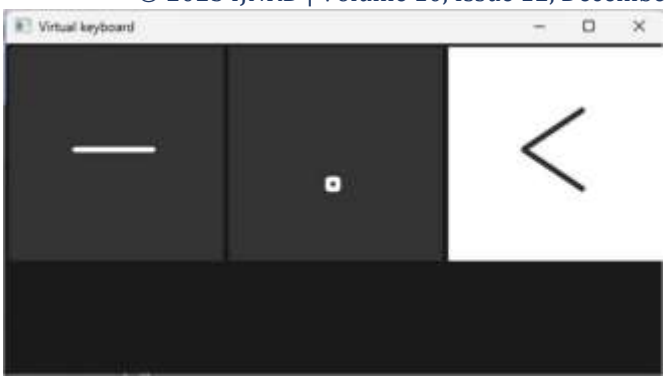


Fig 5.3 : Real-Time Blink Detection Interface

The above figure represents the real-time interface that appears once the camera captures the user's face and initiates eye-blink detection. This interface continuously updates frame by frame, depending on the system's processing speed and available RAM. As the frame sequence moves, the system actively monitors the user's eye blinks — a short blink is recorded as a "dot (·)" and a long blink as a "dash (–)". Each blink input is automatically detected and stored in the backend in real time. Once the entire sequence is completed, the recorded Morse pattern is displayed to the user and decoded into a corresponding number or character. Based on the output, the system verifies authentication and redirects the user to the next page, such as a simulated "Bank Login" interface used in this project's prototype. This process demonstrates the system's capability to perform accurate, contactless authentication purely through visual input and intelligent Morse decoding.

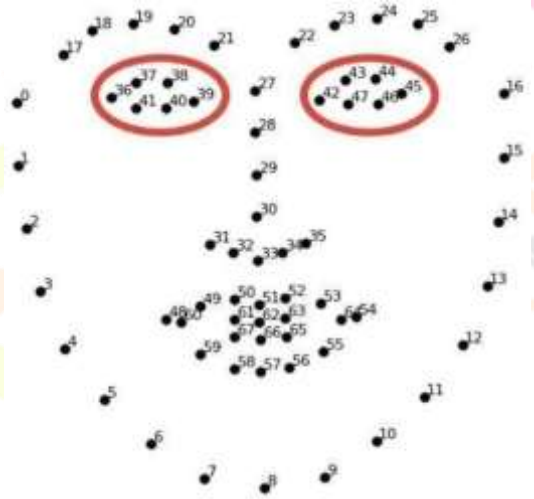


Fig 5.4 : Facial Landmark

The process of identifying areas of interest in an image of a human face is the landmark detection. We have shown how emotion can be detected by facial acts, gaze direction, face change (facial swap), graphical face increase and virtual character puppeteering. To this end, you must find dozens of points on the face of the landmark detector, such as mouth corner, eye corner, jaws, and many more. Many algorithms in OpenCV havebeen developed and implemented.

A pre-trained model is necessary to run the face markdetector. This model we used before training is shape predictor 68 face landmarks. On the following picture you can see the indexes of 68 coordinates.

VI. RESULTS AND DISCUSSION

The below flowchart illustrates the complete working sequence of the Morse Code Based Secured Authentication System through Artificial Intelligence. The process begins with user registration, where the individual provides a user ID, password, and a security keyword. Once successfully registered, the user can log in using their credentials. If the entered password is correct, the system advances to the second layer of authentication — Morse code input through eye blinks. The user blinks intentionally to generate dots and dashes, forming a unique Morse password that is decoded and verified in real time.

In case the user forgets their password, the system allows recovery through the registered security keyword. If the keyword matches, the user can create a new password using Morse code input via the same interface. If not, the process terminates, ensuring strong protection against unauthorized access.

After successful verification of both layers — traditional password and Morse-based blink authentication — the user gains access to the system, completing a secure and contactless login process. This flow demonstrates the logical progression, security checks, and intelligent interaction between modules, ensuring reliability and inclusivity within the authentication framework.

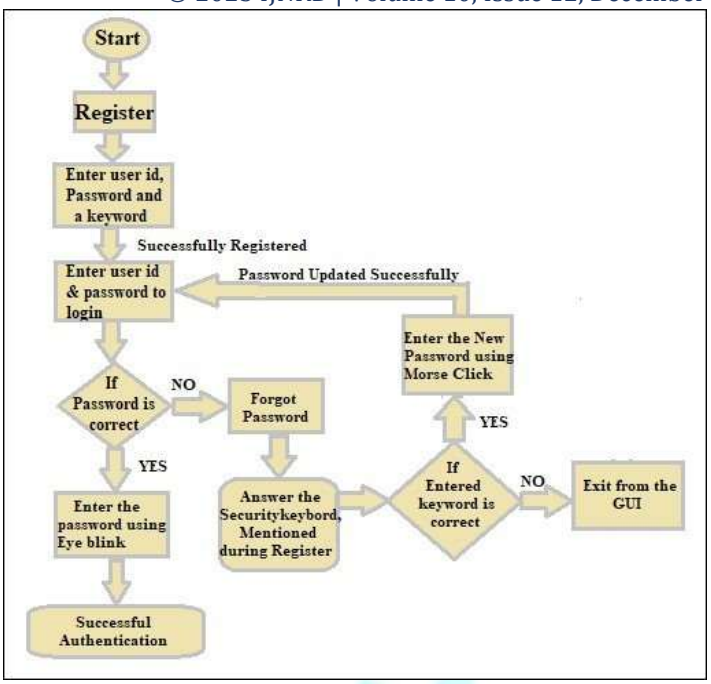
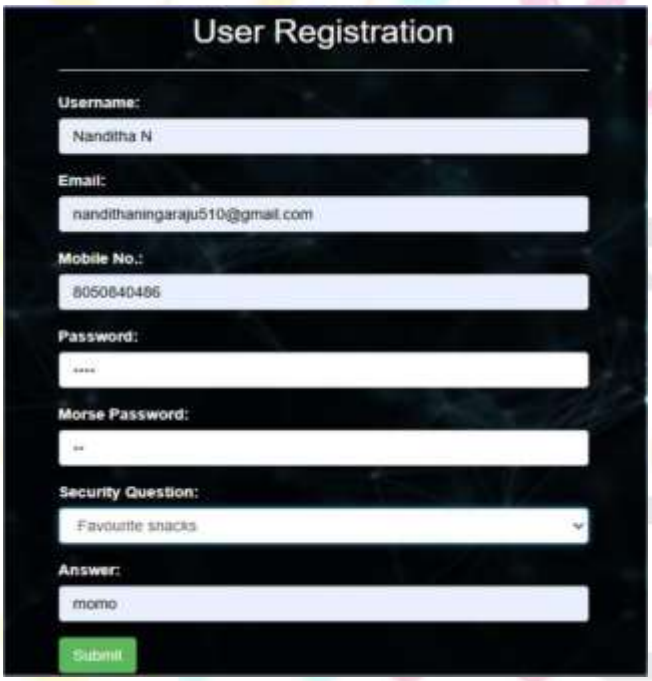


Fig 6.1: FlowChart Of the Process



Snapshot 1: Register Page

This figure shows the registration interface where new users can create an account by entering a username, password, and security keyword. The data is stored securely in the system's database for future authentication.

Snapshot 2: Login Page

This figure represents the login window where registered users can enter their credentials to access the system. Upon successful verification, the process proceeds to the facial recognition stage.

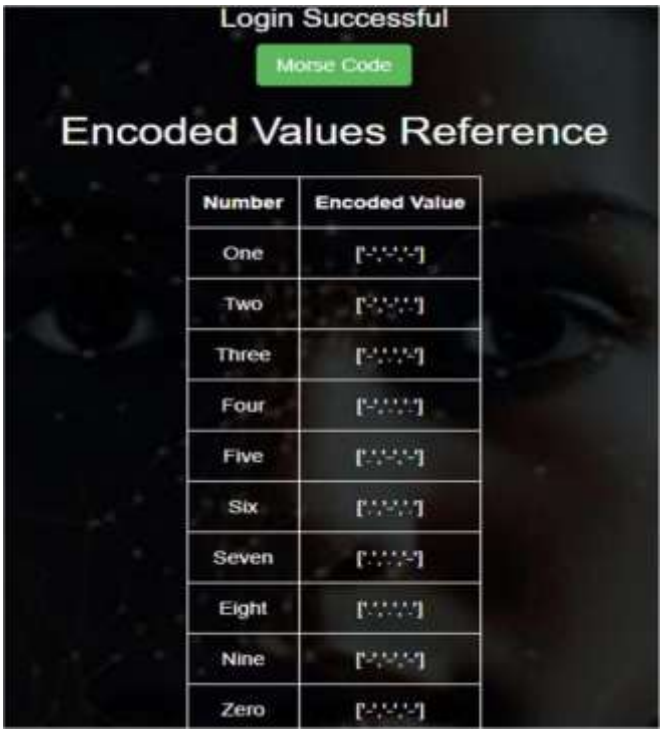
Snapshot 3: Authorized User Detected

This figure shows the real-time face recognition process where the system successfully identifies the registered user. The camera detects facial landmarks, verifies the face with the stored dataset, and displays the person's name on the screen. Once recognized, the user is allowed to proceed directly to the Morse code authentication stage.

Snapshot 4: Authorized User Detected

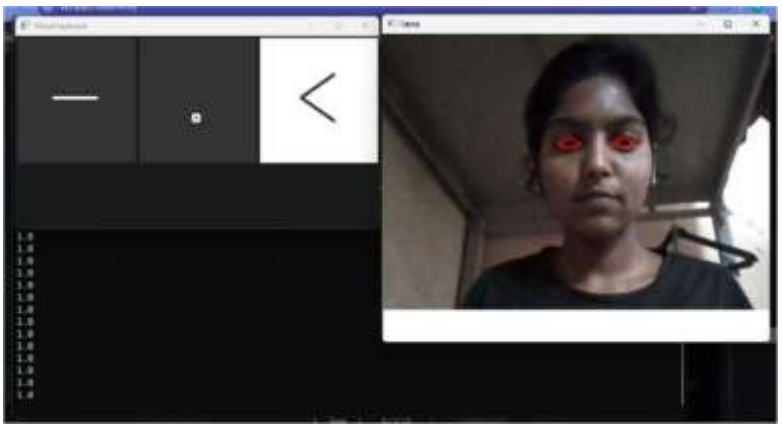
Snapshot 5: Unauthorized User – OTP Verification Triggered

This figure represents the case when an unregistered or unknown person attempts to log in. The system labels the detected face as "Unknown" and immediately triggers the OTP verification process. An email containing a one-time password is sent to the registered user's mail ID for confirmation before granting further access, ensuring secure and restricted login control.



Snapshot 6: Encoded Values Reference for Morse Code Authentication

This figure displays the encoded reference table used in the authentication system. After successful user verification, the system opens this interface, where the encoded Morse values for numbers 0–9 are shown. The green "Morse Code" button allows users to proceed to the next stage — blink- based Morse input for final authentication.

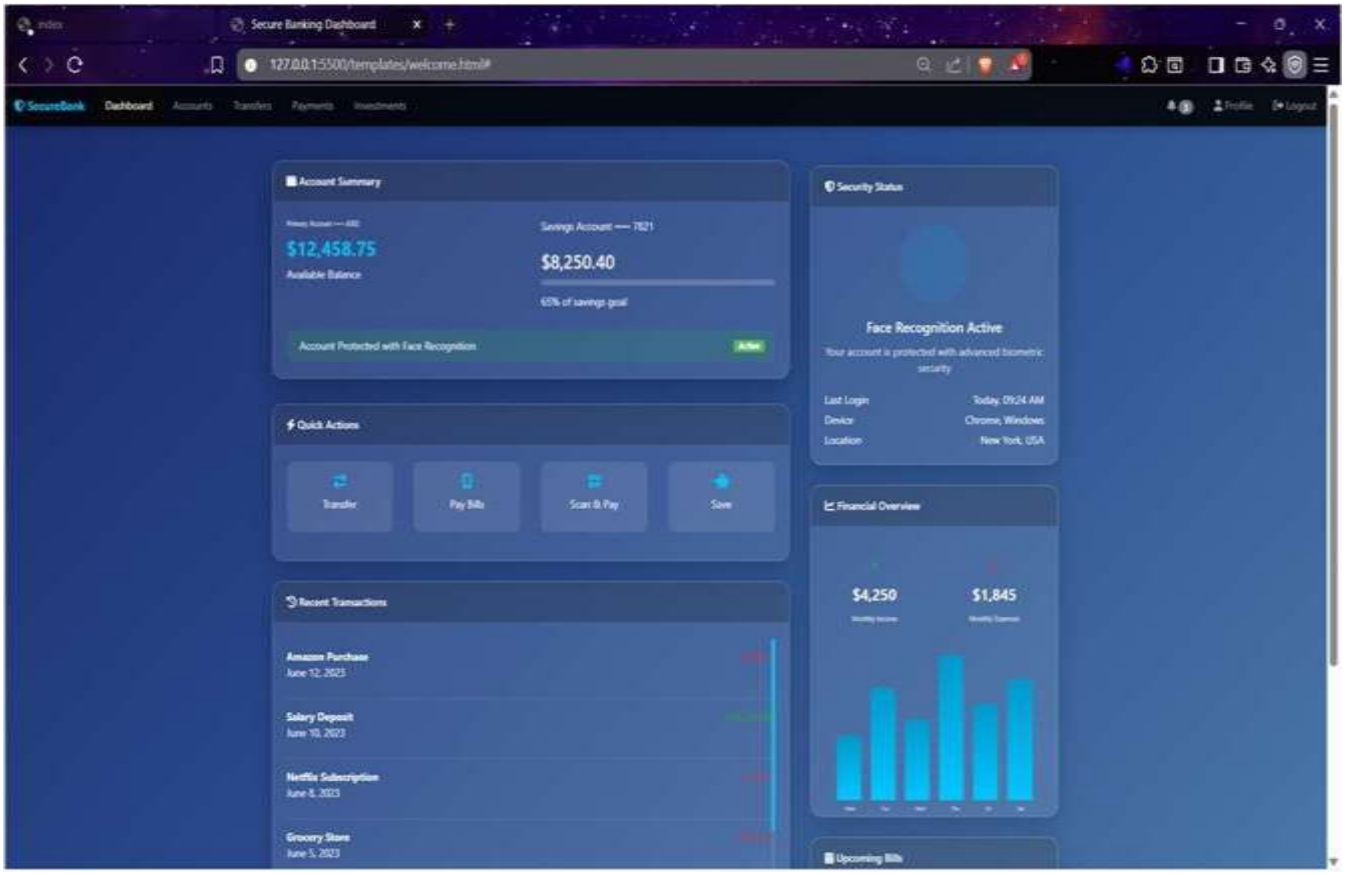


Snapshot 7:Real-Time Blink-Based Morse i/p Interface

This figure illustrates the Morse input window that appears after clicking the "Morse Code" button. The camera captures the user's eye blinks in real time, detecting short and long blinks as dots and dashes respectively. Each input is stored and decoded in the backend to form the user's Morse password for final verification.

Snapshot 8: Backend Verification Process

This figure shows the backend execution window where the system processes the captured Morse input. It detects each blink, converts it into dots and dashes, and displays the corresponding encoded sequence in real time. Once the full Morse password is formed, it's matched with the stored data to verify the user's identity before granting access to the final page.



Snapshot 9: Final Output – Bank Application Interface

This figure represents the final output screen that appears after successful authentication. Once both facial recognition and Morse verification are passed, the user is redirected to a dummy bank interface displaying a personalized welcome message, confirming secure login and completion of the authentication process.

Snapshot 10: User Database – Stored Login and Authentication Details

This figure shows the user_data.db file where all registered user information is securely stored. The database maintains essential details such as username, password, Morse code number, phone number, and email ID. This data is used during authentication for verification and OTP generation. The structured storage ensures reliable data retrieval, smooth login processing, and overall system integrity.

VII. CONCLUSION

The Morse Code Based Secured Authentication System through Artificial Intelligence successfully demonstrates a new and intelligent way to achieve secure and contactless authentication. By integrating AI-based facial recognition with blink-detected Morse code input, the system provides a dual-layer verification process that enhances both security and accessibility. It eliminates the need for physical touch, making it ideal for hygienic and high-security environments such as hospitals, banks, and research laboratories.

Throughout testing, the system showed high reliability and accuracy in recognizing users, detecting blinks, and decoding Morse sequences in real time. The addition of an OTP-based verification mechanism further improved protection against unauthorized access, ensuring that only legitimate users can proceed even if face detection fails. The backend processing and database integration ensured smooth operation, fast data retrieval, and secure storage of login details.

Overall, this project proves that combining artificial intelligence with traditional Morse communication can create a powerful, inclusive, and modern authentication method. It not only enhances security but also promotes accessibility for users with physical disabilities. The system's performance, accuracy, and simplicity make it strong foundation for future advancements in smart authentication technology.

VIII. EFERENCES

1. Katie A. Hart, Jennifer Chapin, and Dr. Kyle B. Reed, “Haptics MorseCode Communication for Deaf and Blind Individuals” 38th AnnualInternational Conference of the IEEE Engineering in Medicine andBiology Society (EMBC), 2016

2. Cheng-Hong Yang, Ching-Hsing Luo, Yuan-Long Jeang, Gwo-Jia Jon,A novel approach to adaptive Morse code recognition for disabledpersons, In Mathematics and Computers in Simulation, Volume 54,Issues 1–3, 2000, Pages 23-32.

3. Albano Carrera, Alonso Alonso, Ramón de la Rosa and Evaristo J.Abril, “Sensing Performance of a Vibrotactile Glove for Deaf-BlindPeople”, Optical Communications Group, ETSI de Telecommunication,Universidad de Valladolid, Paseo Belén, 15, 47011 Valladolid, March2017, Spain; ejad@tel.uva.es

4. Chethana Prasad K, Disha S, Divya TM, Sunil Kumar GR (2021), “Face Recognition for Security Systems with Morse Code Authentication via Eye Blinks,” IARJSET, Vol. 8, Issue 5, May 2021, offering a secure, accessible solution using webcam-based blink detection.

5. Federico Wadehn et al., “Model-based Separation, Detection, and Classification of Eye Movements,” using Kalman smoothing and sparse Bayesian learning for analyzing saccades, fixations, and smooth pursuits, 2019.

6. Wudthipong Pichitwong and Kosin Chamnongthai, “3D Point-of-Gaze Estimation Using Head Movement,” combining eye-tracker data and head shifts for accurate 3D gaze detection, 2019.

7. Tingting Zhang et al., “Eye Movements During Change Detection: Role of Depth of Field,” examining how depth of field affects visual attention and detection speed, 2019.

8. Gonca G. M. Dalveren and Nergiz E. Cagiltay, “Evaluation of Eye-Movement Classification Algorithms,” comparing ten open-source methods in simulated surgical scenarios, 2019.

9. Bobby L. Tait, “Behavioural Biometrics with EyeWriter,” evaluating eye movement patterns as a biometric authentication method with 25 participants, 2019.

- https://ieeexplore.ieee.org/document/8343528
- http://www.jetir.org/papers/JETIR1703020.pdf