



# Morse Code Based Authentication System

<sup>1</sup>Dr. Prashanth Kogali, <sup>2</sup>Akshaya D, <sup>3</sup>Fiza Begum S, <sup>4</sup>K M Nagarakshita, <sup>5</sup>Soujanya M Y,

<sup>1</sup>Professor, <sup>2</sup>Student, <sup>3</sup>Student, <sup>4</sup>Student, <sup>5</sup>Student,

<sup>1</sup>Department of Computer Science and Engineering,

<sup>1</sup>Proudhadevaraya Institute of Technology, Hospet, India.

**Abstract:** Data science combines data inference, algorithms, and technology to solve complex problems and is widely used across industries like education, finance, healthcare, and business. Applications range from stock prediction to cancer detection, image processing, and speech-to-text systems.

With growing concerns about authentication and security, real-time gaze-based PIN entry offers a hands-free, secure alternative to traditional PINs. This technique uses eye-tracking to detect and track eye movement over time, enabling password authentication through Morse code. It eliminates physical traces, enhancing security for users.

**Keywords - Data Science, Machine Learning, Usable Security, Accessibility, Inclusion.**

## I. INTRODUCTION

Technology has always driven change, transforming societies from movable type to the digital age. One significant advancement is data science, which analyse data to uncover insights, optimize processes, and identify opportunities. Machine learning, a subset of data science, enables computers to improve performance through data-driven algorithms, supporting predictive models that reveal hidden insights. These technologies empower businesses and researchers to make informed decisions and achieve competitive advantages.

Usable security focuses on designing systems that balance security and user-friendliness. According to the principle of psychological acceptability, security mechanisms should minimize user effort and align with their abilities and knowledge. For security to be effective, it must feel seamless and unobtrusive.

This project integrates these principles to create an accessible system for all, particularly disabled individuals, ensuring their inclusion in society while addressing usability and security challenges effectively.

## II. PROBLEM STATEMENT

To provide a platform for the physically challenged and disabled people by which they will create a secure private account to which only they will access. Our solution would allow persons with motor disabilities to interact with devices and during this authentication is bit more increased by rather than giving some authentication code by keyboard. This project gives catchphrase and fewer using of hardware sensors which is using in nowadays.

## III. EXISTING SYSTEM

Advancement within the technology of authentication and authorization has be supported within the 21st century. Personal identification numbers (PIN) are widely used for user authentication and security since the late 90's. Since PIN numbers are often easily crack able lately, we like better to follow different approach. PIN authentication with hands off gaze-based PIN entry techniques, on the opposite hand, leaves no physical footprints behind and thus offer a safer password entry option.

## IV. PROPOSED SYSTEM

- The model consists of a interface and rear database. GUI is made such the user can interact with the system. Pygmy or OpenCV is employed in to make it.
- In the frontend firstly the user got to register by providing a user id of choice, a password (PIN) and a keyword. After registration the user can log in by using the credentials i.e. user id and password. With the assistance of an internet camera the PIN is taken as input within the sort of Morse.
- In the backend, the entered PIN is checked with the stored PIN which was entered.

## V. LITERATURE SURVEY

A literature survey or a literature review is a section which shows the various analyses and research made in the field of particular interest and the results already published, taking into account the various parameters of the project and the extent of the project. Most often associated with academic-oriented literature. Literature reviews are a basis for research in nearly every academic field. A narrow-scope literature review may be included as part of a peer-reviewed journal article presenting new research, serving to situate the current study within the body of the relevant literature and to provide context for the reader. In such a case, the review usually precedes the methodology and results sections of the work.

## VI. RESEARCH METHODOLOGY

The system uses computer vision technology for eye pupil detection and tracking. A new image-processing algorithm is employed, involving stages like face detection, eye detection, edge detection, Hough transformation, motion detection, and object tracking. Initially, a webcam captures images, and the system identifies the user's face within the frame. The eye region is then detected and cropped as the region of interest. Corner detection identifies eye corners, and the distance between the eye corner and pupil center is calculated using coordinate logic. Based on the measured distance, the system determines the pupil's movement: minimum distance indicates left, maximum indicates right, and no movement indicates the center position. The detected data is compared with a trained dataset. If the data does not match, an "unauthorized access" error is displayed. Otherwise, the system confirms authentication and allows further transactions.

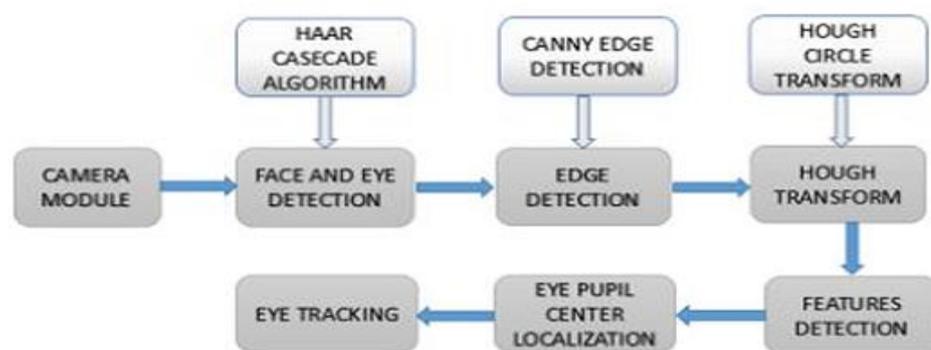


Fig 2.1 System Processing

## VII. SYSTEM REQUIREMENT SPECIFICATION

Project requirements outline tasks and objectives critical for success, improving efficiency, communication, and project outcomes. Functional requirements define system functionality, while non-functional requirements set constraints like performance and security. Evolving requirements can complicate quality assurance, emphasizing the need for clear planning and design.

### 7.1 System requirements

#### 7.1.1 Functional requirements

The major functional requirements are:

- To accurately detect the eye of the user, the data is taken from web camera which provides proper authentication.
- To establish eye typing mechanism for pin entry.

- To enhance security by mitigating replay attacks.

### 7.1.2 Non-functional requirements

A non-functional requirement (NFR) is a requirement that specifies criteria that can be used to judge the operation of a system, rather than specific behaviors. NFR are contrasted with functional requirements that define specific behavior or functions. The plan for implementing functional requirements is detailed in the system design and non-functional requirements is detailed in the system architecture, because they are usually architecturally significant requirements.

## 7.2 SOFTWARE REQUIREMENTS

- Operating system: Windows XP / 7 /8/10
- Coding Language: Python
- Software: Anaconda or Python3.7
- IDE: Python
- Packages: OpenCV

## 7.3 HARDWARE REQUIREMENTS

- System: Pentium IV 2.4 GHz/ intel3/i4, etc.
- Hard Disk: 500 GB.
- Ram: 4GB

## VIII. SYSTEM DESIGN AND ARCHITECTURE

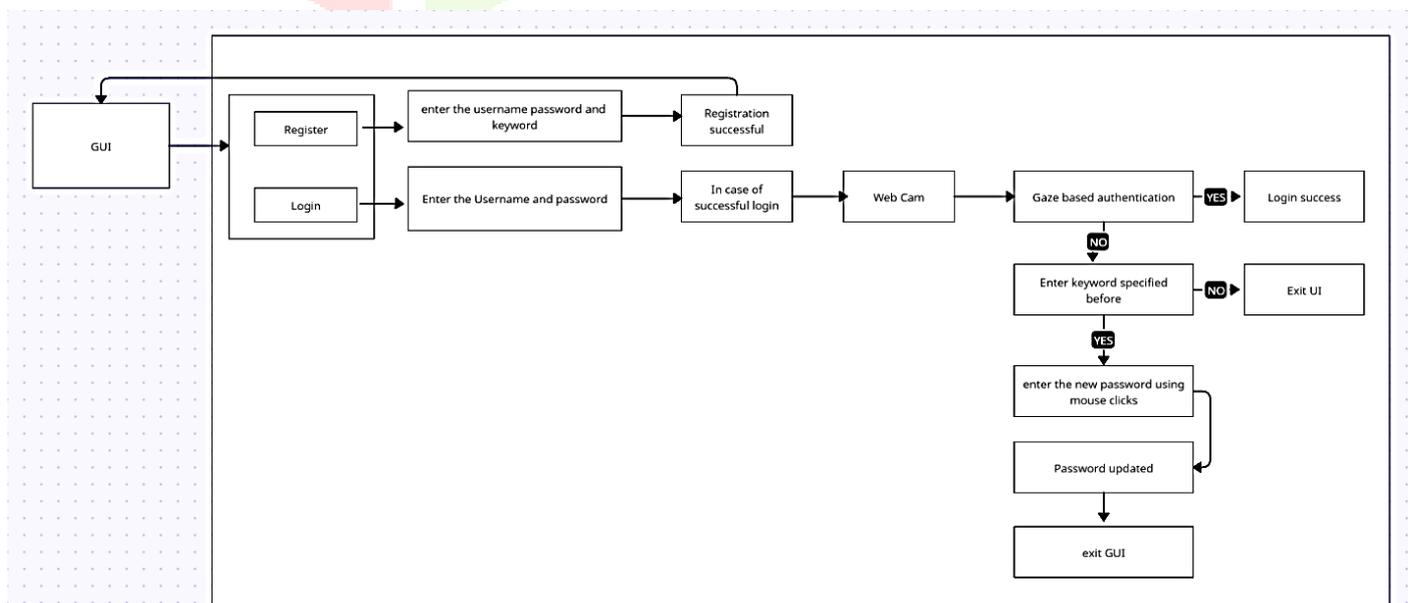
System design defines the architecture, components, interfaces, and data needed to meet specific requirements. It focuses on achieving system objectives by organizing software into components and interfaces.

Key aspects include:

- Architectural Design: Defines system structure, behavior, and views.
- Logical Design: Abstracts data flows, inputs, and outputs.
- Physical Design: Details data input, processing, and display.

As a crucial phase in software development, system design uses requirements, problem analysis, and proposed system needs to produce outputs like data schemas, function hierarchies, and prototypes. It forms the foundation for system development.

### 8.1.1 Architecture of the Model

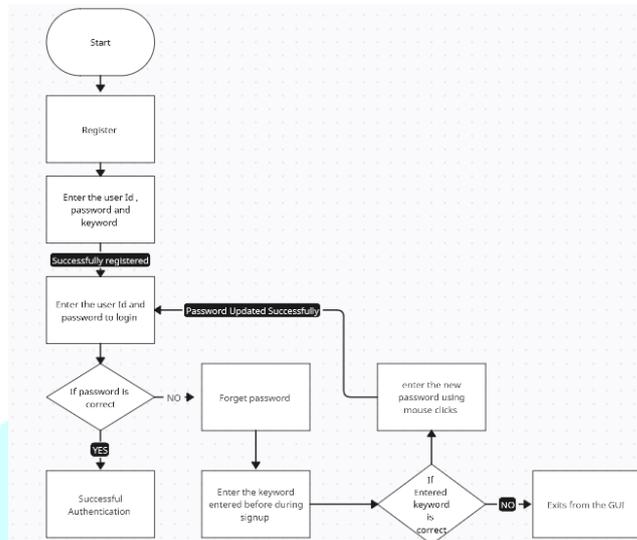


The architecture in Figure outlines the model's essential design, comprising a user interface and a backend database.

The **frontend** uses tools like Pygame or OpenCV to create a GUI where users can interact. Users register by providing a user ID, password (PIN), and keyword. Login is done using these credentials, with the PIN entered as Morse code via a webcam.

In the **backend**, the entered PIN is validated against the stored database PIN. Incorrect PINs exit the system, while correct PINs authenticate successfully. Forgotten passwords can be reset using the keyword, allowing users to update their credentials.

### 8.1.2 Flow Chart



When the user opens the application, a GUI prompts them to either log in or register.

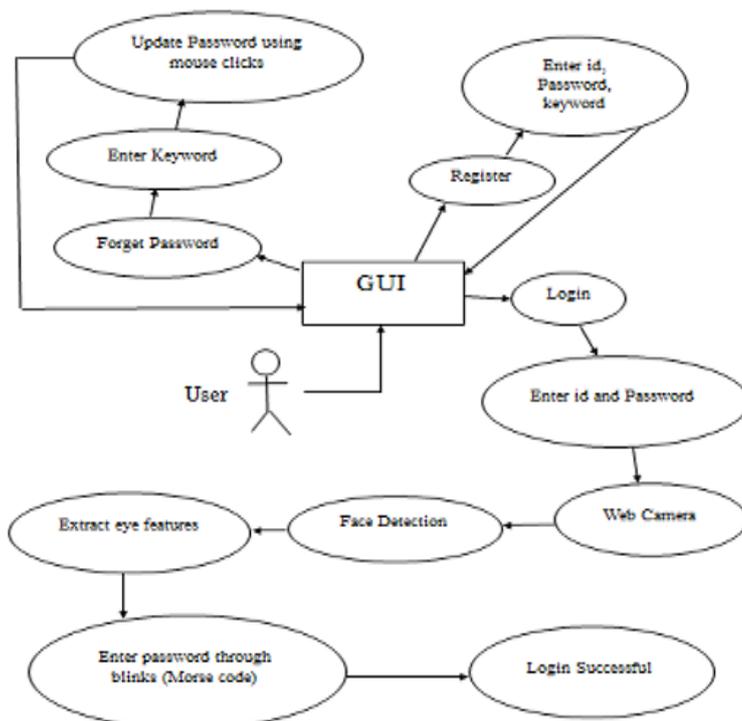
**Registration:** Users provide a user ID, password, and keyword, which are stored in a database.

**Login:** Users enter their credentials. If they match the database, authentication is successful. If not, users can answer a security question using the keyword.

- If the keyword matches, users can update their password via mouse input, and the new password is stored in the database.
- If the keyword is incorrect, the user exits the application.

The updated password is used for future logins.

### 8.2 Use Case Diagram



This system flow provides a straightforward user authentication process:

1. **Initial Screen:** The GUI prompts the user to either log in or register.
2. **Registration:** User inputs a unique ID, password, and keyword. This information is stored in the database.
3. **Login:** User enters the credentials. If they match the stored ones, authentication is successful.
4. **Password Recovery:** If the credentials don't match, the user can enter the keyword for security verification.
  - If the keyword matches, the user can update the password using the mouse, and the new password is stored.
  - If the keyword is incorrect, the user exits the application.

The new password will be used for future logins.

## IX. Implementation Overview

The system uses a GUI where users can register or log in. During registration, users provide a user ID, password, and keyword, which are stored in a database. During login, if credentials match, authentication is successful. If not, users can answer a security question using the keyword. Correct keywords allow password updates, while incorrect ones exit the application.

### Algorithm Used

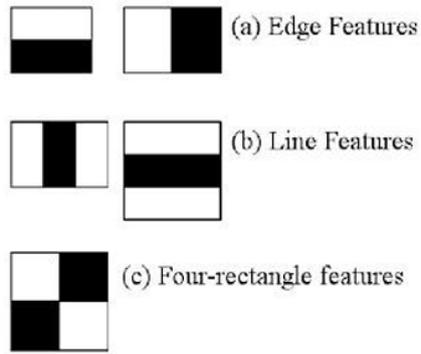


1. **Facial Landmark Detection:** Detects key points on a face (e.g., eyes, mouth, jaw) for tasks like gaze direction and emotion recognition. The system uses a pre-trained model, `shape_predictor_68_face_landmarks`, to identify 68 facial landmarks.
2. **Eye Tracking:** Includes three phases:
  - **Eye Detection:** Uses Haar Cascade to detect eyes from webcam images.
  - **Feature Detection:** Locates eye pupil positions and calculates gaze values.
  - **Eye Tracking:** Tracks eye movement and calculates blink ratios, converting these into PIN entries for authentication.

### Haar Cascade Algorithm

A machine learning algorithm used for object detection:

- **Stages:**
  1. **Haar Feature Selection:** Extracts rectangular regions and calculates intensity differences.
  2. **Integral Images:** Speeds up computation.
  3. **Cascading Classifiers:** Organizes weak classifiers into stages to identify objects.
- **Process:** A sliding window scans the image, calculating Haar features at each step. Positive matches are passed to successive stages until the object is confirmed or rejected. Negative samples are quickly discarded to save time.



## X. RESULTS



Fig.1 Home Page

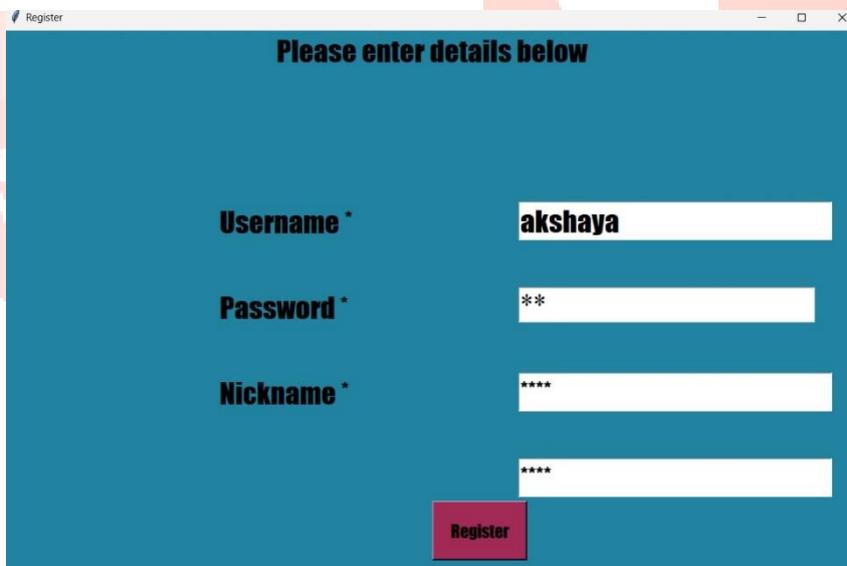


Fig.2 Register Page

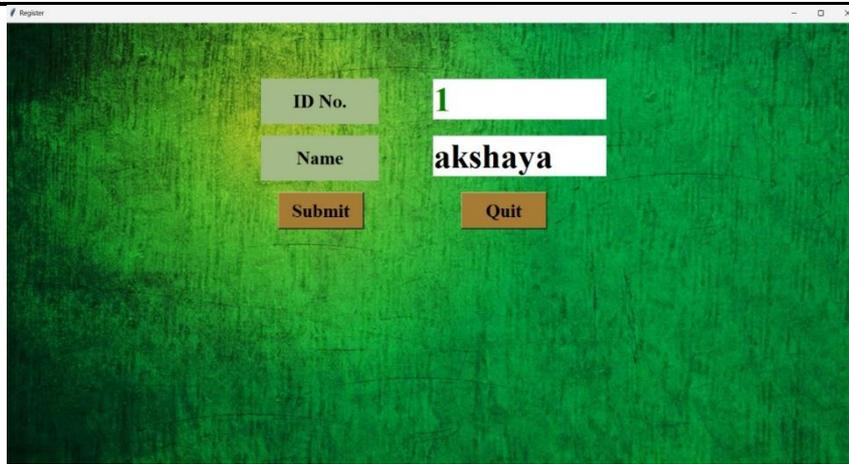


Fig.3 Face recognition for Registration



Fig.4 Register Successful

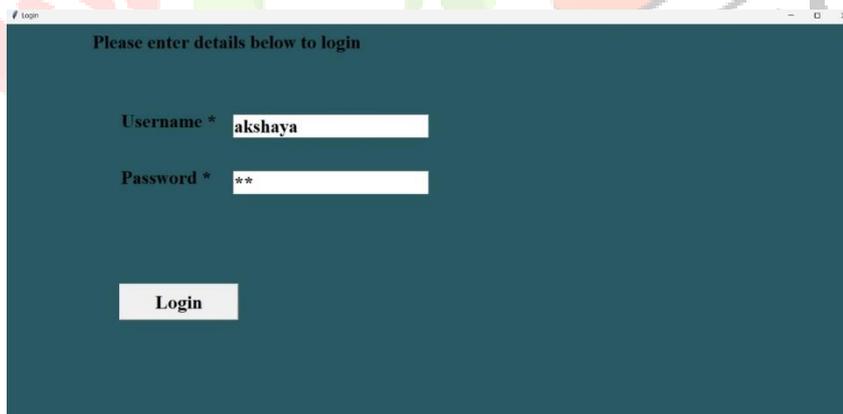


Fig.5 Member Login

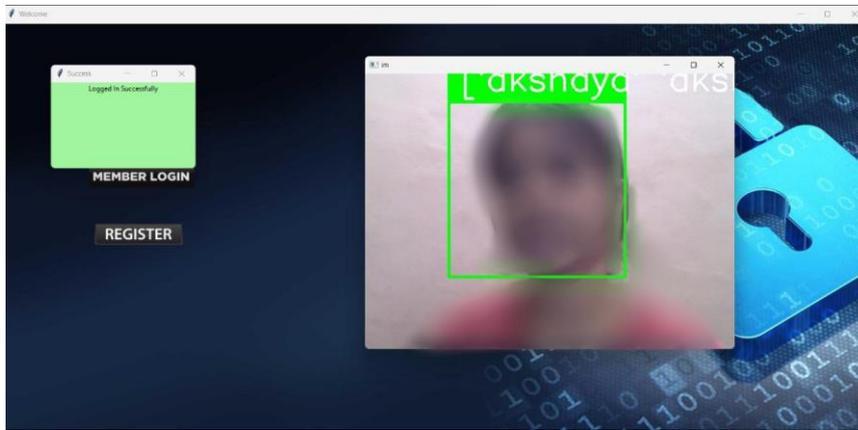


Fig.6 Member Login Successful

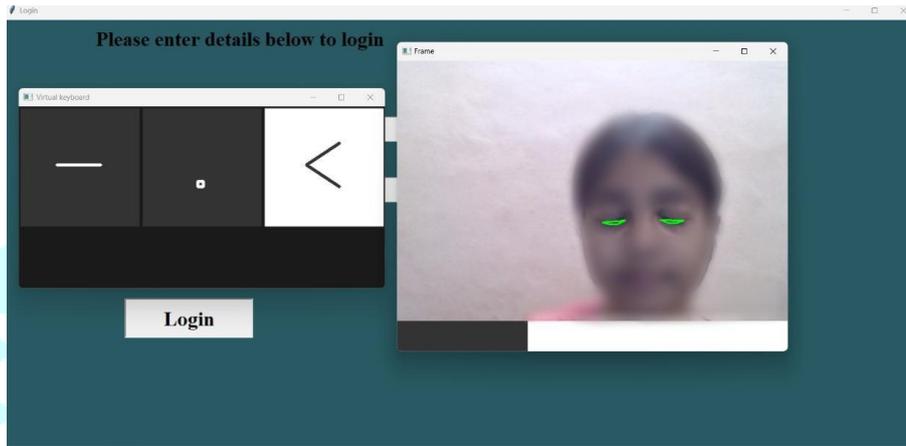


Fig.7 Password Entering

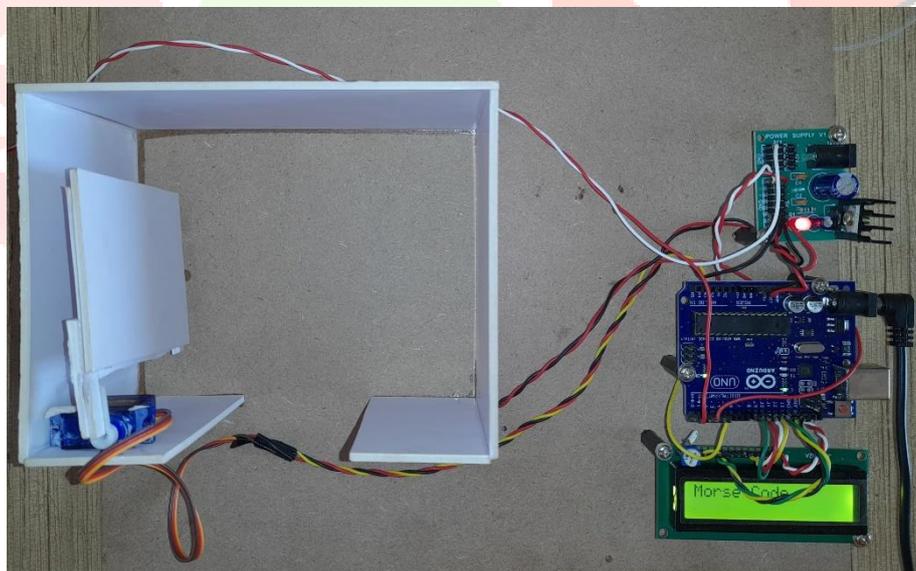


Fig.8 Project Model Top View

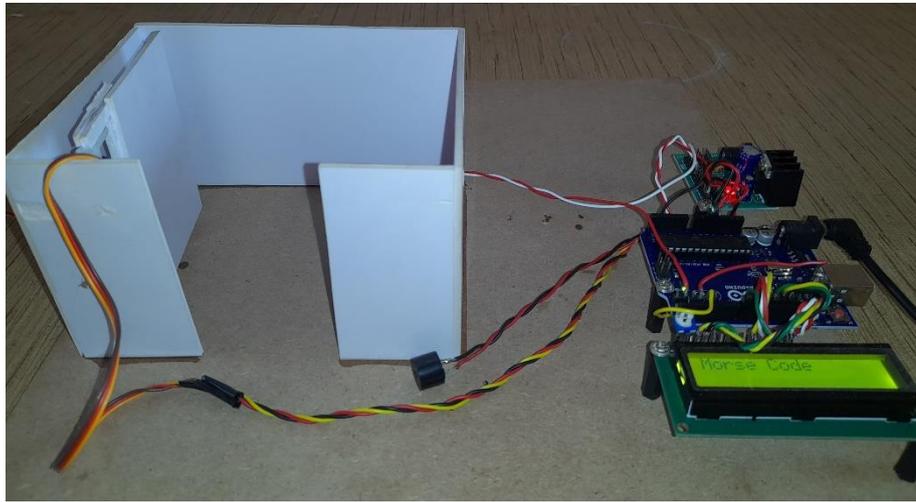


Fig.9 Project Model Side View

## XI. CONCLUSION

Our project provides two-factor authentication by combining gaze-based authentication with click-to-convert inputs like numbers or ASCII, enhancing security. It is designed to support disabled individuals, including children, elderly users, and those familiar with Morse code. For blind users, braille keyboards are compatible. In the future, we aim to incorporate face recognition, eliminating the need for password entry, and plan to deploy this model in government sectors for streamlined authentication.

## XII. REFERENCES

- [1] S. Muller, M. Dieck, and R. W. De Duncker, —Doubly fed induction generator systems for wind turbines, *IEEE Ind. Appl. Mag.*, vol.8, no.3, pp.26 – 33, May/Jun.2002.
- [2] D. Zhiand L. Xu, — Direct power control of DFIG with constants witching frequency and improved transient performance, *IEEE Trans. Energy Convers.* vol.22, no.2, pp.110–118, Mar.2007.
- [3] National Grid Transco, Appendix 1. (Feb.2004). Extracts from the grid code—Connection conditions [Online]. Available: <http://www.Nationalgrid.com>
- [4] IEEE Recommended Practices and Requirements for Harmonic Control in Electrical Power Systems, *IEEEStandard519-1992*,1993.
- [5] J. Hu, H. Xu, and Y. He, — Coordinated control of DFIG's RSC and GSC under generalized unbalanced and distorted grid voltage conditions, *IEEE Trans. Ind. Electron.*, vol. 60, no.7, pp.2808 – 2819, Jul.2013.
- [6] H. Xu, J. Hu, and Y. He, — Integrated modelling and enhanced control of DFIG under unbalanced and distorted grid voltage conditions, *IEEE Trans. Energy Convers.*, vol.27, no.3, pp.725–736, Sep.2012.
- [7] C. Liu, D. Xu, N. Zhu, F. Blaabjerg, and M. Chen, — DC-voltage fluctuation elimination through a DC-capacitor current control for DFIG converters under unbalanced grid voltage conditions, *IEEE Trans. Power Electron.*, vol.28, no.7, pp.3206–3218, Jul.2013.