Morse Code Based Secured Authentication System through Machine Learning

Mrs. Mamatha B N[1], Priyanka R[2], Varsha S[3], Shubhankar R[4]
[1] *Assistant Professor, Department of Information Science and Engineering, East West Institution of Technology, Visvesvaraya Technological University, Karnataka*
[234]*Student, Department of Information Science and Engineering, East West Institution of Technology, Visvesvaraya Technological University, Karnataka*

Abstract **- Data science is a multidisciplinary blend of data inference, algorithm development and technology in order to solve analytically complex problems. Data science is used by almost all the industries like instructive organizations, finance, medical services, business to deal with huge volumes of information. The pragmatic applications range from foreseeing stock development to anticipating disease; utilized in picture preparing to character acknowledgment, sound handling for discourse to message expectation. Since the majority of individuals on the planet are dealing with issues in the field of verification and security. The system provides a real time eye tracing for password authentication for people who authenticate themselves using Morse code. Advancement in the technology of authentication and authorization has be supported in the 21st century a lot as we know. Personal identification numbers (PIN) are widely used for user authentication and security since the late 90's. Since PIN numbers are easily crack able these days, people prefer to follow different approach. PIN validation with hands-off look-based PIN section procedures, then again, abandons no actual impressions and in this manner offers a safer secret word passage alternative. Gaze-based system for authentication alludes to discovering the eye area across consecutive picture frames and following the eye movements by plotting the eye center. Password authentication will be done using Morse code, where numbers will be represented in dots and dashes. This model presents a real-time application for gaze-based PIN entry with face recognition, and eye detection and tracking for PIN identification using a smart camera.**

Index Terms **- Machine learning, Authentication System, Eye Blink, Morse code, Personal Identification Numbers, Face Recognition.**

I.INTRODUCTION

Since the beginning, innovation has been the main thrust of progress. From portable types to television and the Internet, innovation has been embraced and is inculcated in our day-to-day lives. Inside the builds of progressed society, the immense compensations of technological developments have far outweighed the negatives.

With the further development in innovation, comes various manners by which we can improve our lives and make them more proficient. This prompted the presentation of numerous branches, one of them is Data Science. To put it in more straightforward words Data science is the investigation of where data comes from, what it addresses, and how it tends to be transformed into a significant asset in the formation of business. Mining a lot of organized and unstructured information to distinguish examples can help a business get control over costs, increment efficiencies, perceive new market openings, and increment the association's upper hand.

Machine Learning is a field of software engineering that regularly utilizes statistical procedures to enable PCs to "learn" (i.e., logically further develop execution on a particular task) with data, without being expressly programmed.

Machine Learning is utilized in the scope of computing tasks where planning and programming unequivocal calculations with great execution are troublesome or infeasible. Inside the field of data analytics, ML is a method that is used to devise complex models and algorithms that loan themselves to prediction. These analytical models permit specialists, information researchers, data scientists, and data analysts to "produce dependable, choices and results" and reveal "covered up experiences" through past experiences and relationships between the data.

II. EXISTING SYSTEM

Headway in the innovation of verification and approval has been upheld in the 21st century. Individual ID numbers (PINs) are generally utilized for client verification and security since the last part of the '90s. The current framework incorporates entering the secret key or the PIN through a QWERTY console or a numeric console which leads actual path when entered. The current look-based framework is carried out with the numeric PIN by utilizing the following of eye development recognition.

Disadvantages of Existing System

- The existing system projects lack of security considering that the shoulder surfing method for hacking can be easily implemented.
- Entry of the PIN numbers can be easily traced as it leaves physical footprints behind.
- Most of the system have only one layer of authentication.
- The existing gaze-based system is inconvenient as it is done by eye tracking and it maps the numbers directly on the screen.

III. PROPOSED SYSTEM

The model consists of a user interface and a back-end database. GUI is created such that the user can interact with the system. Tkinter or OpenCV is used to create the GUI. In the front-end, firstly, the user needs to register by giving in an ID and a name. Once this is completed, the process of Face Recognition takes place and this information is stored in the database associating it to your respective profile. Later, the user needs 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 help of a web camera, the PIN is taken as input in the form of Morse code. The project is achieved using Morse code encoded through eye blinks. Here, we discuss Morse code detection from eye blinks and decoding using OpenCV. In the backend, the entered PIN is checked with the stored PIN which was entered into the database by the user while registering. If the entered PIN is incorrect, the system exits the screen. If the entered PIN is correct, it displays successful authentication. If the user has forgotten his password, then he can use the keyword to authenticate and update the existing password with a new one.

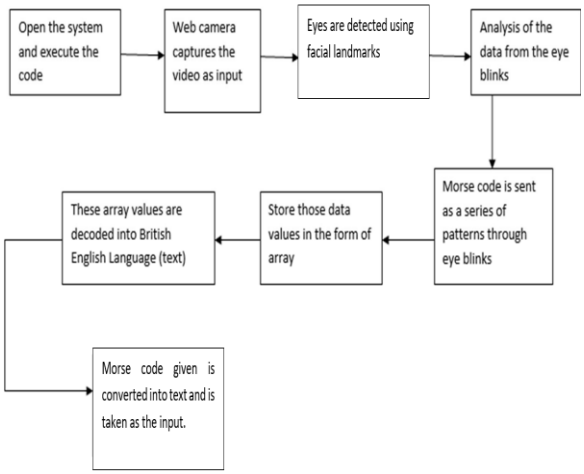

Figure 1: Proposed System

IV. ARCHITECTURE

System architecture is the conceptual model that defines the structure, behavior, and views of a system. A system architecture can consist of system components that will work together to implement the overall system.

The figure 2, represents the architecture or the basic design that is required for the implementation of the model. The model comprises a UI and a back-end database. GUI is made to such an extent that the user can communicate with the framework.

In the frontend firstly, there is a page for registration and login which is authenticated by Face Recognition. Following that there is a registration page where the user needs to enlist themself by giving a username of decision, a password (PIN), and a nickname. After enrollment, there is a login page. Later, with the assistance of a web camera, the PIN is taken as a contribution to the type of Morse code.

There is a backend, where the entered PIN is checked with the put-away PIN which was gone into the data set by the client while enrolling. On the off chance that the entered PIN isn't right, it leaves the screen. If the entered PIN is right, it shows fruitful verification. In the event that the client has failed to remember his secret word, he can utilize the catchphrase to verify and refresh the current secret phrase with another one.

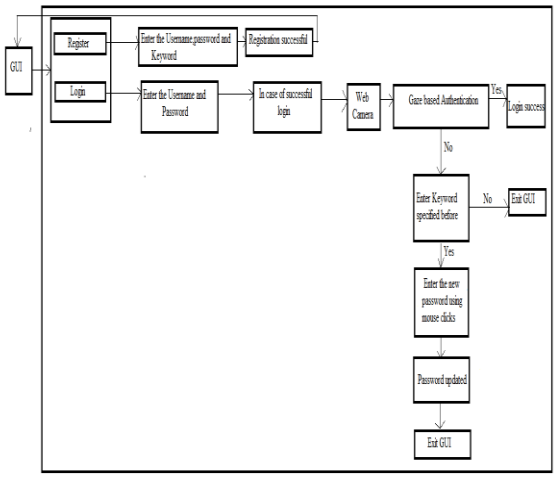

Figure 2: System Architecture

V. METHODOLOGY

A. Registration

This module consists the first page that the user sees to enter his credentials. The entered credentials (Username, Password and keyword) will be stored in a separate text file. This module is represented by using front end implementation of the project.

B. Face Recognition

Once the user has registered, they can register their face in order to activate the authentication system using face recognition. This will be stored in the form of images in the back end and will be used to securely authenticate the system each time when a user wishes to log in. If this fails, a message displaying "Login Unsuccessful" is displayed and an email will be sent to the client's email address as well as the mobile number that consists of the image of the hacker who tried to get access to their system. Also an alarm is set on when the login is unsuccessful to alert the owners of this suspicious activity.

C. Login

In this module, the user or the admin enters his or her credential as per the details given in the register module. If the login is a success, the user can authenticate the password through gaze-based authentication. The conversion of eye blinks to Morse code is represented by using back-end implementation of the project.

D. Forgot Password

In this module, if the user forgets his password, he can create a new password by entering the keyword presented in register module. This new password is also set using the morse code via mouse clicks. A single left click represents a dot. A double left click represents a dash. A single right click is to input next character and a double right click is to input next number.

VI. ALGORITHMS

a) Haar Cascade - Haar Cascade is a machine learning object detection algorithm used to identify objects in an image or video. It is a machine learning based methodology where a cascade function is prepared from a ton of positive and negative pictures. It is then used to recognize objects in different pictures. It is well known for being able to identify almost any object. First step is to collect the Haar Features. A Haar feature considers adjacent rectangle regions at a particular point in a detection window, and it sums up the pixel intensities in each of those regions and it calculates the difference between these sums.

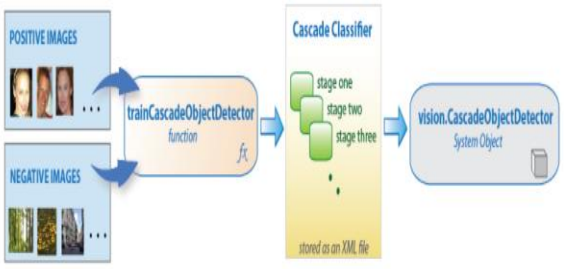

Figure 3: Haar Cascade Algorithm

b) Facial Landmark algorithm - Face Detection Technology is utilized in applications to recognize faces from advanced pictures and recordings. Likewise, simply identifying the face will be of no use. We need more data about the face, for example regardless of whether an individual grin, chuckles, or if dimples are seen while grinning, and so forth. To put it plainly, facial expressions also give us data. To get more data about the face, we take the assistance of Facial Landmarks.

What are Facial Landmarks?

Facial Landmarks are utilized for limiting and addressing notable areas or facial parts of the individual's face, for example,

- Eyebrows
- Eyes
- Jaws
- Nose
- Mouth and so forth.

Facial Landmark is a strategy that can be applied to applications like face arrangement, head poses estimation, face swapping, blink detection, face alignment, drowsiness detection, etc. In this setting of facial landmarks, our crucial point is to identify facial constructions on the individual's face utilizing a technique called shape detection. Facial landmarks Location has 2 steps:

- To detect the key facial structures on the person's face.
- To localize the face in the image.

The facial landmarks identifier which is pre-prepared inside the dlib library of python for identifying landmarks is utilized to appraise the area of 68 points or (x, y) coordinates which guide the facial designs. These indexes of 68 coordinates or points can be effortlessly imagined on the picture underneath:

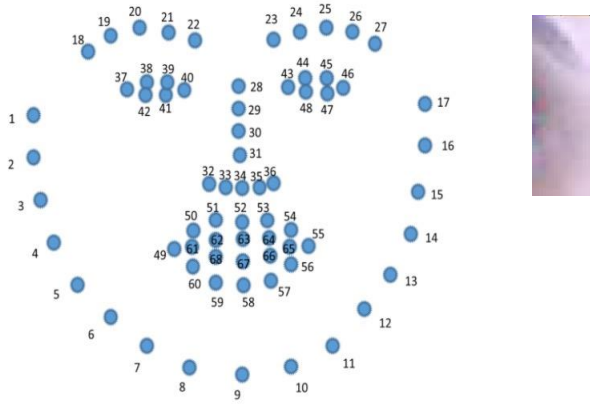

Figure 4: Facial Landmark Algorithm

The Locations of the Eye Parts are as follows:

- The left eye is accessed with points [43,47].
- The right eye is accessed using points [37, 41].

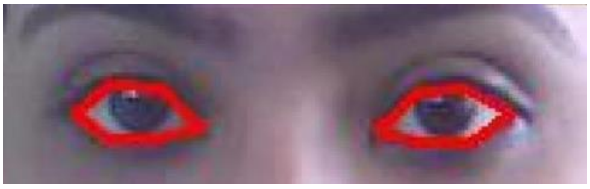

Figure 5: Location of Eye points

VII. ADVANTAGES

- Less reliability on the physical devices like mouse or keyboard.
- Highly efficient.
- System can be extended to eye recognition-based system where with eye movements control of system can be done. This will be efficient for handicapped people.
- Less strain on fingers.

VIII. RESULTS

The project basically provides two factor authentication. Two factor authentication is basically providing two layers of security to protect an account or system. Here, the user is making use of gaze-based authentication and mouse click in order to convert numbers or alphabets into source code thereby increasing the security. This model presents a real-time application for gaze-based PIN entry, and eye detection and tracking for PIN identification using a smart camera.

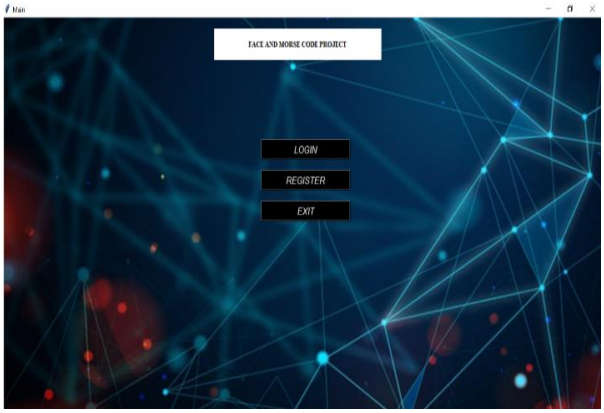

Figure 6: Main Page

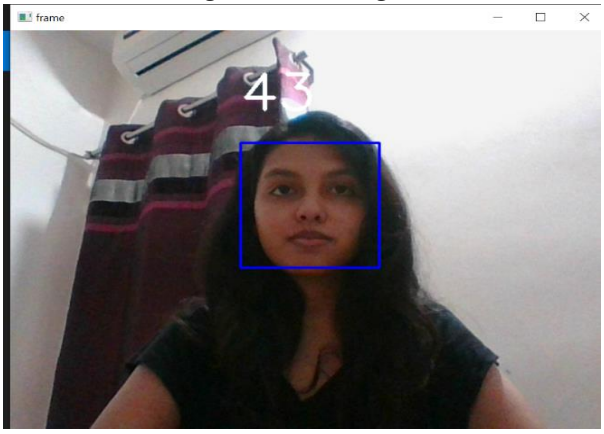

Figure 7: Face Recognition Frame

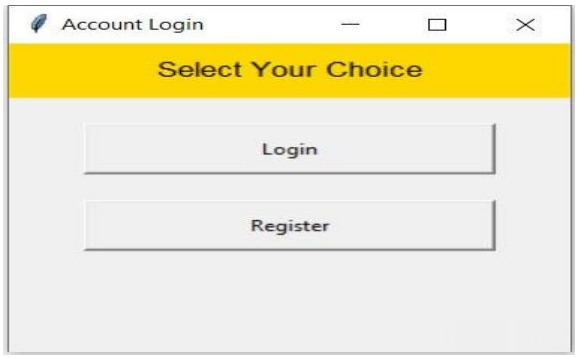

Figure 8: Account Login Page

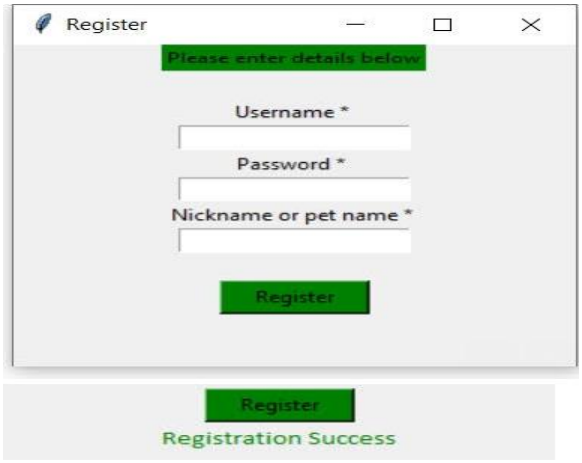

Figure 9: Registration Page

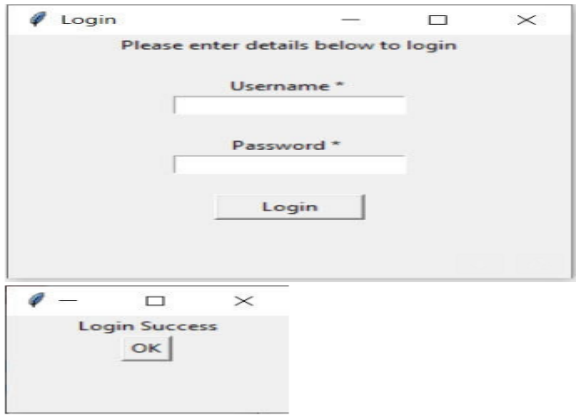

Figure 10: Login Page

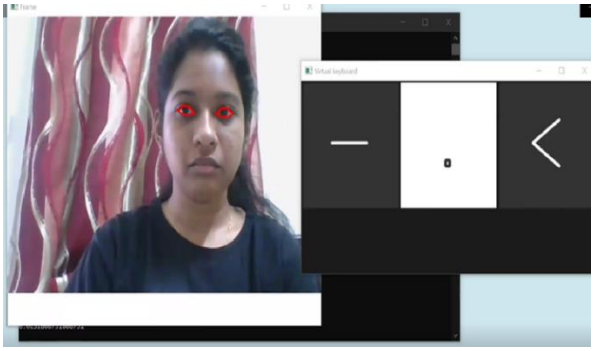

Figure 11: Morse Code password input frame

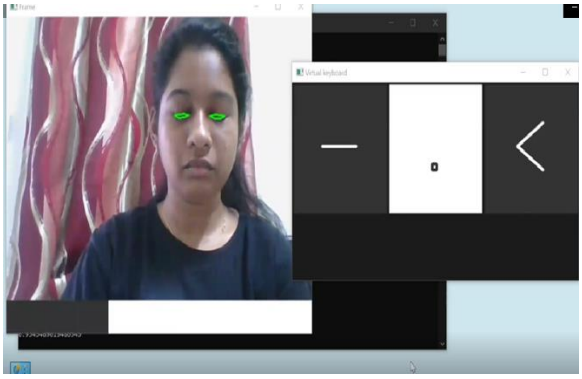

Figure 12: Character input accepted frame

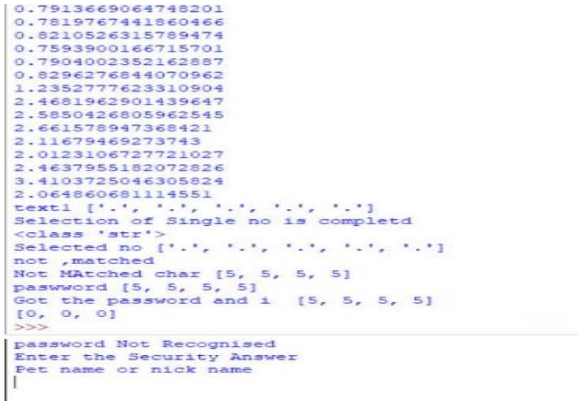

Figure 13: Security Question Page

Figure 14: Password reset page using Mouse Clicks

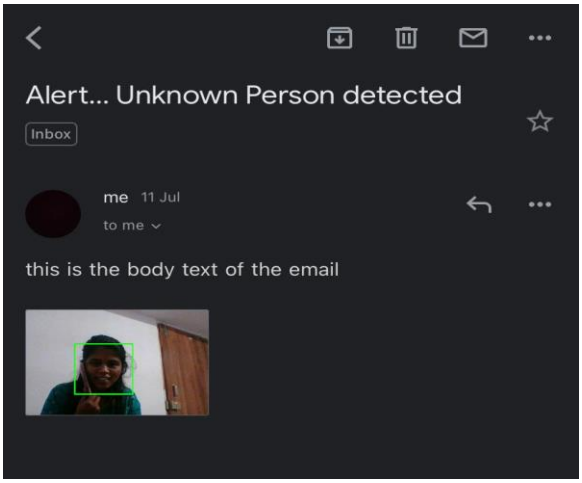

Figure 15: Warning email

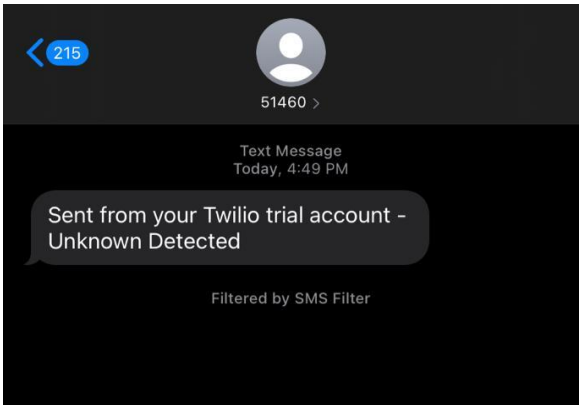

Figure 16: Warning message

VIII. CONCLUSION

Two-factor authentication is basically providing a two-layer of security to protect an account or system. Here we are making use of gaze-based authentication and mouse click in order to convert numbers or alphabets into source code thereby increasing the security. This project is also helpful for disabled people in order to authenticate. People from kids to old people can make use of this model who has basic knowledge of morse code. For blind people, there are keyboards with braille dots present on each button. Concerning the future enhancement, can implement facial recognition for each user, there will be no need to enter the password at all. Also trying to deploy this model in government sectors, with a fewer number of steps required for authentication.

REFERENCES

[1] S. Muller, M. Deicke, and R. W. De Doncker, "Doubly fed induction generator systems for wind turbines," IEEE Ind. Appl. Mag., vol. 8, no. 3, pp. 26–33, May/Jun. 2002.

[2] D. Zhi and L. Xu, "Direct power control of DFIG with constant switching 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, IEEE Standard 519-1992, 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 modeling 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.

[8] Sarangi, P., Grassi, V., Kumar, V., Okamoto, J.:"Integrating Human Input with autonomous behaviours on an Intelligent Wheelchair Platform", Journal of IEEE Intelligent System, 22, 2, 33-41, [2007].

[9] Matt Bailey, ET. Al, "Development of Vision Based Navigation for a Robotic Wheelchair", in Proceedings of 2007 IEEE 10th International conference on rehabilitation robotics.

[10] Shafi. M, Chung. P. W. H:"A Hybrid Method for Eyes Detection in Facial Images", International Journal of Electrical, Computer, and Systems Engineering, 231-236, [2009].

[11] Automation of wheelchair using ultrasonic and body kinematics, Preethika Britto, Indumathi. J, Sudesh Sivarasu, Lazar Mathew, CSIO Chandigarh, INDIA, 19-20 March 2010.

[12] Poonam S. Gajwani & Sharda A. Chhabria, "Eye Motion Tracking for Wheelchair Control", International journal of information technology and knowledge management, Dec 2010.

[13] Eye Controlled Wheelchair Using EOG, Alex Dev, Horizon C Chacko and Roshan Varghese, International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April 2012.