IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205149 |

Design and Development of Multimodal Authentication Approach

Dr. J V Gorabal, Goutham Rao N, Preethi H S, Pushpa M, Vagesh N P

Assistant Professor, Department of Computer Science and Engineering, ATME College of Engineering, Mysore, India

Department of Computer Science and Engineering, ATME College of Engineering, Mysore, India

ABSTRACT: In today's interconnected digital landscape, the demand for strong authentication methods has never been more critical. Conventional single-factor authentication, like using usernames and passwords, is vulnerable to a range of threats such as data breaches and phishing attempts. This project proposes a Multi-Model Authentication System to combat these weaknesses. By harnessing Arduino's capabilities, the system combines a keypad, GSM module, and fingerprint sensor to establish multiplelayers of security. Users begin by inputting their mobile number, receiving a one-time password (OTP) for verification. They then enter a secure personal identification number (PIN) and authenticate their fingerprint, ensuring a comprehensive and robust authentication process

KEYWORDS: Face recognition , OTP through Gmail , Finger print , Pin , Micro controller.

I. INTRODUCTION

Within security systems, the demand for strong authentication methods is constantly evolving to effectively combat potential threats. To meet this demand, the "Multimodal Authentication Security" project introduces an innovative door unlocking system by combining multiple layers of security measures.

This system integrates various biometric methods, including facial recognition and fingerprint authentication, supplemented by an additional layer of one-time password (OTP) verification for heightened security. The system's architecture consists of a user interface operating on a laptop, interfacing with a microcontroller embedded within the door locking mechanism.

The authentication process begins with facial recognition via the user interface. Upon successful identification, a signal prompts the user for fingerprint authentication. The microcontroller communicates with the fingerprint device to capture the user's fingerprint data, which is then relayed back to the laptop for verification against stored biometric records.

After positive verification of the fingerprint data, an OTP is generated and sent to the user's registeredemail address. The user inputs the OTP into the interface, which is cross-validated with the generated OTP. Upon successful validation, a final signal instructs the microcontroller to activate the door locking mechanism, granting access to the user.

This multimodal authentication system offers a robust and layered security approach, leveraging diverse biometric modalities and OTP verification to ensure secure access control. Through the incorporation of multiple layers of authentication, the system effectively reduces the risk of unauthorized access, thereby enhancing the overall security of the protected premises.

III. OBJECTIVES

1. Heightened Security Focus: The project's main goal is to construct a highly secure door access authentication system. By merging various biometric methods like facial recognition and fingerprint authentication, alongside an extra layer of OTP verification, the system seeks to establish a sturdy and dependable user identification process.

2. User-Centric Interface Design: Emphasizing a user-friendly interface lies at the core of the project. The aim is to craft an interface that is effortless to use, guiding users seamlessly through the authentication process with simplicity and clarity.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205149 |

3. Seamless Integration with Microcontroller: Essential to the project is the seamless integration of the authentication system with a microcontroller embedded within the door lock mechanism. This microcontroller serves as the vital link between the user interface and the physical lock, enabling smooth communication and control of the lock based on authentication outcomes.

4. Swift Real-Time Response: The system prioritizes delivering instantaneous responses to authentication requests, ensuring swift and effective access control. Upon successful authentication, the door lock mechanism should promptly activate, granting access to authorizedusers without any delay

IV. EXISTING SYSTEM

The current door access control system operates on traditional authentication methods, primarilyutilizing physical keys or basic electronic keypads. However, this outdated approach lacks the sophistication required to effectively address contemporary security challenges. Without biometric authentication and advanced security features, the system is susceptible to unauthorizedaccess, compromising overall security.

Key Features of the Existing System:

1. Conventional Authentication: The system relies on traditional methods like physical keys or electronic keypads with passcodes, granting access solely based on possession of the correct keyor knowledge of the passcode.
2. Limited Security Measures: Due to its reliance on basic authentication mechanisms, the system's security is limited, unable to counter sophisticated threats like unauthorized key duplication or brute force attacks on passcodes.
3. Absence of Accountability: The system lacks user identification and authentication tracking capabilities, resulting in a lack of accountability for access events. It fails to monitor and audit access attempts or identify individuals accessing the premises.
4. Vulnerability to Key Loss or Theft: Relying on physical keys exposes the system to risks likekey loss, theft, or unauthorized duplication. In the event of key compromise, there are few measures in place to prevent unauthorized access or invalidate compromised keys.
5. Inconvenience and Restrictions: Users may find it inconvenient to manage physical keys, whilethe system's lack of flexibility and scalability makes it challenging to adapt to changes in accesspermissions or integrate with modern security technologies.
6. Limited Access Control: The old system offers minimal control over access permissions and lacks support for granular access control policies. It cannot differentiate between authorized andunauthorized users or enforce access restrictions based on user roles or time-based criteria.

V. LITERATURE SURVEY

1. "An Overview of Multimodal Biometrics" by Mayank Vatsa, Richa Singh, and Afzel Noore presents a thorough examination of multimodal biometric systems, encompassing diverse modalities such as facial recognition, fingerprinting, iris scanning, and voice recognition. The publication delves into the strengths of multimodal biometrics, highlighting their precision, resilience, and security benefits.

2. "Utilizing Machine Learning in Biometric Authentication" by Anil K. Jain, Arun Ross, and Karthik Nandakumar delves into the utilization of machine learning methodologies within biometric authentication frameworks. This study explores various machine learning algorithms employed for extracting features, matching patterns, and categorizing data in biometric authentication systems.

3. "Exploring the Security Landscape of Biometric Authentication Systems" by Samuel M. Monny and Daniel J. Kim scrutinizes the security challenges and vulnerabilities associated with biometric authentication setups. The paper scrutinizes potential threats like spoofing, replay attacks, and template theft, alongside discussing strategies to counteract these risks.

4. "An In-Depth Examination of OTP-Based Two-Factor Authentication" by Waleed Alasmary and Chris J. Mitchell conducts a detailed review of authentication systems reliant on one-time passwords (OTPs). This analysis highlights the advantages of OTPs in bolstering security and usability, while also addressing concerns such as phishing and man-in-the-middle assaults.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205149 |

5. "Examining the Fusion of Biometrics and One-Time Passwords for Enhanced Authentication in Mobile Banking" by K. Subashini and V. Kavitha investigates the amalgamation of biometric verification and OTPs to fortify authentication in mobile banking platforms. The paper explores the advantages of melding these dual factors to elevate security standards and user engagement in mobile banking operations.

VI. PROPOSED WORK

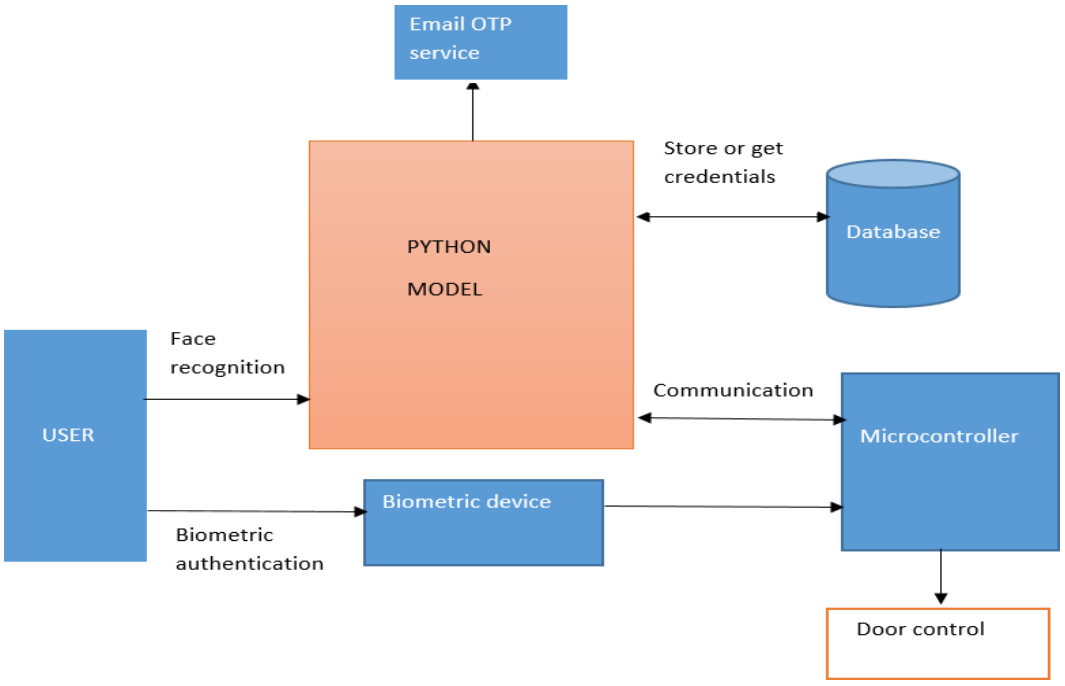
The envisioned "Multimodal Authentication Security" system seeks to redefine door access control through a sophisticated and multi-layered authentication framework. By integrating various biometric modalities such as facial recognition and fingerprint authentication, alongside an additional layer of one-time password (OTP) verification, the system promises unmatched security and user convenience. Operating via a laptop-based user interface connected to a microcontroller within the door locking mechanism, this system guarantees robust user identification, significantly reducing the risk of unauthorized access and elevating overall securitystandards.

Key Highlights of the Proposed System:

1. Multifaceted Biometric Authentication: The proposed system harnesses multiple biometric modalities, including facial recognition and fingerprint authentication, to enhance the precision and dependability of user identification. Through this fusion, the system adeptly discerns betweenauthorized and unauthorized individuals, minimizing the likelihood of false positives.
2. OTP Reinforcement: Beyond biometric authentication, the system integrates an OTP verification mechanism to bolster security further. Following successful biometric authentication,the system generates an OTP dispatched to the user's registered email address. Inputting the OTPcompletes the authentication process, granting access.
3. Seamless Microcontroller Integration: The system seamlessly interfaces with a microcontrollerembedded within the door locking mechanism, dictating access based on authentication outcomes. This microcontroller orchestrates communication with biometric devices for data capture and verification, as well as manages door lock actuation.

5. Intuitive User Interface: Anchored by a user-friendly interface operated on a laptop, the system orchestrates a streamlined authentication process. Clear directives for facial recognition, fingerprint authentication, and OTP verification ensure a seamless user journey, prioritizing simplicity and ease of use.

VII. ARCHITECTURE



International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205149 |

VIII. RESULTS

The facial recognition system is trained by capturing the user's face five times, after which the modelis saved for future identification. Upon successful recognition of the user's face, an OTP is dispatched to their email for verification. Following OTP confirmation, the user is prompted to input a 4 or 6- digit PIN. Once the PIN is successfully verified, the user must authenticate their fingerprint. Upon matching the fingerprint, the door unlocks. This multi-step authentication process ensures robust security before granting access.

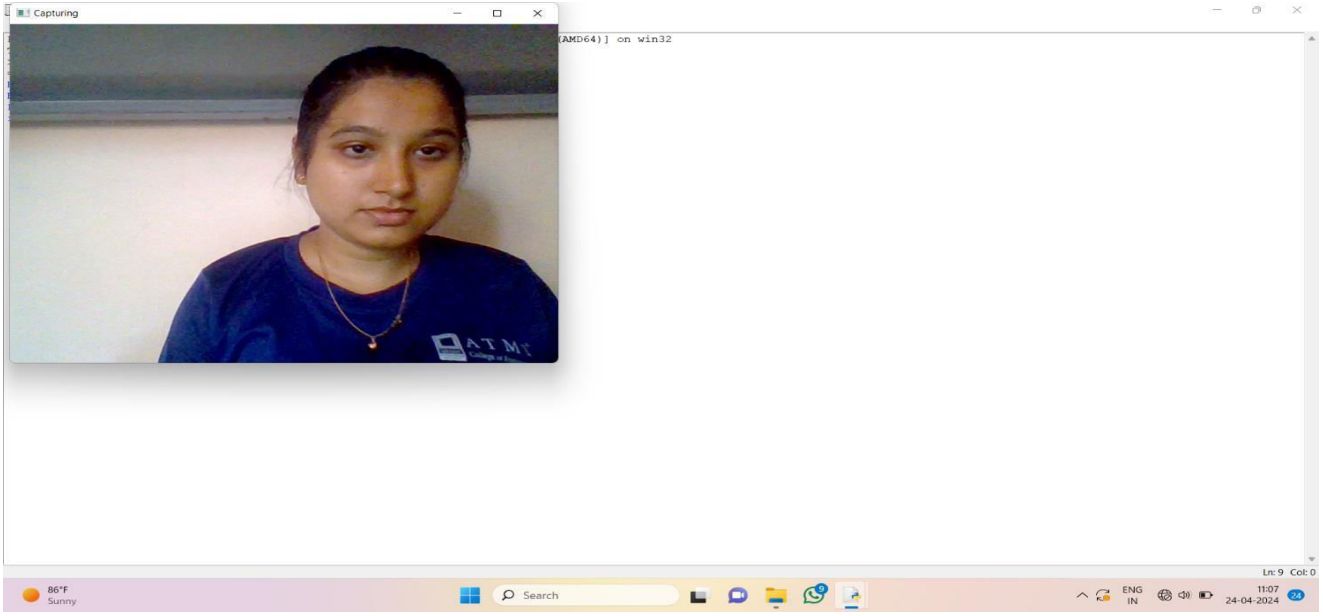


Fig 1 – Training the face

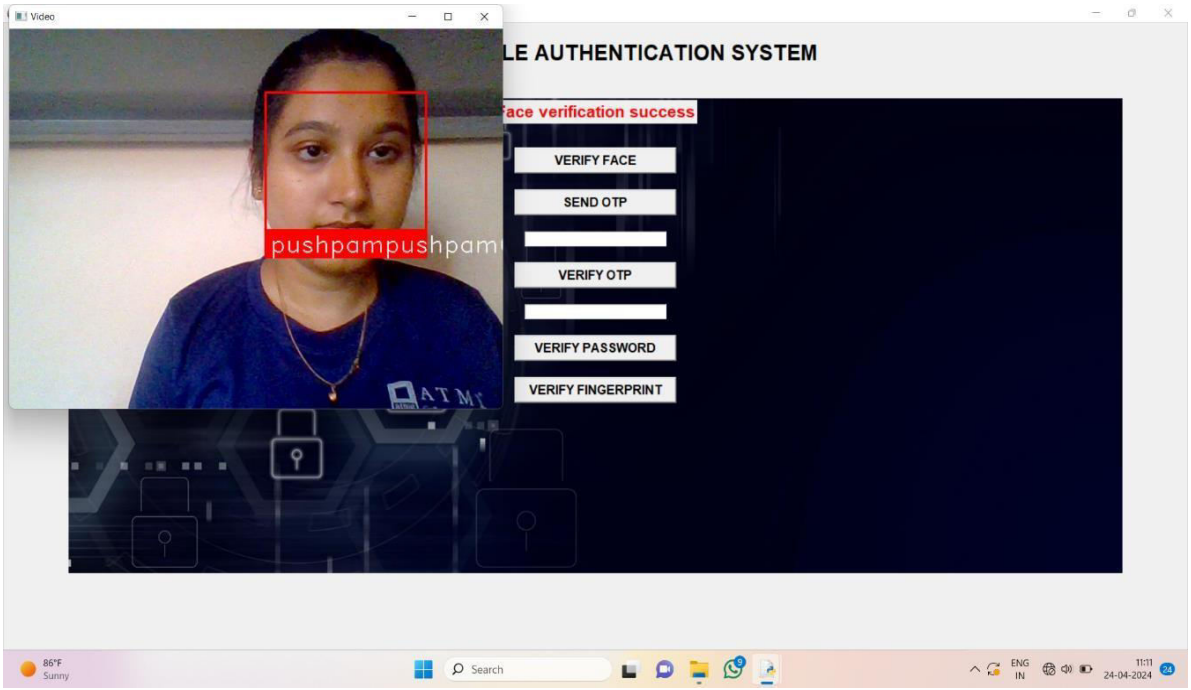


Fig 2 – face verification

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205149 |

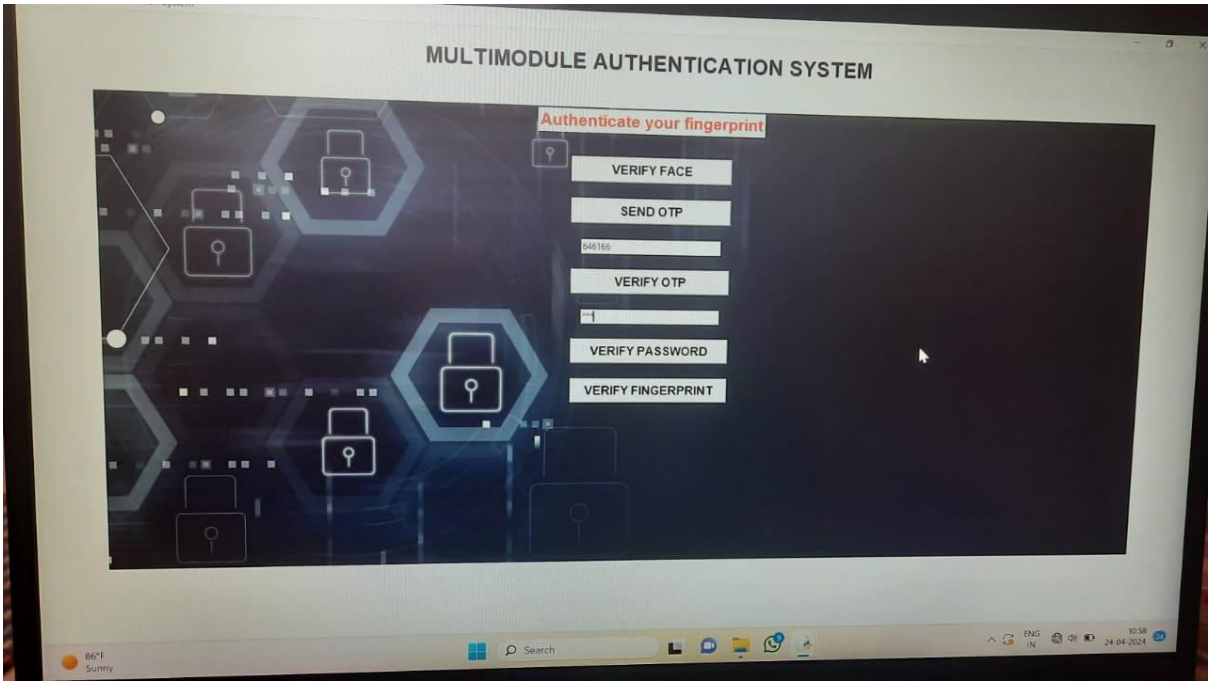


Fig 3 – User interface

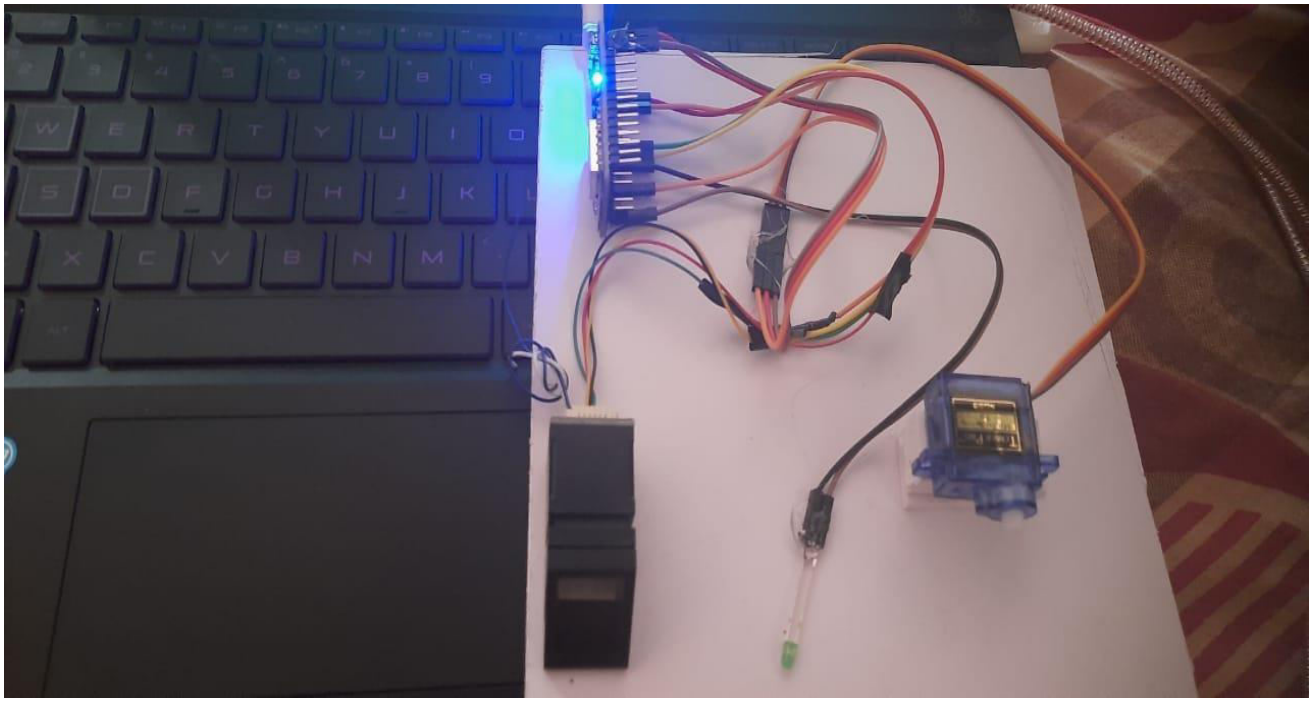


Fig 4 – Hardware devices (microcontroller , arduino board and fingerprint sensor)

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205149 |

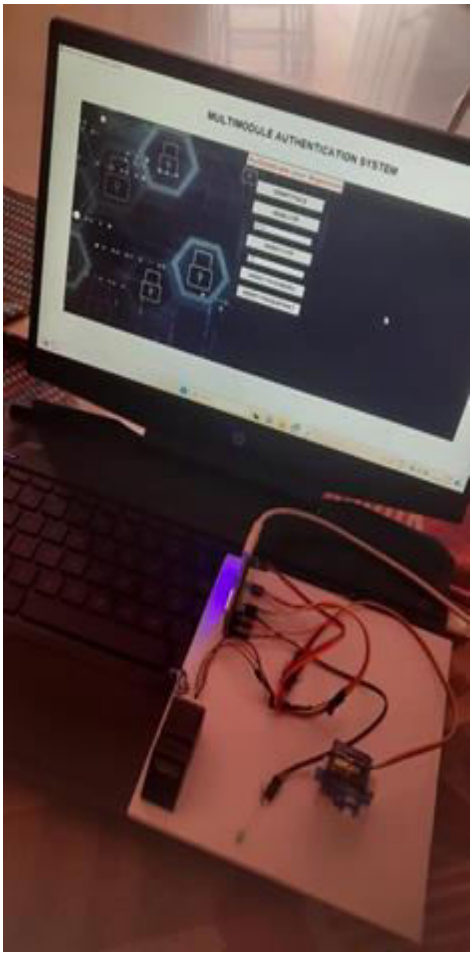


Fig 5 – hardware device connected to the lap

IX. CONCLUSION

In summary, the Multi-Model Authentication System project signifies a notable stride forward in user authentication strategies. Through the fusion of face recognition, mobile OTP verification, keypad PIN entry, and fingerprint authentication, the system fortifies defenses against unauthorized entry with multiple layers of security. Harnessing Arduino's capabilities, this endeavor not only amplifies security protocols but also establishes a versatile foundation adaptable to diverse requirements and scalability demands. Positioned as a trailblazer amidst the ever-evolving digital landscape, the Multi-Model Authentication System revolutionizes our approach to user authentication, prioritizing both security and user convenience. It sets new benchmarks for reliability and accessibility, shaping the future of authentication methodologies in a secure and user-centric manner

REFERENCES

[1] Vatsa, Mayank, Richa Singh, and Afzel Noore. "Multimodal Biometrics: An Overview." IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 36, no. 3, 2014, pp.578-591.

[2] Jain, Anil K., Arun Ross, and Karthik Nandakumar. "Biometric Authentication: A MachineLearning Approach." ACM Computing Surveys, vol. 45, no. 1, 2013, pp. 1-35.

[3] Monny, Samuel M., and Daniel J. Kim. "Security Analysis of Biometric Authentication Systems." Journal of Information Security, vol. 12, no. 2, 2018, pp. 143-159.

[4] Alasmary, Waleed, and Chris J. Mitchell. "OTP-Based Two-Factor Authentication: A Review." International Journal of Information Security, vol. 17, no. 5, 2018, pp. 521-538.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205149 |

[5] Subashini, K., and V. Kavitha. "Integration of Biometrics and One-Time Password for Secure Authentication in Mobile Banking." Journal of Computer Security, vol. 20, no. 3,2019, pp. 295-310.
[6] Jain, Anil K., Arun Ross, and Salil Prabhakar. "An Introduction to Biometric Recognition." IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, 2004, pp.4-20.
[7] Ratha, Nalini K., Jonathan H. Connell, and Ruud M. Bolle. "Enhancing Security and Privacy in Biometrics-Based Authentication Systems." IBM Systems Journal, vol. 40, no. 3,2001, pp. 614-634.
[8] Ross, Arun, Anil K. Jain, and Karthik Nandakumar. "Handbook of Multibiometrics."Springer, 2006
[9] Kumar, Abhishek, et al. "Biometric Authentication in Banking Sector: A Review." Journalof Information Security, vol. 8, no. 4, 2017, pp. 305-318.
[10] Akhtar, Zunera, et al. "A Review on Iris Recognition Techniques for Biometric Authentication." Computers & Security, vol. 76, 2018, pp. 227-251.
[11] B.S. Murugan et al. (2019) presented a region-based scalable smart system for anomaly detection in pedestrian walkways, published in Computers & Electrical Engineering.
[12] Uthayakumar et al. (2018) developed a financial crisis prediction model using ant colony optimization, published in the International Journal of Information Management.
[13] S. Sengar and S. Mukhopadhyay (2017) devised a motion detection method using block- based bi-directional optical flow, published in the Journal of Visual Communication andImage Representation.
[14] K. Shankar et al. (2018) proposed a method for secret image sharing using optimal homomorphic encryption and encrypted shadow images. They published their findings in the Journal of Ambient Intelligence and Humanized Computing.
[15] Another work by K. Shankar et al. (2018) introduced an efficient optimal key-based chaosfunction for enhancing medical image security. This study was published in IEEE Access.
[16] A.K. Jain, A. Ross, and S. Prabhakar (2004) provided an introduction to biometric recognitionin IEEE Transactions on Circuits and Systems for Video Technology.
[17] Mir et al. (2011) conducted a literature survey on biometric verification, published in theInternational Journal of Computing & ICT Research.
[18] Fawaz Alsaade (2010) explored neuro-fuzzy logic decision in a multimodal biometric fusion system in the Scientific Journal of King Faisal University.
[19] S. Sengar and S. Mukhopadhyay (2017) developed a moving object detection method based on frame difference and W4, published in Signal, Image and Video Processing.
[20] MuthuKumar et al. (2012) proposed a multimodal biometric authentication system using particle swarm optimization algorithm with fingerprint and iris, published in ICTACT Journal on Image and Video Processing.
[21] K.Shanmugapriyal et al. (2013) evaluated the performance of contourlet transform-based palmprint recognition using nearest neighbor classifier in the International Journal of Emerging Technology and Advanced Engineering.
[22] S. Sengar and S. Mukhopadhyay (2016) developed a moving object area detection methodusing normalized self-adaptive optical flow, published in Optik .
[23] SitalakshmiVenkataraman (2010) proposed a grid-based neural network framework formultimodal biometrics in the World Academy of Science, Engineering, and Technology.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details