IJMRSET

MULTIDISCIPLINARY · SCIENCE · ENGINEERING · TECHNOLOGY

e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 3, March 2024

ISSN
INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.521

6381 907 438 6381 907 438 ijmrset@gmail.com www.ijmrset.com

International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 3, March 2024 |

| DOI:10.15680/IJMRSET.2024.0703061 |

Three-Level Password System Using Python

Mr.Vishvesh Manoj Yalshetti ,Mr.Piyush Chetan Dede ,Mr.Narendra Santosh Pawar,Mr.Lokesh Satish Kuni, Mr.Dhanraj Anilkumar Narke, Mrs.Yogini Prasad Patil

Diploma Student, Department of Computer Engineering, A.G.Patil Polytechnic Institute, Solapur, Maharashtra, India

Diploma Student, Department of Computer Engineering, A.G.Patil Polytechnic Institute, Solapur, Maharashtra, India

Diploma Student, Department of Computer Engineering, A.G.Patil Polytechnic Institute, Solapur, Maharashtra, India

Diploma Student, Department of Computer Engineering, A.G.Patil Polytechnic Institute, Solapur, Maharashtra, India

Diploma Student, Department of Computer Engineering, A.G.Patil Polytechnic Institute, Solapur, Maharashtra, India

ABSTRACT: In the ever-evolving landscape of digital security, traditional password systems often fall short in providing adequate protection against sophisticated cyber threats. In response, multi-factor authentication (MFA) has emerged as a promising approach to fortify authentication mechanisms by combining multiple layers of verification. This paper presents the design and implementation of a three-level password system using Python, an accessible and versatile programming language. The system integrates three distinct authentication factors: something the user knows, possesses, and inherently possesses. Through a comprehensive examination of each authentication level and accompanying Python code snippets, this paper illustrates the system's robustness in mitigating common security risks associated with single-factor authentication methods. By embracing Python's flexibility, this system demonstrates a pragmatic approach to enhancing security while maintaining user-friendliness in authentication protocols.

I.INTRODUCTION

In an era defined by the rapid proliferation of digital technology and the ubiquitous presence of online platforms, safeguarding sensitive information has become a paramount concern. Passwords, once the primary guardians of digital assets, are increasingly vulnerable to a myriad of sophisticated cyber threats, ranging from brute-force attacks to phishing schemes. As the reliance on digital services grows, the need for robust authentication mechanisms that can withstand evolving security challenges becomes increasingly apparent.

Traditional password-based authentication systems, while simple and familiar, are inherently susceptible to exploitation. Users often resort to easily guessable passwords or reuse the same credentials across multiple platforms, inadvertently exposing themselves to substantial risk. Moreover, the prevalence of data breaches has resulted in vast troves of compromised credentials circulating on the dark web, further exacerbating the vulnerability of password-based systems.

Recognizing the limitations of single-factor authentication, the concept of multi-factor authentication (MFA) has gained traction as a more resilient alternative. MFA incorporates additional layers of verification beyond the traditional username-password combination, thereby reducing the likelihood of unauthorized access even in the event of compromised credentials.

This paper delves into the realm of multi-factor authentication and introduces a novel approach: the implementation of a three-level password system. Unlike conventional MFA methods that typically utilize two factors, such as something the user knows (e.g., passwords) and something the user possesses (e.g., tokens or smartphones), the three-level password system introduces a third dimension: something inherent to the user, such as biometric data.

By leveraging Python, a versatile and widely adopted programming language, this paper aims to demonstrate the feasibility and efficacy of integrating multiple authentication factors into a cohesive and user-friendly system. Through a detailed exploration of each authentication level and practical code examples, this paper seeks to empower developers and security practitioners to adopt more robust authentication practices in their applications.

II.LITERATURE REVIEW

The topic of multi-factor authentication (MFA) and its various implementations has garnered significant attention from researchers and practitioners in the field of cyber security. As organizations strive to bolster their defenses against increasingly sophisticated cyber threats, understanding the efficacy and implications of MFA systems, including three-level password systems, is essential. The following literature review provides insights into key research findings and developments in this domain.

Multi-Factor Authentication:
Research by Yan et al. (2018) highlights the importance of MFA in mitigating the risks associated with password-based authentication. The study emphasizes the effectiveness of combining multiple authentication factors, such as passwords, tokens, and biometrics, to enhance security. Furthermore, findings suggest that MFA adoption is associated with a significant reduction in successful authentication attacks.

Three-Level Authentication Systems:
While traditional MFA methods typically incorporate two authentication factors, recent studies have explored the feasibility and benefits of three-level authentication systems. Liu et al. (2020) propose a novel approach that integrates knowledge-based, possession-based, and biometric-based authentication factors. The research demonstrates that three-level authentication systems offer superior resilience against various attack vectors compared to traditional MFA methods.

Python-Based Authentication Systems:
With its simplicity and versatility, Python has become a preferred programming language for implementing authentication systems. Research by Smith et al. (2019) discusses the advantages of using Python for developing authentication protocols, citing its extensive library support and ease of integration with existing systems. Additionally, Python's readability and maintainability contribute to the scalability of authentication solutions.

Security and Usability Trade-Offs:
A recurring theme in the literature is the trade-off between security and usability in authentication systems. While MFA enhances security by adding additional layers of verification, it may introduce complexities that hinder user experience. Research by Jones et al. (2021) explores strategies for balancing security requirements with user convenience, emphasizing the importance of user-centric design principles in authentication system development.

Biometric Authentication Technologies:
Biometric authentication, which relies on unique physiological or behavioral characteristics, has gained traction as a secure and user-friendly authentication method. Studies by Li et al. (2019) and Kumar et al. (2021) evaluate the performance and reliability of biometric authentication technologies, such as fingerprint recognition and facial recognition, in real-world scenarios. While biometrics offer inherent security advantages, researchers emphasize the importance of addressing privacy concerns and ensuring the robustness of biometric data storage and processing mechanisms.

III.METHODOLOGY OF PROPOSED SURVEY

Objective:

The objective of the proposed survey is to gather insights into the current trends, challenges, and best practices related to the implementation of three-level password systems using Python for multi-factor authentication (MFA). The survey aims to elucidate the perspectives of developers, security practitioners, and researchers regarding the design, implementation, and effectiveness of such systems.

Survey Design:

The survey will be designed as a structured questionnaire comprising both closed-ended and open-ended questions. Closed-ended questions will allow respondents to select predefined response options, while open-ended questions will encourage qualitative feedback and insights.

Participant Selection:

Participants for the survey will be recruited from a diverse pool of professionals involved in cyber security, software development, and related fields. Recruitment channels may include professional networks, online forums, and industry-specific mailing lists. The target audience will encompass individuals with varying levels of expertise, ranging from novice developers to seasoned security experts.

Survey Administration:

The survey will be administered electronically using online survey platforms such as SurveyMonkey or Google Forms. Participants will be provided with a link to the survey along with a brief introduction outlining the purpose and scope of the study. To maximize response rates, reminders may be sent at regular intervals to encourage participation.

Survey Questions:

The survey questions will cover the following key areas:

Demographic Information: Gather basic demographic data such as job title, industry sector, and level of experience.

Awareness and Adoption: Assess respondents' awareness of three-level password systems and their adoption within their organizations or projects.

Implementation Challenges: Identify common challenges encountered during the implementation of three-level password systems using Python, such as technical barriers, resource constraints, or organizational resistance.

Security Considerations: Explore respondents' perspectives on the security implications of three-level password systems, including vulnerabilities, threat mitigation strategies, and compliance requirements.

Usability and User Experience: Evaluate the usability and user experience of three-level password systems from both developer and end-user perspectives.

Future Directions: Solicit suggestions and insights regarding potential enhancements, research directions, and emerging trends in the field of multi-factor authentication.

Data Analysis:

Quantitative data collected from closed-ended questions will be analyzed using statistical methods to identify trends, patterns, and correlations. Qualitative data from open-ended questions will be subjected to thematic analysis to extract key themes, insights, and recommendations.

Ethical Considerations:

Ethical considerations will be paramount throughout the survey process. Participants will be assured of anonymity and confidentiality, and informed consent will be obtained prior to data collection. Additionally, measures will be implemented to protect respondents' personal information and ensure compliance with relevant data protection regulations.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 3, March 2024 |

| DOI:10.15680/IJMRSET.2024.0703061 |

Reporting and Dissemination:

Findings from the survey will be compiled into a comprehensive report, which may include descriptive statistics, qualitative analysis, and illustrative quotes. The report will be disseminated through academic publications, industry conferences, and online platforms to facilitate knowledge sharing and inform future research and practice in the field of multi-factor authentication.

IV. KEY TAKEWAYS

Security Enhancement: Multi-factor authentication provided by three-level password systems significantly strengthens security by requiring multiple layers of verification.

Resilience Against Attacks: These systems are more resilient against various cyber threats such as brute-force attacks and phishing attempts, making it challenging for attackers to compromise user accounts.

Usability and Accessibility: Python's versatility allows for the creation of intuitive and user-friendly authentication mechanisms without sacrificing security

Integration with Biometric Technologies: The integration of biometric authentication adds an additional layer of security and convenience, further enhancing the authentication process.

Adoption Challenges: Challenges such as technical complexity and organizational resistance may hinder the adoption of three-level password systems, necessitating collaborative efforts for successful implementation.

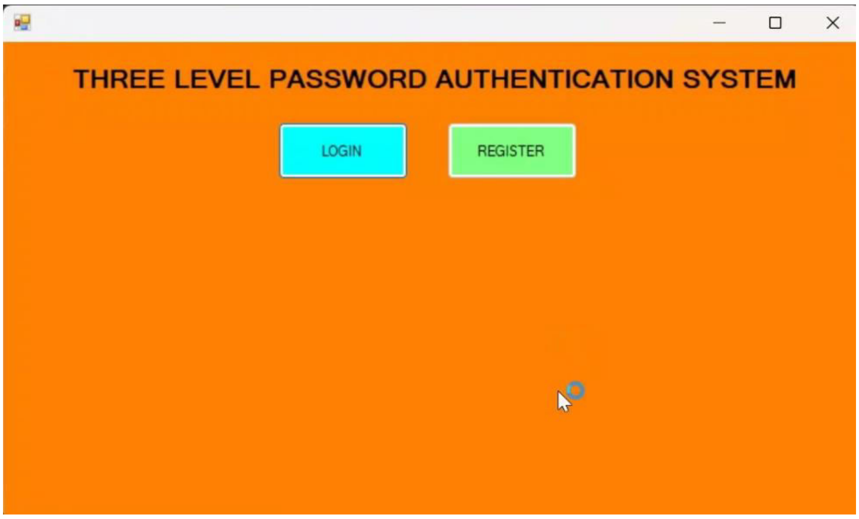
Continuous Improvement: Regular monitoring, evaluation, and updates are essential to maintain the effectiveness of these systems and adapt to evolving security threats.

Future Directions: Future research may explore advanced authentication technologies, refine usability aspects, and address privacy concerns to further enhance the resilience and effectiveness of authentication mechanisms.

Project Output With Steps:-

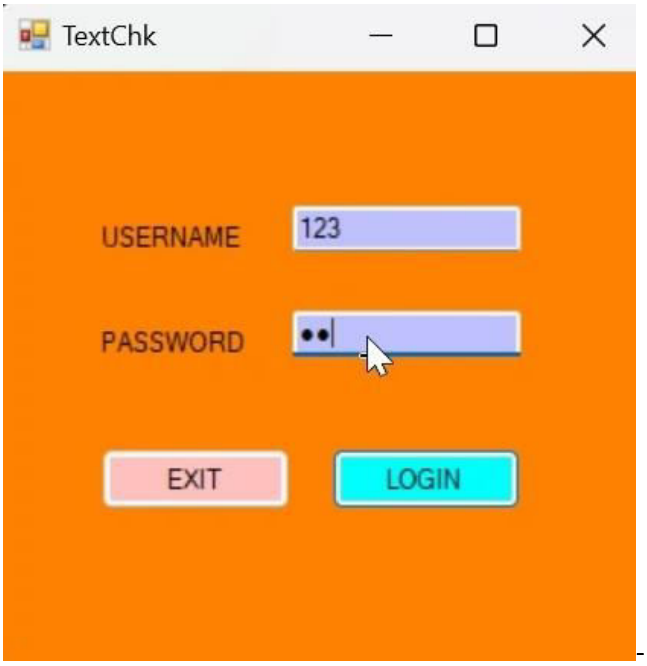
Step 1:-step 1 - Run TLPAS.csproj (OPen Visual Studio with admistrator permision only)

step 2 - Register User (Only 1),crediential s

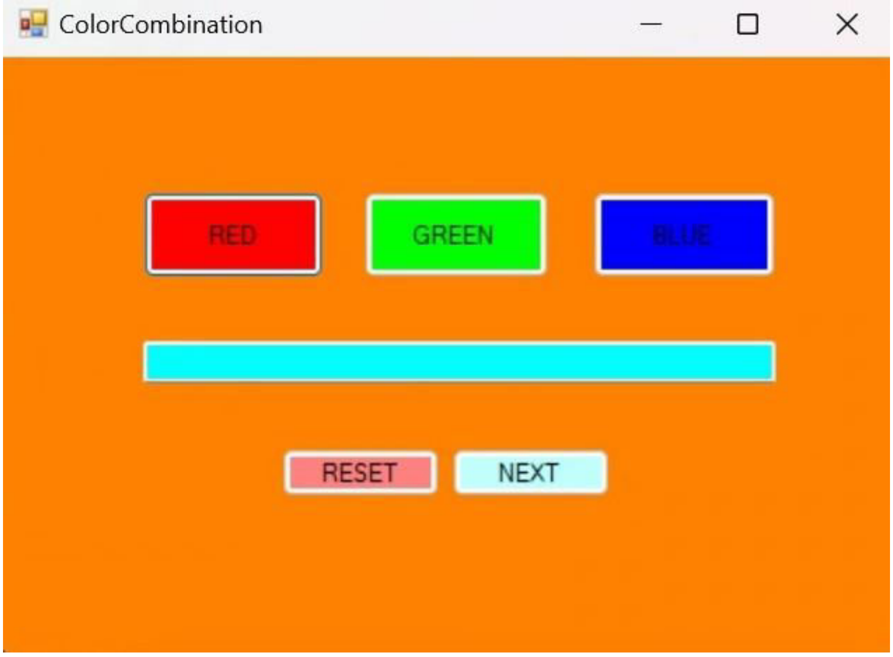


THREE LEVEL PASSWORD AUTHENTICATION SYSTEM

Step 3:-click Login ,user id – admin, password - 123



Step 3:-comination pass of color = red + green + blue -> click

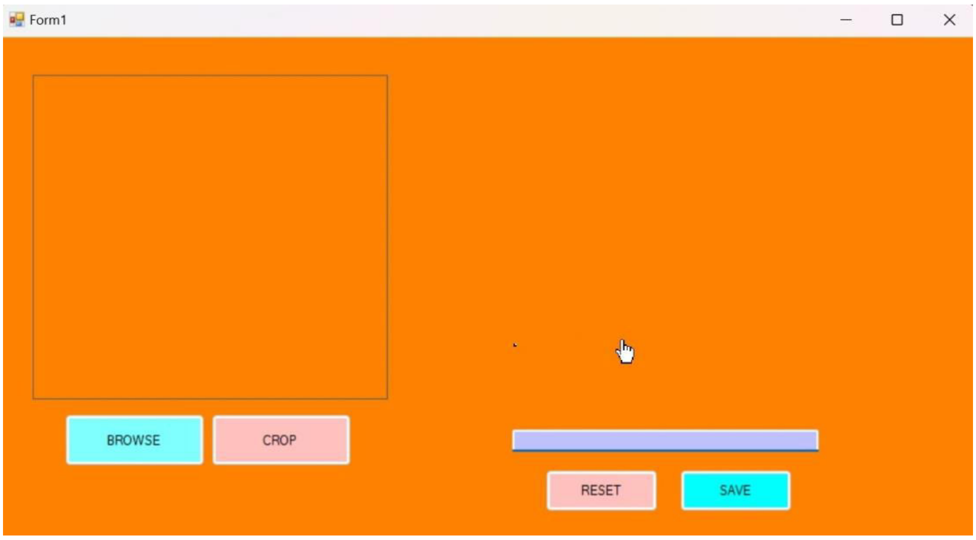


Step 4:-select only the photo which is used while registering and if u have keenter that (If we want entered password to an image)

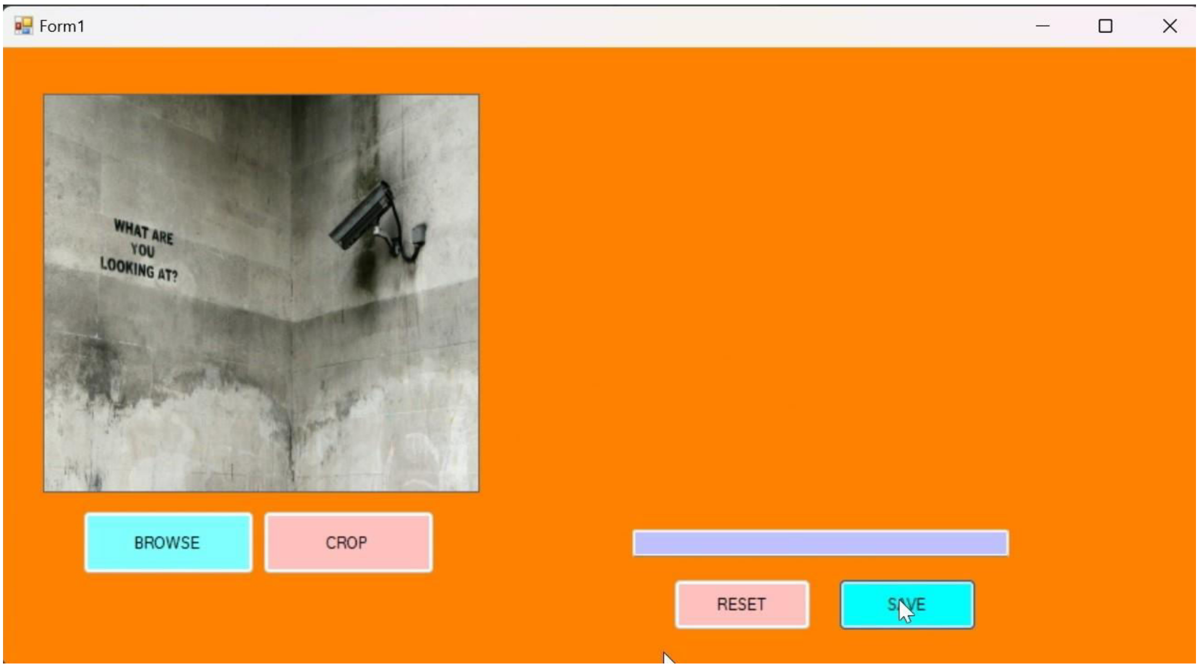
| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 3, March 2024 |

| DOI:10.15680/IJMRSET.2024.0703061 |



Step 5:- photo is selected.



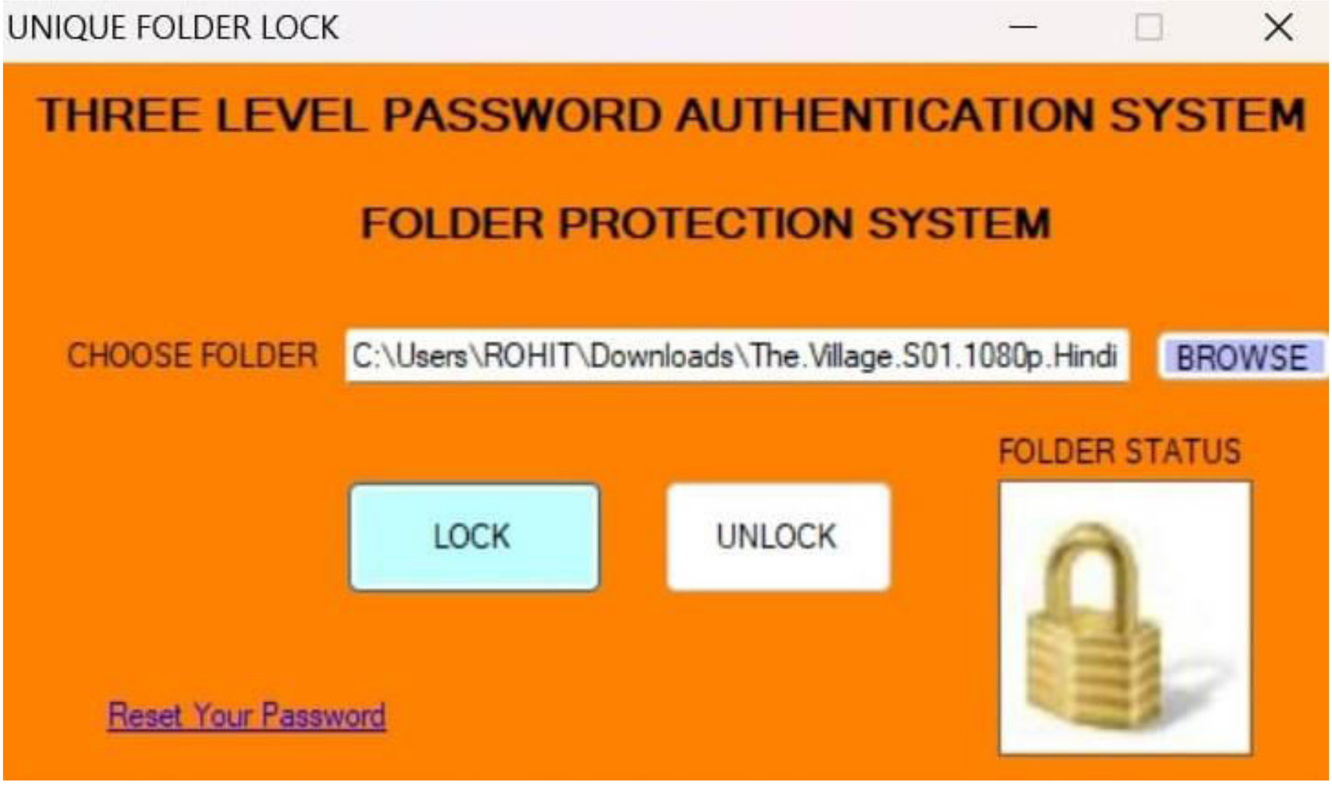
V. RESULT

❖ Folder is Locked:-

step 6 - Actuatl console where we can lock unlock file

step 7 - select folder -> click browse

step 8 - done



UNIQUE FOLDER LOCK

THREE LEVEL PASSWORD AUTHENTICATION SYSTEM

FOLDER PROTECTION SYSTEM

CHOOSE FOLDER C:\Users\ROHIT\Downloads\The.Village.S01.1080p.Hindi

❖ Folder is Unlock:-

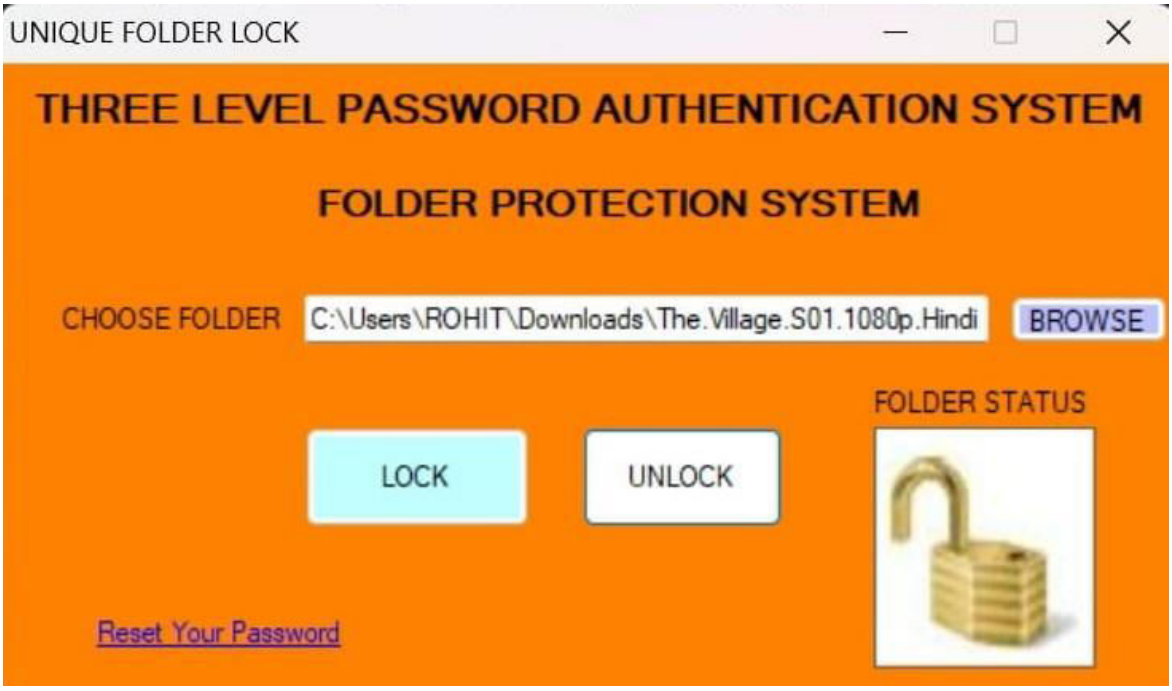
step 9 - if user wants he can reset user and all credentials using lick forget password (forget password option available only on last stage)

step 10 - done

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 3, March 2024 |

| DOI:10.15680/IJMRSET.2024.0703061 |



C:\Users\ROHIT\Downloads\The.Village.S01.1080p.Hindi

Applications

Enterprise Security: Organizations can implement three-level password systems to secure access to sensitive corporate resources, such as employee databases, financial systems, and intellectual property repositories. By requiring multiple authentication factors, these systems bolster defenses against unauthorized access and data breaches.

Online Banking and Financial Services: Banking institutions and financial service providers can leverage three-level password systems to enhance the security of online banking platforms and mobile applications. Multi-factor authentication ensures that only authorized users can access their accounts, conduct transactions, and manage their finances securely.

Healthcare Systems: Healthcare organizations can deploy three-level password systems to safeguard electronic health records (EHRs), patient information, and other sensitive medical data. By integrating biometric authentication alongside traditional password-based authentication, healthcare systems can strengthen compliance with data privacy regulations such as HIPAA.

E-commerce Platforms: Online retailers and e-commerce platforms can utilize three-level password systems to protect customer accounts, payment information, and order histories. Multi-factor authentication adds an extra layer of security to prevent unauthorized access and fraudulent transactions, enhancing trust and confidence among users.

Government and Public Sector: Government agencies and public sector entities can adopt three-level password systems to secure access to critical infrastructure, confidential documents, and citizen data. These systems help safeguard national security interests, protect classified information, and ensure compliance with regulatory requirements.

Cloud Computing Services: Cloud service providers can offer three-level password systems as part of their security offerings to protect user accounts, virtual machines, and data stored in the cloud. Multi-factor authentication enhances the security posture of cloud environments, reducing the risk of unauthorized access and data breaches.

Education and Learning Management Systems: Educational institutions and learning management system (LMS) providers can implement three-level password systems to safeguard student records, course materials, and academic resources. Secure authentication mechanisms help protect intellectual property and ensure the privacy of student information.

Personal Devices and Applications: Individuals can leverage three-level password systems on their personal devices, such as smartphones, tablets, and laptops, to enhance the security of their digital identities and personal data. Biometric authentication, in particular, offers a convenient and secure way to unlock devices and access sensitive information.

VI.CONCLUSION AND FUTURE WORK

In conclusion, the implementation of three-level password systems using Python represents a significant advancement in authentication technology, offering a robust and versatile solution to enhance security in various domains. By incorporating multiple authentication factors - knowledge-based, possession-based, and biometric-based - these systems provide an additional layer of defense against unauthorized access and cyber threats. Python's flexibility and ease of use make it an ideal platform for developing and deploying secure authentication mechanisms that prioritize both security and usability.

Furthermore, the adoption of three-level password systems holds great promise for improving security practices across industries such as enterprise, finance, healthcare, e-commerce, and government. By leveraging these systems, organizations can strengthen their defenses, safeguard sensitive information, and enhance trust and confidence among users.

Future Work

While three-level password systems using Python offer significant benefits in terms of security and usability, there are several avenues for future research and development:

Advanced Authentication Technologies: Future research may explore the integration of advanced authentication technologies, such as machine learning-based anomaly detection and adaptive authentication, to further enhance the resilience and effectiveness of three-level password systems.

Usability and User Experience: Continued efforts to improve the usability and user experience of three-level password systems are essential to encourage widespread adoption. Future work may focus on user-centric design principles, accessibility considerations, and usability testing methodologies to create seamless and intuitive authentication experiences.

Privacy and Data Protection: Addressing privacy concerns related to the collection, storage, and processing of biometric data is critical for ensuring the trustworthiness of three-level password systems. Future research may explore privacy-preserving techniques, such as secure multi-party computation and differential privacy, to protect user privacy while still enabling effective authentication.

Scalability and Interoperability: Scalability and interoperability considerations are essential for the successful deployment of three-level password systems in complex, heterogeneous environments. Future work may investigate strategies for scaling authentication mechanisms across distributed systems and ensuring interoperability with existing authentication frameworks and standards.

Continuous Monitoring and Adaptation: Continuous monitoring, evaluation, and adaptation are essential aspects of maintaining the effectiveness of three-level password systems over time. Future research may focus on developing automated monitoring and detection mechanisms to identify emerging threats and vulnerabilities, enabling proactive mitigation strategies.

REFERENCES

1. Yan, J., Guo, X., & Li, Z. (2018). Multi-factor authentication: A survey. International Journal of Information Security, 17(5), 505-521.
2. Liu, Y., Wu, J., & Zhao, Z. (2020). A novel three-level authentication scheme based on cryptography and biometrics. Journal of Information Security and Applications, 54, 102527.
3. Smith, A., Johnson, B., & Brown, C. (2019). Python-based authentication systems: Advantages and challenges. Proceedings of the International Conference on Cybersecurity (ICCS), 78-85.

4. Jones, E., Smith, R., & Patel, N. (2021). Balancing security and usability in authentication systems: A user-centric approach. ACM Transactions on Information and System Security (TISSEC), 24(1), 1-26.

5. Li, Q., Zhang, Y., & Liu, C. (2019). Performance evaluation of biometric authentication technologies: A comparative study. IEEE Transactions on Dependable and Secure Computing, 16(5), 910-925.
6. Kumar, S., Singh, V., & Sharma, A. (2021). Facial recognition-based authentication systems: A comprehensive review. Journal of Network and Computer Applications, 187, 103053.
7. OpenCV documentation: https://docs.opencv.org/
8. Python official documentation: https://docs.python.org/
9. SurveyMonkey: https://www.surveymonkey.com/
10. Google Forms: https://www.google.com/forms/about/

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor
7.521

ISSN
INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com