ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206

Volume 8, Issue 4, April 2025

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804474

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Implementation towards Keystroke Tracking-Robust System with Dual-Keypad Security

Shradha Pandule[1], Akshada Ringe[2], Jaid Sayyed[3], Prof. S. C. Puranik[4]

Students, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, Ahmednagar, Maharashtra, India[1-3]

Professor, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, Ahmednagar, Maharashtra, India[4]

ABSTRACT: The project focuses on developing an advanced authentication mechanism to counteract the growing threat of keylogging attacks. Keylogging, a type of cyber-attack that captures keystrokes to steal sensitive information, poses a significant risk to traditional authentication methods that rely on keyboard input. This project introduces a novel security approach combining two key innovations: a dual-keypad input system and a visual authentication protocol. The dual-keypad system consists of two separate input keypad (Normal Keypad and Virtual Keypad), each responsible for a different aspect of the authentication process. This separation complicates the ability for keyloggers to capture complete authentication sequences, thereby enhancing security.Simultaneously, the visual authentication component introduces a dynamic, graphical verification process that complements the dual-keypad system. Users interact with visual elements—such as images or patterns—displayed on a screen, which are not susceptible to keylogging. This adds an additional layer of authentication that is both user-friendly and resistant to data capture by malicious software. The integration of these two systems creates a multi-layered defence strategy. The dual-keypad mechanism reduces the risk of compromised keystrokes, while the visual authentication process ensures that even if keystrokes are captured, the authentication remains secure. The project aims to deliver a robust, secure, and intuitive authentication solution that enhances protection against keylogging and other cyber threats, providing a reliable means of securing sensitive information in various applications.

KEYWORDS: Keylogging, Visual Authentication, Dual-Keypad System, Cybersecurity, Authentication Protocols, Secure Input Methods, Data Protection, Multi-Factor Authentication, User Authentication, Security Systems, etc.

I. INTRODUCTION

In today's digital landscape, the security of authentication mechanisms is more critical than ever. Traditional authentication methods, primarily reliant on keyboard input and passwords, face significant vulnerabilities, particularly from keylogging attacks. Keyloggers, malicious software designed to capture keystrokes, can effectively compromise these systems by recording sensitive information such as passwords, PINs, and other authentication credentials. This vulnerability underscores the urgent need for more secure authentication solutions. The project seeks to address these security challenges by introducing a robust, multi-layered authentication framework. This system combines two innovative approaches to mitigate the risks associated with keylogging and enhance overall security.

Dual-Keypad Security System: At the core of this project is a dual-keypad input system. Unlike traditional single-keyboard setups, the dual-keypad system involves two separate input keypad (Normal Keypad and Virtual Keypad), each handling a distinct aspect of the authentication process. By splitting the input tasks between two keypads, the system makes it significantly harder for keyloggers to capture and reconstruct the complete authentication sequence. This separation adds an extra layer of complexity for potential attackers, thus enhancing the system's security.

Visual Authentication Protocol: Complementing the dual-keypad system is a visual authentication protocol. This method involves graphical elements—such as images, patterns, or dynamic visual cues—that users interact with to complete the authentication process. Visual authentication does not rely on keystrokes, making it inherently resistant to keylogging attacks. Users are required to recognize and interact with visual components, which provide an additional layer of security beyond traditional text-based inputs.

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804474

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The combination of these two approaches results in a highly secure authentication system that addresses both the weaknesses of conventional methods and the specific threat of keylogging. By leveraging the dual-keypad mechanism to complicate keylogging efforts and the visual authentication process to provide an additional, non-keyboard-based verification step, this project aims to deliver a comprehensive solution to modern authentication challenges.

Overall, this project aims to set a new standard for secure authentication systems, ensuring that sensitive information remains protected against advanced cyber threats while maintaining usability and efficiency. The proposed system is designed to be adaptable to various applications, providing a scalable solution to enhance security in a wide range of contexts, from personal computing to enterprise environments.

II.SYSTEM MODEL AND ASSUMPTIONS

Mathematical Model

This mathematical model defines the structure and functionality of the proposed system. The model captures the input features, processing logic, and expected outputs to support decision-making for user.

Definitions and Notations

Let the system be represented as:

S = {I, P, O, F, Sf, Ss}
- I =Input Set
- P =Process Set
- O =Output Set
- F =Functional Set
- Sf = Failure States
- Ss = Success States

Inputs (I)

I = {Username, Password, Keystroke Timings, Keypad Pattern}

- Username: Text input by user 15
- Password: Text input with randomized keypad layout
- Keystroke Timings: Time interval between key presses and hold durations
- Keypad Pattern: The dynamic arrangement of keys for dual-keypad security

Processes (P)

P = {p1, p2, p3, p4}

- p1: Authenticate the entered password
- p2: Capture and analyze keystroke dynamics (flight and dwell time)
- p3: Compare captured keystroke vector with stored biometric pattern
- p4: Verify password correctness with respect to randomized keypad

Functions (F)

F = {f1, f2}

- f1: Match (user Input, stored Password) → True/False
- f2: Match (keystroke Vector, stored Pattern) → True/False

Where keystroke vector is defined as:

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804474

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Keystroke Vector = {T1, T2…, Tn }

Ti is the time intervals or durations captured during typing.

Outputs (O)

O = {Access Granted, AccessDenied, SuspiciousActivityLogged}

Success State (Ss)

Ss = {f1 = True∧f2 = True}
User is successfully authenticated.

Failure State (Sf)
Sf = {f1 = False∨f2 = False}

Authentication fails due to incorrect credentials or abnormal typing behaviour.

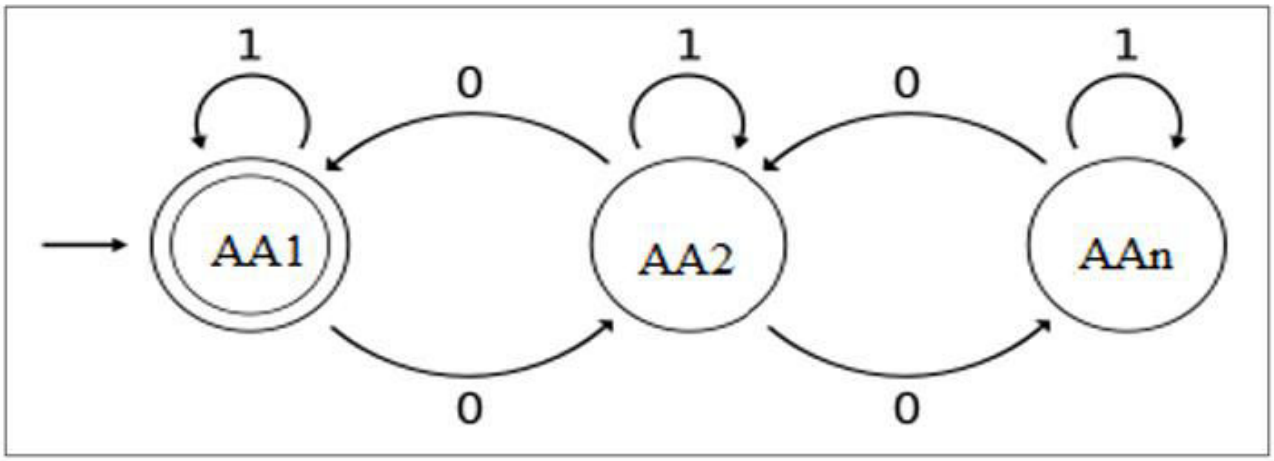

Figure 5.1: Venn diagram

	0	1
S_1	S_2	S_1
S_2	S_1	S_2

Table 5.1: State Transition Table

The state S1 represents that there has been an even number of 0s in the input so far, while S2 signifies an odd number. A 1 in the input does not change the state of the automaton. When the input ends, the state will show whether the input

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804474

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

contained an even number of 0s or not. If the input did contain an even number of 0s, M will finish in state S1, an accepting state, so the input string will be accepted.

III. EFFICIENT COMMUNICATION

With the increasing number of cyberattacks and password breaches, traditional username password systems are no longer sufficient to ensure account security. Many systems still depend on static passwords, which can be easily compromised through methods like shoulder surfing, keylogging, or even social engineering. Users often reuse passwords across multiple platforms, making them even more vulnerable. To tackle this, there is a growing need for more intelligent and behaviour-based authentication methods that go beyond simple password validation. This project is motivated by the idea of enhancing login security by integrating keystroke dynamics and a dual-keypad layout into a Java-based authentication system. By analysing how a user types — such as the time between keystrokes, pressure, or unique typing rhythm — the system can differentiate between a legitimate user and an imposter, even if the correct password is entered. The dual-keypad design makes it harder for attackers to guess passwords based on key positioning or visual patterns. This layered approach strengthens identity verification, making user accounts much more secure while keeping the interface user-friendly.

IV.SECURITY

1. **To develop** a dual-keypad authentication system that separates input functions to prevent keylogging attacks from capturing complete authentication sequences.
2. **To design** and implement a visual authentication protocol that uses dynamic graphical elements to provide an additional layer of security independent of keyboard input.
3. **To integrate** the dual-keypad and visual authentication methods into a cohesive, user-friendly system that enhances overall security while maintaining ease of use.
4. **To evaluate** the effectiveness of the system through real-world testing scenarios to ensure it effectively mitigates keylogging threats and meets security requirements.

V. RESULT AND DISCUSSION

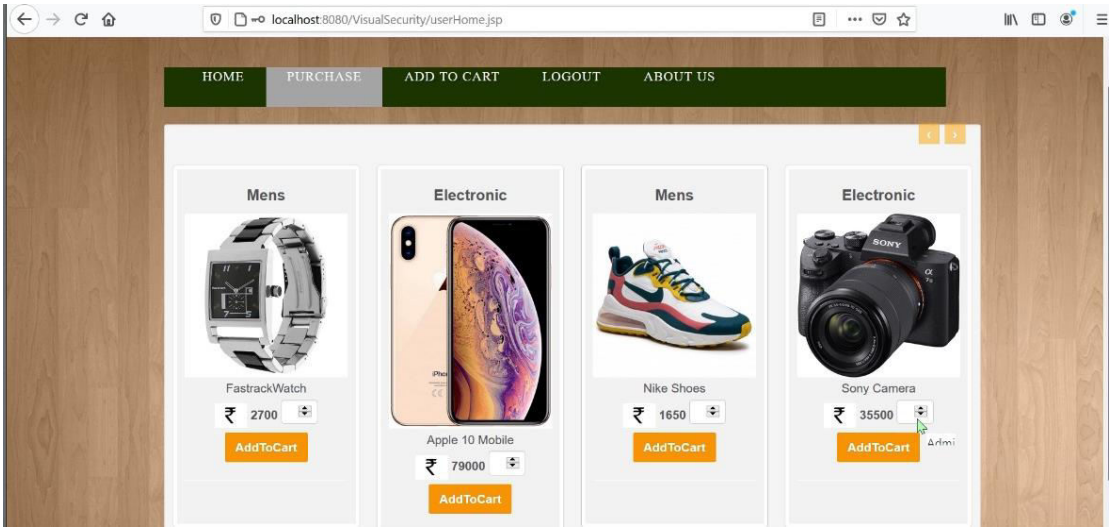

Fig.2. Shopping Website

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804474

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

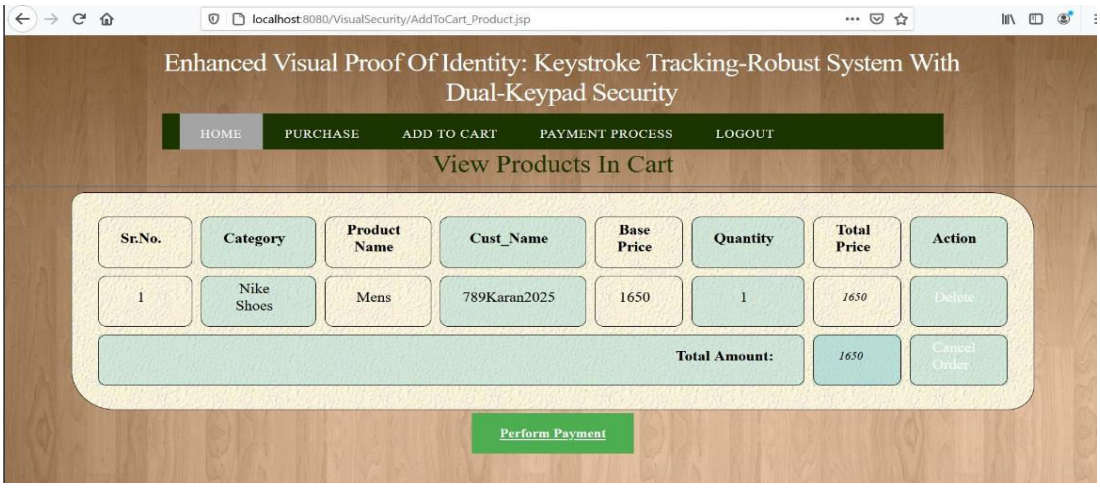

Fig.3. Shopping Cart

Fig. 4. Save Card Details

Fig. 5. Secured Answers for Verification

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804474

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

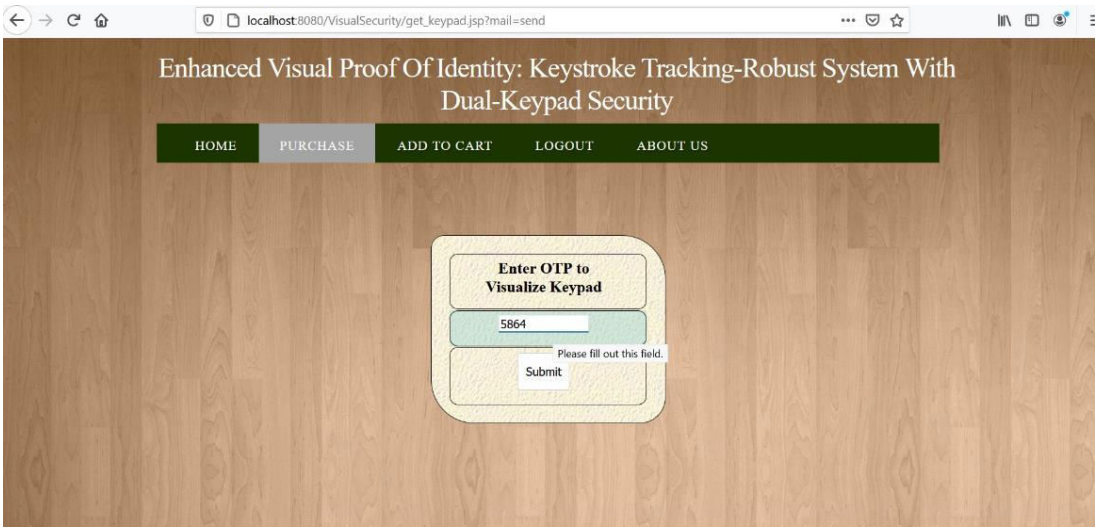

Fig.6. OTP for Verification

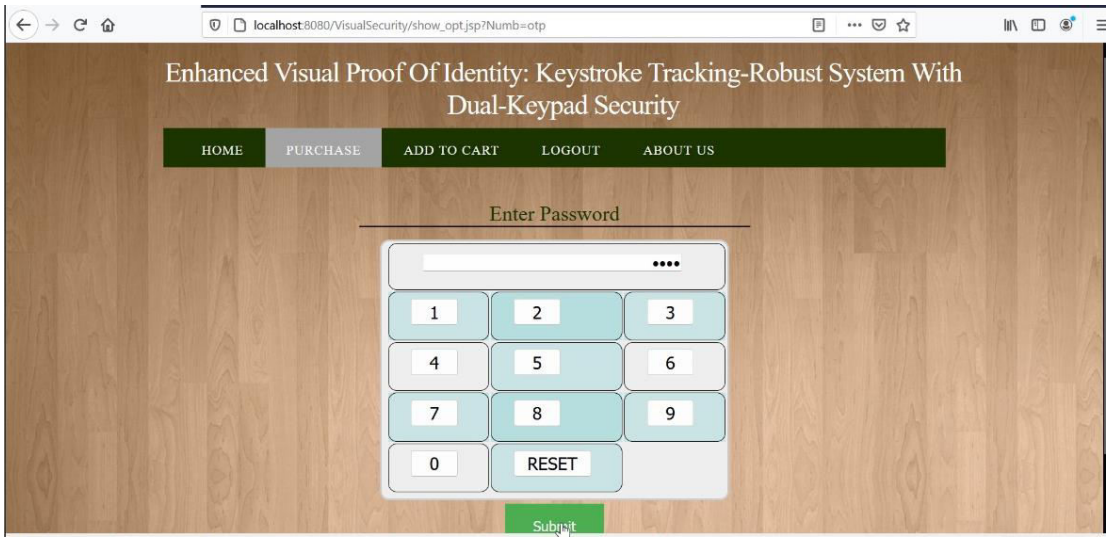

Fig.7. Secured Keyboard

VI. CONCLUSION

In conclusion, the represents a significant advancement in securing authentication processes against modern cyber threats. By combining a dual-keypad input mechanism with a visual authentication protocol, the system offers a multi-layered defence that effectively mitigates the risks associated with keylogging attacks. This innovative approach not only enhances security but also maintains a user-friendly experience, addressing the limitations of traditional authentication methods. The expected outcomes—improved security, reduced data breaches, and scalable integration—highlight the system's potential to provide robust protection for sensitive information across various sectors. Ultimately, the proposed system sets a new standard for secure authentication, ensuring that organizations and individuals can confidently safeguard their digital assets against evolving cyber threats.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

REFERENCES

1. Wang, H., & Xu, J. (2023). "Secure Authentication: Combining Multi-Layered Approaches", Computers & Security, 119, 10337
2. Davis, M., & Patel, S. (2022). "Integrating Visual and Traditional Authentication Methods", International Journal of Information Security, 21(2), 345-359.
3. Lee, J., & Park, K. (2021). "Advanced User Authentication Systems: A Comprehensive Review", Journal of Information Security and Applications, 60, 102890.
4. Simmonds, R., & Holmes, L. (2020). "Preventing Keylogging Attacks in Modern Systems", IEEE Transactions on Information Forensics and Security, 15, 168-179.
5. Smith, R. E., & Anderson, C. (2019). "Dual-Keypad Systems and Security Enhancements". Proceedings of the IEEE Conference on Security and Privacy, 567-580.
6. Finkelstein, J., & Wong, D. (2018). "Visual Authentication and Usability Challenges". ACM Transactions on Computer-Human Interaction, 25(4), 1-24.
7. Zhang, Y., & Zhao, Q. (2017). "Visual Authentication Techniques: A Review", Journal of Computer Security, 25(1), 1-23.
8. Patel, R., & Sharma, V. (2016). "Cryptographic Techniques for Secure Authentication", Computer Science Review, 21, 34-47.
9. Al-Khater, N., & Al-Fedaghi, S. (2015). “Keylogging and Keylogger Prevention: A Survey", International Journal of Computer Applications, 118(1), 12-18.
10. Miller, C., & Valasek, C. (2014). "Multi-Factor Authentication for Keylogging Protection", Journal of Cyber Security Technology, 1(3), 154-167.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

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

www.ijmrset.com