

Keystroke Tracking-Robust System with Dual-Keypad Security

Shradha Pandule¹, Akshada Ringe², Jaid Sayyed³, Prof. S. C. Puranik⁴

^{1,2,3}Students of Department of Computer Engineering Vishwabharti Academy's College of Engineering, Ahmednagar, Maharashtra, India.

⁴Prof. of Department of Computer Engineering, Vishwabharti Academy's College of Engineering, Ahmednagar, Maharashtra, India.

Emails: shradhapandule8484@gmail.com¹, snehalata3516@gmail.com²

Abstract

The development of an advanced authentication mechanism designed to mitigate the increasing risk of keylogging attacks, a prevalent cyber threat that captures keystrokes to steal sensitive information. Traditional authentication methods relying on keyboard input are particularly vulnerable to such attacks. To address this, a novel security framework is introduced, combining two innovative components: a dual-keypad input system and a visual authentication protocol. The dual-keypad system employs two distinct input interfaces—a physical keypad and a virtual keypad—each handling separate aspects of the authentication process. This division significantly complicates the ability of keyloggers to capture complete authentication sequences, thereby enhancing security. Complementing this, the visual authentication component incorporates a dynamic, graphical verification process. Users interact with visual elements, such as images or patterns displayed on a screen, which are inherently resistant to keylogging. This approach not only strengthens security but also ensures a user-friendly experience. Together, these systems form a multi-layered defense strategy. The dual-keypad mechanism minimizes the risk of keystroke compromise, while the visual authentication ensures that even if keystrokes are intercepted, the authentication process remains secure. This research aims to deliver a robust, secure, and intuitive authentication solution that effectively counters keylogging and other cyber threats, offering a reliable method for safeguarding sensitive information across various applications.

Keywords: Authentication Protocols; Cybersecurity; Dual-Keypad System; Keylogging; Multi-Factor Authentication; Secure Input Methods; Data Protection; User Authentication; Security System; Visual Authentication.

1. 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 [1-3].

1.1 Dual-Keypad Security System

At the core of this project is a dual-keypad input system. Unlike traditional single-keyboard setups [4], 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 [5-7].

1.2 Visual Authentication Protocol

Complementing the dual-keypad system is a visual authentication protocol [8]. This method involves graphical elements—such as images, patterns, or dynamic visual cues—that users interact with to

2. Method

The system offers robust protection against keylogging while maintaining operational efficiency.



3. Results and Discussion

3.1.Results

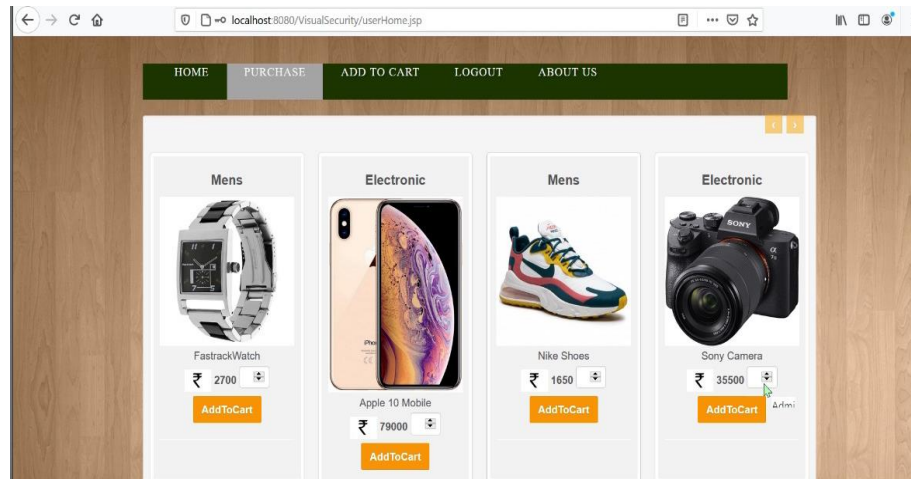


Figure 2 Shopping Website



Figure 3 Shopping Cart



Figure 4 Save Card Details



Figure 5 Secured Answers for Verification

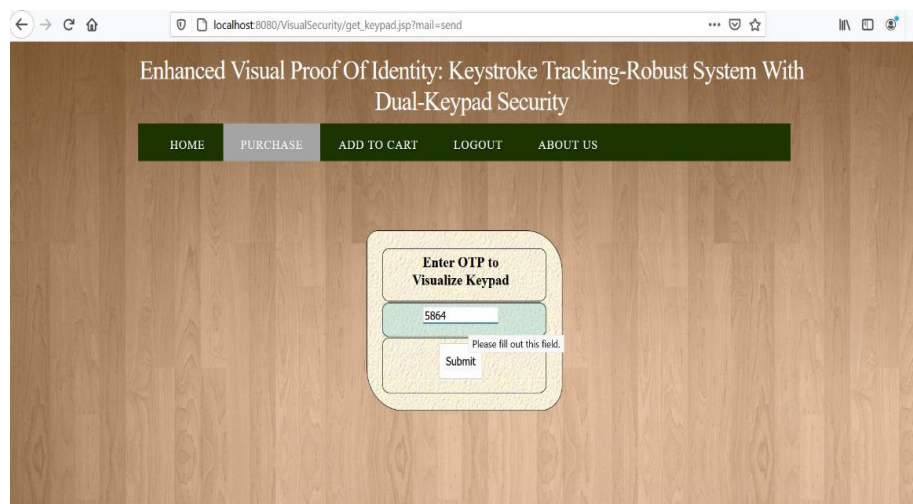


Figure 6 OTP for Verification

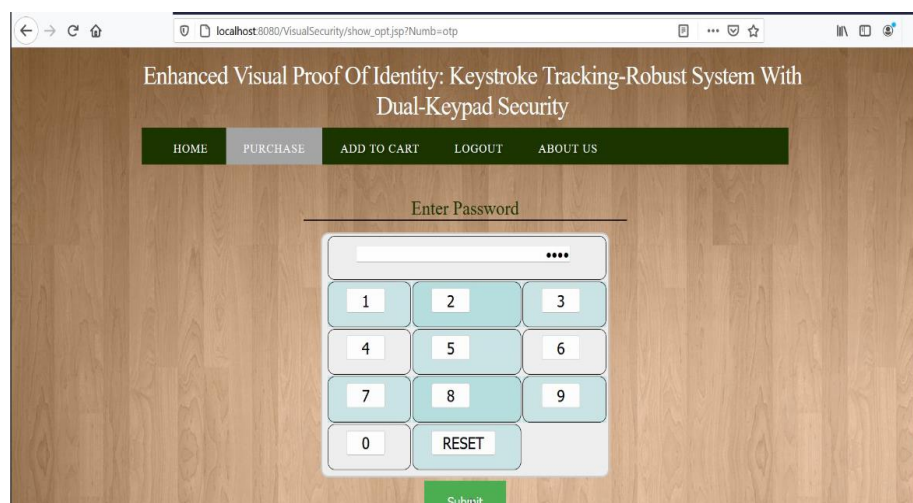


Figure 7 Secured Keyboard

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 defense 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.

Acknowledgements

We would prefer to give thanks the researchers likewise publishers for creating their resources available. We are conjointly grateful to guide, reviewer for their valuable suggestions and also thank the college authorities for providing the required infrastructure and support.

References

- [1].Wang, H., & Xu, J. (2023). "Secure Authentication: Combining Multi-Layered Approaches", *Computers & Security*, 119, 103372.
- [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.