International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2160-2164
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0288

AI-Based Typing Biometric for Behavior-Locked Decryption Using Kernel Ridge Regression

Mrs.K.Kartheeswari[1], Pavan S[2], Pradeepan B[3], Anand S[4]
[1234]Department of Information Technology, Kamaraj college of Engineering and Technology, Virudhunagar, Tamil Nadu – 626001, India
Email ID: *kartheeswariitkcet@gmail.com[1], spavan0823@gmail.com[2] , pradeep102004@gmail.com[3] , arunjunai82@gmail.com[4]*

Abstract
Modern information systems require strong security mechanisms to protect sensitive data from unauthorized access. Traditional authentication methods such as passwords and PINs are widely used, but they are vulnerable to security threats like password theft, phishing attacks, and credential leakage. In many cases, attackers can gain access to confidential data simply by obtaining the correct password. Therefore, there is an increasing need for intelligent authentication systems that can verify the identity of users more accurately and securely. This paper proposes an AI-Based Typing Biometric System for Behaviour-Locked Decryption using Kernel Ridge Regression with Face Recognition to enhance system security. The proposed system utilizes behavioural biometrics by analysing a user's typing pattern, also known as keystroke dynamics. Typing features such as dwell time, flight time, and typing rhythm are captured when the user enters credentials. These features are processed using the Kernel Ridge Regression (KRR) machine learning algorithm to identify unique typing behaviour patterns of authorized users. In addition to typing biometrics, the system integrates a face recognition module as a second-level authentication mechanism. The system captures the user's facial image through a camera and compares it with stored facial data to verify the user's identity. Only when both the typing pattern and facial recognition match the registered user profile will the system allow the behaviour-locked decryption of protected data .In this context, the proposed project introduces an AI-Based By combining behavioural and physiological biometrics, the proposed system provides a multi-factor authentication framework that significantly improves data security and reduces the risk of unauthorized access. The system can be effectively used in applications such as secure login systems, financial platforms, and confidential data protection environments.

Keywords: *Artificial Intelligence, Typing Biometrics, Keystroke Dynamics, Kernel Ridge Regression, Face Recognition, Behaviour-Locked Decryption, Biometric Authentication, Cybersecurity*

1. Introduction
With the rapid growth of digital technologies and online services, ensuring the security of sensitive information has become a major concern. Many systems today rely on traditional authentication methods such as passwords and PINs to protect confidential data. However, these methods are vulnerable to various security threats including password theft, phishing attacks, and unauthorized access. Attackers can easily compromise passwords, which makes traditional authentication systems less reliable in highly secure environments. With the rapid growth of digital technologies and online services, ensuring the security of sensitive information has become a major concern. Many systems today rely on traditional authentication methods such as passwords and PINs to protect confidential data. However, these methods are vulnerable to various security threats including password theft, phishing attacks, and unauthorized access. Attackers can easily compromise passwords, which makes traditional

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2160-2164
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0288

authentication systems less reliable in highly secure environments. Recent advancements in Artificial Intelligence (AI), Machine Learning, and Biometric Authentication have opened new possibilities for developing secure access control systems. Behavioral biometrics such as typing patterns can be used to identify users based on their unique typing rhythm and keystroke dynamics. Machine learning algorithms can analyze these typing patterns and accurately distinguish between legitimate users and unauthorized individuals In this context, the proposed project introduces an AI-Based Typing Biometric System for Behaviour-Locked Decryption using Kernel Ridge Regression with Face Recognition. The system captures typing behavior such as dwell time and flight time while the user enters credentials. These features are analyzed using a Kernel Ridge Regression model to verify the user's typing pattern

1.1.Background of the Study

With the rapid growth of digital technologies, ensuring the security of sensitive information has become a major challenge. Traditional authentication methods such as passwords and PINs are widely used, but they are vulnerable to security threats like phishing, brute-force attacks, and credential theft. Users often create weak passwords or reuse them across multiple platforms, increasing the risk of unauthorized access. As cyberattacks continue to rise, there is a need for more reliable and secure authentication mechanisms. Biometric-based systems, especially behavioral biometrics like typing patterns, provide an advanced solution by identifying users based on unique characteristics, enhancing security and reducing dependency on passwords.

1.2.Problem Statement

Traditional authentication systems based on passwords are vulnerable to security threats such as hacking, phishing, and unauthorized access. Even when strong passwords are used, they can be compromised or shared, leading to data breaches. These limitations highlight the need for a more secure and reliable authentication method. Therefore, an advanced system that verifies user identity using behavioral patterns and biometric features is required to ensure secure access to sensitive data.

2. Method

The proposed system utilizes a multi-factor authentication approach combining typing biometrics and facial recognition for secure user verification. Initially, keystroke dynamics are captured during user input, including features such as dwell time and flight time. These features are preprocessed and structured into feature vectors for analysis. A Kernel Ridge Regression (KRR) model is trained using authorized user data to learn individual typing patterns. During authentication, the system compares real-time typing input with the trained model to verify behavioral identity. Upon successful verification, a face recognition module is activated to capture and match the user's facial image with stored data using computer vision techniques. Only when both authentication stages are satisfied, behaviour-locked decryption is performed to grant access to protected resources. Existing machine learning and biometric techniques are referenced from prior studies to ensure reliability and reproducibility.

Table 1 Experimental input parameters for Biometric Sample

INPUT TEXT	DWELL TIME (ms)	FLIGHT TIME(ms)
User 1 Sample	120	80
User 2 Sample	135	95
User 3 Sample	110	75
User 4 Sample	140	100
User 1 Sample	118	82
User 2 Sample	130	90
User 3	112	78

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2160-2164
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0288

Sample		
User 4 Sample	145	105
User 1 Sample	122	85
User 2 Sample	138	92
User 3 Sample	115	80
User 4 Sample	142	98

2.1.Tables

Tables are used to present the experimental data collected from the typing biometric authentication system. Each table is numbered using Arabic numerals and includes a clear and descriptive title. The tables are formatted to ensure readability and are placed separately from the main text where required. Each column in the table represents important keystroke features such as dwell time and flight time, which are used for analyzing user typing behavior. These parameters are processed by the Kernel Ridge Regression model to identify unique user patterns. Any abbreviations used in the table are clearly defined below the table for better understanding. The tabular representation helps in comparing user typing characteristics and evaluating system performance effectively. Figures 1 are used to visually represent the workflow and outputs of the proposed typing biometric authentication system. All figures are numbered using Arabic numerals (e.g., Figure 1, Figure 2) based on their order of appearance in the paper. The figure number is placed clearly outside the image boundaries for proper identification.

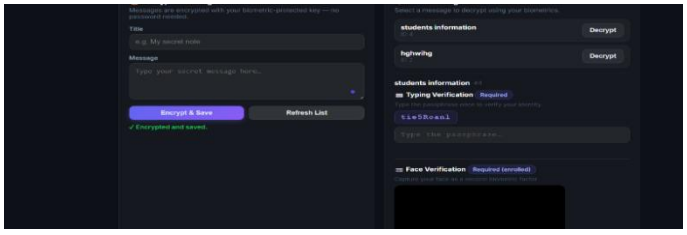

Figure 1 User Interface for Behaviour-Locked Decryption with Typing and Face Verification

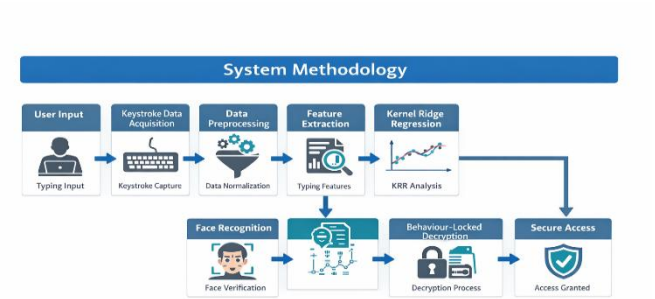

Figure 2 Overall Architecture of Typing Biometrics and Face Recognition-Based Security System

3. Result and Discussion

3.1.Results

The Results should include the rationale or design of the experiments as well as the results of the experiments. Results can be presented in figures, tables, and text. The Results should include the rationale or design of the experiments as well as the results of the experiments. Results can be presented in figures, tables, and text. The experimental setup of the proposed system involves collecting typing data from multiple users and capturing their corresponding facial images for authentication. The system records keystroke dynamics such as dwell time and flight time while users enter predefined text. These features are used to train the Kernel Ridge Regression (KRR) model to learn individual typing behavior patterns. During testing, real-time typing input is compared with the trained model to verify user identity. The results show that the system is able to accurately distinguish between authorized and unauthorized users based on their typing patterns. The integration of the face recognition module further improves authentication reliability by verifying the user's physical identity after behavioral verification. The results are presented using tables

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2160-2164
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0288

and system output screenshots, showing successful authentication when both typing biometrics and facial recognition match the stored data. In cases of mismatch, the system correctly denies access, demonstrating effective prevention of unauthorized entry. Overall, the experimental results confirm that the proposed system provides accurate, secure, and reliable multi-factor authentication.

3.2.Discussion

The proposed system demonstrates that combining typing biometrics with face recognition significantly enhances authentication security compared to traditional password-based methods. The use of keystroke dynamics allows the system to capture unique behavioral characteristics, making it difficult for unauthorized users to replicate typing patterns even if credentials are known. The implementation of Kernel Ridge Regression (KRR) helps in effectively modeling non-linear typing behavior, improving the accuracy of user identification. The addition of the face recognition module provides an extra layer of verification, ensuring that authentication is not solely dependent on behavioral data. This dual authentication approach reduces the chances of impersonation and strengthens system reliability. The behaviour-locked decryption mechanism ensures that sensitive data is accessed only after successful verification, enhancing data protection. Overall, the system highlights the effectiveness of integrating behavioral and biometric techniques for secure authentication. It also indicates that multi-factor systems are more robust and adaptable for real-world security applications compared to single-factor methods.

Conclusion

The proposed system addresses the limitations of traditional password-based authentication by integrating typing biometrics and face recognition. The results confirm that the system can accurately verify user identity using behavioral and biometric features. The behaviour-locked decryption mechanism ensures secure data access only for authorized users, thereby improving security and reducing the risk of unauthorized access.

Acknowledgements

I would like to express my sincere gratitude to my faculty mentors and the Department of Information Technology at Kamaraj College of Engineering and Technology for their valuable guidance, encouragement, and continuous support throughout the development of the project titled “AI-Based Typing Biometric for Behaviour-Locked Decryption using Kernel Ridge Regression with Face Recognition.” Their suggestions and technical guidance helped in successfully completing this research work.

References

The References section includes all relevant published works related to typing biometrics, machine learning, and face recognition used in this study. All references are listed in the order in which they appear in the text. Within the manuscript, references are cited using APA style by mentioning the author’s last name and year of publication (e.g., Kumar, 2023). The authors are responsible for ensuring the accuracy and correctness of all cited references, as the journal will not be liable for any citation errors. This paper follows the APA (American Psychological Association) referencing style for both in-text citations and the reference list. Authors are encouraged to use reference management tools such as Mendeley, Zotero, or EndNote to organize citations efficiently. Proper referencing supports the reliability of the proposed system and acknowledges prior research in biometric authentication and security systems.

[1]. S. Banerjee and D. L. Woodard, “Biometric Authentication Using Keystroke Dynamics: Current Trends and Challenges,” IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1209–1224, 2020.

[2]. A. K. Jain, A. Ross, and K. Nandakumar, “Introduction to Biometrics and Behavioral Authentication,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 43, no. 3, pp. 913–928, 2021.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2160-2164
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0288

[3]. · M. A. Ferrer and A. Morales, "Keystroke Dynamics Recognition Based on Machine Learning Techniques," Pattern Recognition Letters, vol. 145, pp. 80–87, 2021.
[4]. · R. Giot, M. El-Abed, and C. Rosenberger, "User Authentication Using Keystroke Dynamics and Machine Learning," International Journal of Information Security, vol. 21, no. 2, pp. 215–229, 2022.
[5]. · Y. Li and J. Wang, "Deep Learning Approaches for Behavioral Biometric Authentication," IEEE Access, vol. 10, pp. 55821–55834, 2022.
[6]. · H. Kim and S. Park, "Continuous User Authentication Using Keystroke Dynamics and Neural Networks," IEEE Access, vol. 11, pp. 45678–45690, 2023.
[7]. · P. Sharma and R. Singh, "Machine Learning-Based Keystroke Dynamics for Secure Authentication Systems," International Journal of Computer Applications, vol. 185, no. 15, pp. 25–31, 2023.
[8]. · L. Zhang and M. Chen, "Multimodal Biometric Authentication Using Face Recognition and Behavioral Biometrics," IEEE Internet of Things Journal, vol. 11, no. 4, pp. 6021–6033, 2024.
[9]. · S. Kumar and V. Gupta, "AI-Based User Authentication Using Keystroke Dynamics and Facial Recognition," IEEE Access, vol. 12, pp. 23411–23425, 2024.
[10]. · R. Patel and A. Desai, "Secure Multi-Factor Authentication Using Behavioral Biometrics and Machine Learning," Journal of Cybersecurity and Privacy, vol. 5, no. 1, pp. 45–59, 2025.