Dynamic Keystroke And Biometric User Authentication

Mr. K.Pazhanivel[1], Amala Bridget V[2], Amirtha G R[3], Jerusha Karen A[4], Arokiya Mejella B [5]
[1, 2, 3, 4, 5] Dept of Computer Science and Engineering
[1, 2, 3, 4, 5] Anjalai Ammal Mahalingam Engineering College Kovilvenni, Tamil Nadu, India

Abstract- *Traditional authentication mechanisms such as passwords and PINs are widely used for system security; however, they remain vulnerable to attacks such as password theft, shoulder surfing, and replay attacks. To address these limitations, this research proposes a dynamic multi-modal biometric authentication system that integrates keystroke dynamics and face recognition using a Support Vector Machine (SVM) classifier. The proposed system continuously verifies user identity by analyzing typing behaviour and facial features captured through a webcam. Keystroke timing characteristics such as dwell time and flight time are extracted, while facial features are obtained using computer vision-based face recognition techniques. The proposed model demonstrates strong potential for applications requiring continuous and secure authentication such as online banking and financial platforms.*

I. INTRODUCTION

With the rapid growth of digital technologies and online services, secure user authentication has become a critical requirement. Traditional authentication techniques such as passwords, PINs, and one-time passwords provide only static verification and are vulnerable to several types of cyber-attacks. Once authentication is completed, these systems do not continuously verify whether the authenticated user remains the same throughout the session.

Keystroke dynamics is a behavioural biometric that identifies users based on their typing patterns, while face recognition is a physiological biometric that analyses facial features.

This research proposes a multi-modal authentication system combining keystroke dynamics and face recognition, where a Support Vector Machine (SVM) classifier is used to identify authorized users and detect intruders.

II. LITERATURE REVIEW

Biometric authentication has been extensively studied in recent decades.

Joyce and Gupta (1990) introduced keystroke dynamics as a behavioural biometric technique for user authentication based on typing rhythm. Their research demonstrated that typing patterns can uniquely identify individuals.

Cortes and Vapnik (1995) proposed the Support Vector Machine (SVM) algorithm, which has become a powerful supervised machine learning method used for classification problems due to its strong generalization capability.

Viola and Jones (2001) developed the Viola–Jones face detection algorithm, which became widely used in computer vision applications for real-time face detection.

III. PROBLEM DEFINITION

In modern digital systems, user authentication is commonly performed using traditional methods such as passwords, PINs, or one-time passwords (OTPs). Although these techniques are widely adopted, they provide only initial verification and do not continuously monitor whether the authenticated user remains the same throughout the session. As a result, these systems are vulnerable to security threats such as password theft, impersonation, shoulder surfing, and unauthorized access.

To overcome this issue, the proposed solution focuses on developing a dynamic multi-modal authentication system that combines keystroke dynamics and face recognition and applies a Support Vector Machine (SVM) classifier to analyse biometric features and classify users as either authorized or unauthorized. The goal is to improve authentication accuracy, enhance system security, and reduce the risks associated with traditional single-factor authentication methods..

IV. EXISTING SYSTEM

The existing authentication systems primarily rely on traditional security mechanisms such as passwords, Personal Identification Numbers (PINs), and One-Time Passwords

(OTPs) to verify user identity. These methods provide only static authentication, meaning the system verifies the user only at the time of login and does not monitor user identity continuously during the session.Therefore, the existing systems often suffer from limitations such as limited security, lack of continuous monitoring, vulnerability to attacks, and reduced reliability when using single authentication factors. These limitations highlight the need for a more advanced and reliable authentication mechanism that combines multiple biometric modalities for improved security.

V. PROPOSED SYSTEM

The proposed system introduces a dynamic multi-modal authentication approach that combines keystroke dynamics and face recognition to enhance system security and ensure continuous user verification.In this system, keystroke dynamics is used as a behavioural biometric to analyse typing patterns such as dwell time and flight time, which are unique to each user. At the same time, face recognition is used as a physiological biometric to identify the user by analyzing facial features captured through a webcam. The extracted features from both keystroke dynamics and facial recognition are combined and processed using a Support Vector Machine (SVM) classifier, which classifies users as either authorized users or intruders.

VI. SYSTEM ARCHITECTURE

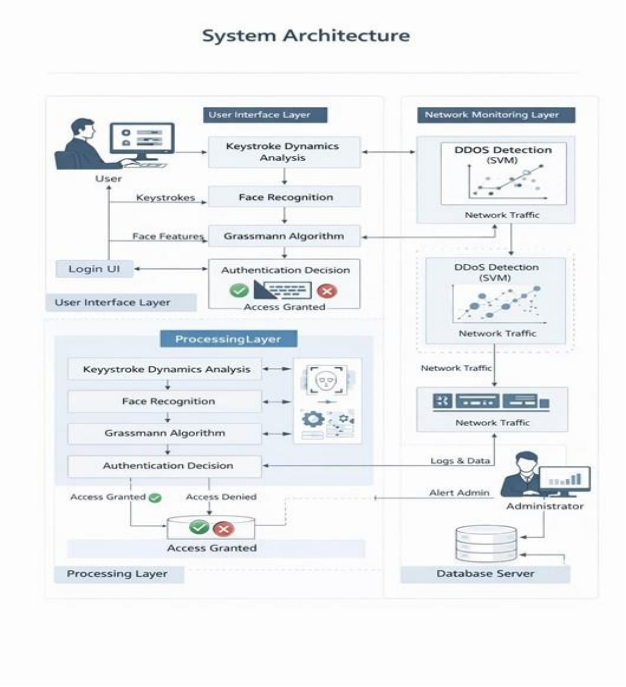

Fig. 1. Architecture of the Proposed Visual Test

Automation Framework

The system architecture of the proposed Dynamic User Authentication System is designed to provide secure, reliable, and continuous user verification by integrating multiple functional layers. The architecture mainly consists of the User Interface Layer, Processing Layer, Network Monitoring Layer, and Database Server, each responsible for specific tasks within the authentication process.In the User Interface Layer, users interact with the system through a login interface. During the login process, the system captures keystroke data while the user types and simultaneously acquires facial images through a webcam. The keystroke inputs are used to analyze typing patterns, while facial images are used to extract facial features for identity verification. In this layer, keystroke dynamics analysis is conducted to extract behavioural features such as dwell time and flight time, while facerecognition techniques are used to extract facial embeddings from the captured images. This layer uses a Support Vector Machine (SVM**)** based DDoS detection mechanism

VII. IMPLEMENTATION DETAILS

The proposed Dynamic User Authentication System is implemented using a combination of machine learning techniques, biometric feature extraction, and computer vision methods to ensure accurate and continuous user verification.

Next, the machine learning classification stage is implemented using a Support Vector Machine (SVM) algorithm. The extracted keystroke and facial features are combined into a feature vector and used to train the SVM model.

To enhance security, the system also includes a network monitoring component that analyses network traffic patterns to detect potential DDoS attacks using an SVM-based detection model

VIII.RESULTS AND DISCUSSION

The proposed dynamic user authentication system was evaluated to analyze its performance in accurately identifying authorized users and detecting intruders. The system integrates keystroke dynamics and face recognition features and uses a Support VectorMachine (SVM) classifie**r** for classification. Experimental testing was conducted using biometric data collected from multiple users during the login process.

Overall, the results indicate that the proposed multi-modal authentication system provides higher security, better

accuracy, and improved resistance to unauthorized access compared to traditional authentication methods

TABLE I. PERFORMANCE COMPARISON

Metric	Traditional Authentication System	Proposed Multi-Modal Biometric System (Keystroke + Face with SVM)
Authentication Method	Passwords, PINs, or OTP-based verification	Biometric authentication using keystroke dynamics and face recognition
Security Level	Moderate security; vulnerable to password theft and phishing attacks	High security due to multi-modal biometric verification
Continuous Authentication	Not supported (only login-time verification)	Supported through continuous monitoring of typing patterns and facial features
Accuracy	Lower accuracy due to dependency on user credentials	Higher accuracy using SVM classification and biometric feature analysis
False Acceptance Rate (FAR)	Higher possibility of unauthorized access	Reduced FAR due to dual biometric verification
False Rejection Rate (FRR)	May reject legitimate users due to password errors	Lower FRR through behavioral and physiological biometric combination

IX. ADVANTAGES AND APPLICATIONS

Advantages

- Does not require any additional biometric hardware.
- Non-intrusive and transparent to the user
- Cost-effective and easy to deploy

Applications

- Secure login systems in educational institutions and organizations.
- Online examination and remote assessment platforms.
- Banking and financial transaction authentication.

X. CONCLUSION AND FUTURE WORK

This paper presented a keystroke dynamics-based biometric authentication system using a Support Vector Machine (SVM) classifier. The experimental results demonstrate that typing behaviour can be effectively modelled to authenticate users with high accuracy and low error rates. The system enhances security without compromising usability and does not require additional hardware, making it practical for real-world deployment.

REFERENCES

[1] P. Kasprowski, Z. Borowska, and K. Harezlak, "Biometric Identification Based on Keystroke Dynamics," *Sensors*, vol. 22, no. 9, p. 3158, 2022.

[2] R. Shadman, M. E. Bours, and S. Mondal, "KeystrokeDynamics: Concepts, Datasets, and Machine Learning Techniques," *arXiv preprint*, 2023.

[3] Ł. Wyciślik, P. Wylężek, and A. Momot, "Keystroke Dynamics-Based User Identification Using Machine Learning," *Sensors*, vol. 24,no. 12, p. 3763, 2024.

[4] H. Nybø Risto and O. H. Graven,"Fixed-Text Keystroke Dynamics Authentication Dataset and Evaluation," *Annals of Telecommunications*, 2024.

[5] Kannan Nova, *Feature Extraction & ML Models in User Authentication*, 2022

[6] J. Guo, H. Mu, X. Liu, et al., "Federated Learning for Biometric Recognition: A Survey," *Artificial Intelligence Review*, 2024.

[7] V. Krivokuća Hahn and S. Marcel, "Biometric Template Protection for Neural-Network-Based Face Recognition Systems: A Survey of Methods and Evaluation Techniques," 2021.