Multi-Modal User Authentication: Integrating Keystroke Dynamics and Facial Recognition

Taduvai Satvik Gupta
Department of Electronics and Communication Engineering
Amrita School of Engineering, Bengaluru,
Amrita Vishwa Vidyapeetham, India
satviktaduvai@gmail.com

Konduru Praveen Karthik
Department of Electronics and Communication Engineering
Amrita School of Engineering, Bengaluru,
Amrita Vishwa Vidyapeetham, India
praveenkarthik2290@gmail.com

Sri Sai Suhas Sanisetty
Department of Electronics and Communication Engineering
Amrita School of Engineering, Bengaluru,
Amrita Vishwa Vidyapeetham, India
ssuhaas24@gmail.com

Sagar Basavaraju
Department of Electronics and Communication Engineering
Amrita School of Engineering, Bengaluru,
Amrita Vishwa Vidyapeetham, India
b_sagar@blr.amrita.edu

***Abstract*—User authentication is a process of confirms a user's identity before allowing entry into a system. This paper presents a multi-modal user authentication system by integrating the keystroke dynamics and the facial biometrics of the person. The system uses both machine learning for keystroke recognition and deep learning for facial recognition techniques for building a secure user authentication system. In addition to this, the model also alerts the user if there is a frequent unauthenticated user is trying to access their account. From the experimental results it has been noted that the model is achieving an accuracy of 93.4% for the keystroke detection giving optimal results compared to the Benchmark dataset and the face recognition model is achieving an accuracy of 96% with slight increase in the performance compared to the SOTA models.**

***Keywords*—SVM, KNN, Random Forest, Logistic Regression, Keystroke, Facial Recognition, Resnet.**

I. Introduction

In the digital age, most individuals rely on online platforms for a wide range of activities, which necessitates the use of numerous websites that store personal data. If an unauthorized person gains access to your password, they could misuse this data for unethical purposes, leading to potential security breaches. To mitigate such risks, user authentication processes are employed.

User authentication is the method of confirming the identity of an individual attempting to access a system, application, or network, ensuring that access is granted only to legitimate users [1]. This process is vital for safeguarding systems from unauthorized access and protecting sensitive information. Authentication can take various forms, including password-based, keystroke-based, biometric-based, and token-based methods, each contributing to enhanced security and trust in digital interactions [2].

User authentication techniques have changed significantly since the introduction of digital technologies. But as technology has advanced, cybersecurity risks have also increased, especially with regard to illegal access. A research by the Identity Theft Resource Center(ITRC) claims that in 2023,The ITRC tracked 3,205 data compromises, 1,404 more than in 2022 and 1,345 more than the previous high in 2021. There were 1,802 more data breaches in the United States alone, affecting the digital accounts and personal data of millions of people [3]. Finally, according to Verizon's 2023 Data Breach Investigations Report, phishing attempts and compromised credentials were implicated in almost 82% of breaches [4].

Conventional authentication techniques, which mostly use passwords, are susceptible to a number of security risks, such as credential stuffing and brute-force assaults. Even if two-factor authentication (2FA) has somewhat increased security, highly secure, non-intrusive authentication methods are still necessary [5]. This authentication mechanism is essential for strengthening access control by verifying user identities through multi-factor biometric validation, thereby mitigating unauthorized access and enhancing system security.

This paper presents an innovative approach to user authentication by integrating keystroke dynamics and facial recognition.Keystroke dynamics analyzes users' typing patterns—an implicit biometric trait—based on timing and rhythm, while facial recognition uses facial features for identity verification. Individually, both modalities offer distinct advantages; combined, they enhance security and reduce false positive rates. By combining these methods, a multi-modal authentication system can be created that capitalizes on the advantages of both modalities and increases its resistance to fraud and impersonation. Recent studies show that keystroke dynamics

can reach up to 90% accuracy in user identification, and modern facial technologies boast accuracy rates exceeding 95% in optimal conditions. The major contributions in this paper:

- Developing a low computing system for multi modal user authentication using Keystroke dynamics and Facial Recognition.
- Develop a algorithm for recording the keystrokes easily and create a own dataset (Classroom dataset).
- Develop a Resnet architecture from scratch for easy facial Recognition even in occlusion conditions.
- Evaluating the performance of both the model by using evaluation metrics like Accuracy, Precision, Recall and F1-Score
- Comparison of the results with the SOTA (state-of-the-art).

The research is further discussed in such a way that, section 2 gives overview of recent works that used keystroke dynamics and facial recognition. Section 3 discusses about the proposed model, section 4 discusses about the result and Finally the paper is concluded in the section 5 this section also gives insights into further research

II. Literature Survey

This section about the key researches in the keystroke dynamics and the facial detection. The recent works in the keystroke dynamics are as follows: Initially the authors in the [6] provided an in-depth analysis of security practices based on keystroke dynamics, comparing physiological and behavioral biometrics. The research highlights keystroke dynamics' advantages, such as high data accessibility and minimal user disruption. By calculating dwell and flight times, it offers a robust authentication framework. The research in [7] aims to assess the viability of using keystroke dynamics for emotion recognition. This paper evaluates data acquisition, extracted features, classification methods, and performance metrics from existing studies and also introduces a web application to create new datasets. The authors in [8] proposes a new method for free text keystroke dynamics using an instance-based graph comparison metric. The algorithm significantly reduces the number of keystrokes needed for authentication, making it faster and also reliable.

The researchers in [9] presents a unique framework which applies time frequency analysis to keystroke dynamics for user authentication. Using dynamic time warping and Wigner distribution, the methods captures both time and frequency based features. The study achieved better accuracy than traditional approaches. The authors in [10] explores user authentication framework leveraging dynamics in online examinations. It combines both static and continuous authentication methods using edge computing architecture and Gaussian based anomaly detection for enhanced accuracy. the authors in [11] introduced WiPass, a novel system that leverages WIFI signals and keystroke dynamics for device free authentication using deep learning models. Hight accuracy was also seen, but environmental interferences could affect the performance. The study in [12] focuses on utilizing machine learning to identify fraudulent patterns through keystroke dynamics in remote working scenarios, also worked on offering real time remote monitoring without user awareness. While the study highlighted its effectiveness in monitoring, but lacked comparison with other biometrics like facial recognition. Finally the study in [13] focused on deep learning and data fusion techniques to enhance keystroke dynamics-based authentication, particularly focused on critical infrastructures. Used two state of the art data fusion techniques, these approaches adapt very well to different user typing behavior and achieved high accuracy.

The recent works in the facial recognition are as follows: Initially the researchers in [14] presented a face gender classification algorithm that involves face detection, pre processing, and machine learning classification using vectors generated by one face recognition model. The method achieved high recognition rates on datasets like FEI and SCIEN. The study in [15] focuses on enhancing face recognition performance with occluded faces, such as those wearing masks. It introduces an efficient algorithm using CNN and VGG models to improve recognition of partially visible faces and achieved 90% accuracy on top half facial images. The authors in [16] proposed a face recognition and tracking system for surveillance applications to identify and trace individuals using multi camera networks and deep learning methods like Face net and One-shot learning. It also addresses challenges like occlusion and tracking across camera networks.

The authors in [17] proposes an automated system for recording student's attendance using face recognition. By leveraging OpenCV, the system captured student faces and matches them against a database for an efficient and accurate attendance records. The study in [18] demonstrates an approach for face detection and recognition using OpenCV and few python libraries. Focused more on handling challenges like variable lighting and facial poses, also provides practical applications in security and online proctoring. The researchers in [19] introduces a multilevel system for face recognition using component-based classifiers to make soft decisions on facial components. Authors combined local classifiers' decisions; the system enhances the reliability of face recognition.

III. Methodology

Fig. 1 displays the suggested model workflow, and the functionality of each block is explained further below.

A. Keystroke Dataset Creation

The creation of classroom dataset consists of creating 2 CSV files. The first file contains the user credentials. The attributes in this CSV file are username, password and email_id. The second file consists of the keystrokes of the persons using the Algorithm. 1. This file contains the keystroke of each user typing a string "CS@prjt21". This reason for selecting this string is it contains all the combination of lowercase, upper case letters along with numerical and special characters and the letters in this string spread across the keyboard [20]. The

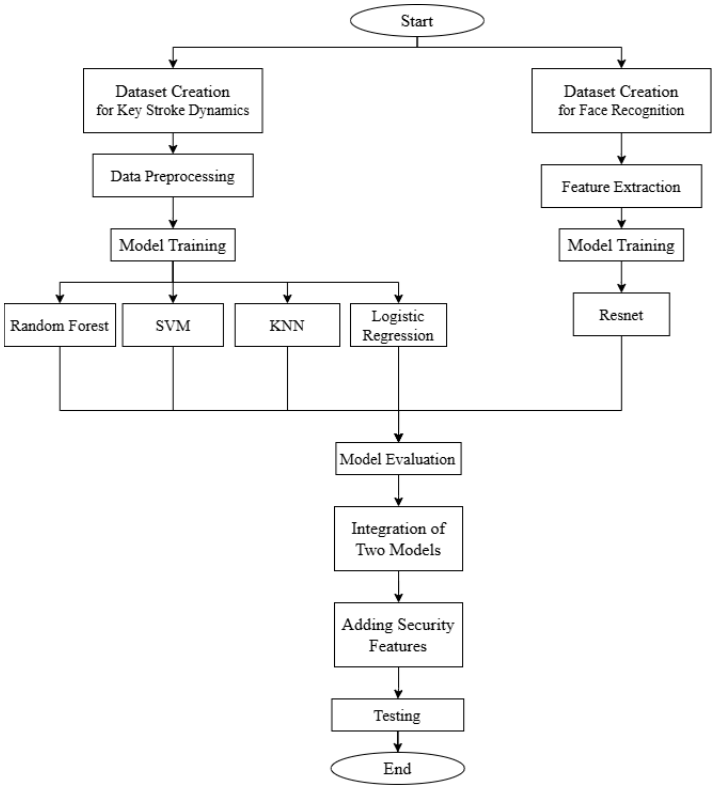

Fig. 1: Flowchart of the Proposed Model

attributes in this file are username, H(Hold Time), UD(Up-down Time), DD(Down-Down Time) time for every character. Hold time is the duration between pressing and releasing the same key. Down-down time measures the interval between pressing consecutive keys, while up-down time records the period between releasing one key and pressing the next. The calculation of the H, DD, and UD periods is shown in Fig. 2.

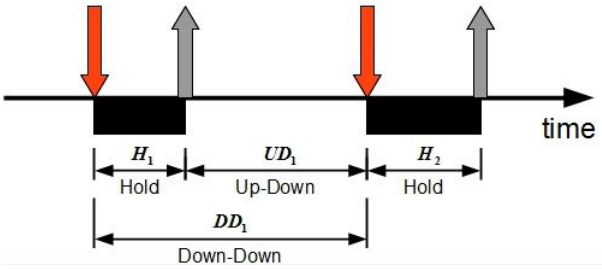

Fig. 2: Key timing metrics in keystroke dynamics

B. Data Pre-Processing

After data collection, null values are identified and replaced with the average values specific to each user. Additionally, user labels (usernames) are converted into numerical representations to simplify the training process and reduce complexity.

C. Model Training for Keystrokes

After the data pre-processing the model is trained using the different models viz. Random Forest, SVM, KNN, Logistic Regression. The best parameters for these model are found out using the Grid Search algorithm. The following gives the brief about each of the model used for the training:

- Logistic Regression: Logistic Regression models authentication probability based on keystroke features, using a linear classification approach.
- Random Forest: Random Forest uses multiple decision trees to reduce overfitting and improve keystroke classification accuracy.
- SVM: SVM identifies the optimal hyperplane to separate genuine and imposter keystroke data for accurate classification.
- KNN: KNN classifies keystroke patterns based on feature proximity, offering a simple yet effective approach to authentication [21].

Algorithm 1 Keystroke Dynamics Data Capture

1. **Input:** *user_credential* & *keypattern* – Username and password of the individual, along with a pre-defined sequence to collect data for key strokes.
2. **Output:** CSV file with columns representing *Username*, *Hold Times*, *Down-Down Times*, and *Up-Down Times*
3. Initialize timing metrics: Hold (H), Down-Down (DD), and Up-Down (UD) times.
4. Ask User to type String (ex: *CS@prjt21*) multiple times to collect keystroke patterns.
5. FOR : each repetition of the password entry
6. FOR: each character in the password
7. Capture *press_time* when the key is pressed down.
8. Capture *release_time* when the key is released.
9. Compute *Hold Time (H)* for the character as:

$$H = release\_time - press\_time$$

10. END FOR
11. FOR: each pair of consecutive characters in the password
12. Compute *Down-Down Time (DD)*:

$$DD = press\_time[next\_key] - press\_time[current\_key]$$

13. Compute *Up-Down Time (UD)*:

$$UD = press\_time[next\_key] - release\_time[current\_key]$$

14. END FOR
15. END FOR
16. Save the recorded dynamics into a csv file.

D. Face Recognition Dataset

For each individual in the user credentials dataset, a corresponding image is collected to create a facial recognition dataset. This process ensures that every user is represented by a unique facial image, which is then used to train and evaluate the facial recognition model.

E. Feature Extraction

After creating the dataset, the 68 facial landmarks are extracted using the pretrained dlib library. Subsequently, the

VGG-16 pretrained model is utilized to extract 128 facial discriminative features, which are then saved into a CSV file for use in model training. This process enables the capture of distinct facial characteristics that are crucial for accurate facial recognition.

F. Model Training for face recognition

Using the 128 facial discriminators the Resnet model is trained. The ResNet model consists of 20 layers, including one fully connected layer, an initial convolutional layer, sixteen residual blocks, and a final global average pooling layer [22].

G. Model Evaluation

The model evaluation for both keystrokes and facial recognition is done considering the 4 parameters i.e, Accuracy, precision, Recall, F1-score with the corresponding formulas provided in Eqns. 1, 2, 3 and 4. Where TP is true positive, TN is true negative, FP is false positive and FN is false negative.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

$$Recall = \frac{TP}{TP + FN} \tag{3}$$

$$F1 - Score = \frac{2 * Precision * Recall}{Precision + Recall} \tag{4}$$

H. Integration of Models

The final authentication result is calculated by combining the outputs from both models. This method lowers the possibility of false positives or negatives while offering a more thorough and trustworthy user verification procedure.

I. Adding Security Features

To enhance security, if a false user passes the keystroke dynamics test but fails facial recognition, the system triggers a warning to the legitimate user. The warning includes a photo of the person attempting to log in, alerting the user to potential security threats. This adds an extra layer of protection to the authentication process.

IV. Implementation And Results

For the implementation of the proposed model Python3 is used. Starting with creation of the classroom dataset. The dataset has been created by collecting the keystrokes of 81 people typing the string ”CS@prjt21” 30 times each using the Alg. 1 and pre-processing is done to fill the null values with the average speech of the user based on the remaining attributes. The dataset is shown in Table. I & II. Table. I is the sample of data in ”user_credential.csv” having the username, password and email_id after pre-processing. Table. II is the sample of ”keystrokes.csv” file having the keystrokes of the people after pre-processing. Parallelly the images of these people are also for creating the dataset for the face recognition. After the creation of the dataset for the face recognition the landmarks are extracted as shown in the Fig. 3 using the landmarks he 128 face discriminators are found using the pretrained VGG-16 model these features are shown in Table III.

TABLE I: Sample of user_credentials.csv file

username	password	email_id
satvik	satvik17	satviktaduvai@gmail.com
suhas	coolsu12	ssuhas24@gmail.com
praveen	12345678	praveenkarthik2290@gmail.com
...	...	...
praveen	wav2sync	bl.en.u4eac21075@bl.students.amrita.edu

TABLE II: Sample of keystrokes.csv file

username	H.ch1	H.ch2	...	DD.ch8.ch9	UD.ch8.ch9
satvik	0.0584	0.0636	...	0.2227	0.1176
suhas	0.0909	0.0857	...	0.0942	0.1062
praveen	0.111	0.1324	...	0.1735	0.0735
...	...	...	...	...	...
wav2sync	0.141	0.1583	...	0.2044	0.0992

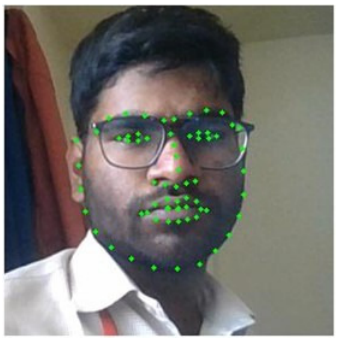

Fig. 3: Landmarks of the face Extracted

After the completion of the pre-processing the models are trained and the results of the key stroke model are shown in the Table. IV & V. As shown in the Tables IV & V the Random forest model is performing best with a training accuracy of 96.9% and testing accuracy of 93.4%.

The face recognition model demonstrates excellent performance across key evaluation metrics. It achieves an accuracy of 96% of the predictions were correct overall. The precision score of 1.00 signifies perfect precision, meaning there were no false positives among the positive predictions. Furthermore, the recall of 0.96 highlights the model’s ability to correctly identify 96% of all actual positives. Lastly, the F1 Score stands at 0.96, reflecting a strong balance between precision and

TABLE III: Features of the faces Extracted

Name	Feature-1	Feature-2	...	Feature-127	Feature-128
satvik	0.0741	0.095	...	0.191	-0.199
suhas	-0.0864	0.0179	...	0.027	0.050
praveen	0.1629	0.0930	...	0.475	0.1795
...	...	...	...	...	...
wav2sync	-0.1718	0.1058	...	0.0137	0.0235

TABLE IV: Model Performance Metrics - Training

Model	Accuracy	Precision	Recall	F1-Score
KNN	90.4	92.1	90.4	90.5
SVM	94.7	96.2	94.7	94.8
Logistic Regression	81.7	83.5	81.6	80.9
Random Forest	96.9	98.4	96.9	97.1

TABLE V: Model Performance Metrics - Testing

Model	Accuracy	Precision	Recall	F1-Score
KNN	81.8	85.4	81.8	81.3
SVM	87.5	90.0	87.5	87.4
Logistic Regression	73.8	74.9	75.4	72.5
Random Forest	93.4	95.0	93.4	93.2

recall.

After the successful implementation of both keystroke and face recognition models these two models are integrated to form a multi-modal user authentication system. The results after integration of both the model are discussed in the further figures. If the user enters the password wrong then the model will print the message as password is wrong and the authentication fails as shown in the Fig. 4.

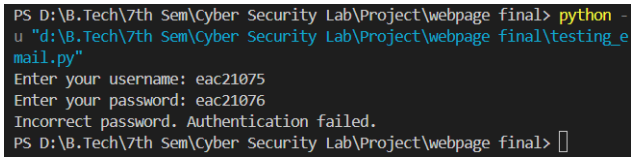

Fig. 4: Output of Password Wrong

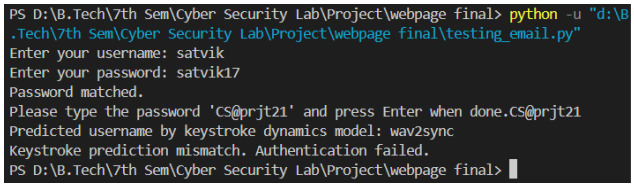

Fig. 5: Output of Keystrokes Wrong

If the password is correct and the keystrokes of the person is not matched then the model will print the message and the authentication fails as shown in the Fig. 5. If the key stroke is matched but the face is mot matched after three attempts then the model will send a warning mail to the actual user telling that an unauthenticated person is logging into your account and a photo of the person is also attached in the mail. The model's output is shown in the Fig. 6, Fig. 7 shows the mail sent form the server and Fig. 8 shows the received mail by the user.

If the user is authenticated by both key strokes and Face recognition then the user will be allowed to access their account as shown in the Fig. 9.

Subsequently, The performance of the keystroke i.e, classroom dataset was compared with the benchmark dataset provided by the CMU School of Computer Science [23]. The comparison utilized identical models, with accuracy serving as

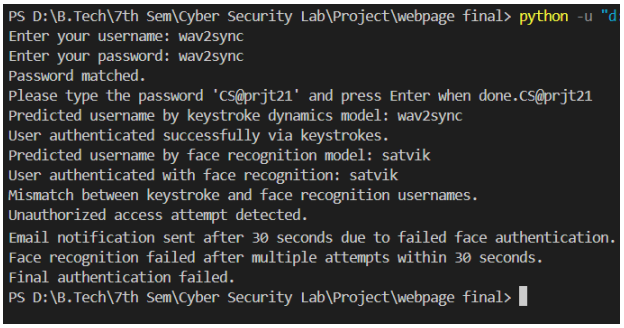

Fig. 6: Output of Face Recognition Wrong

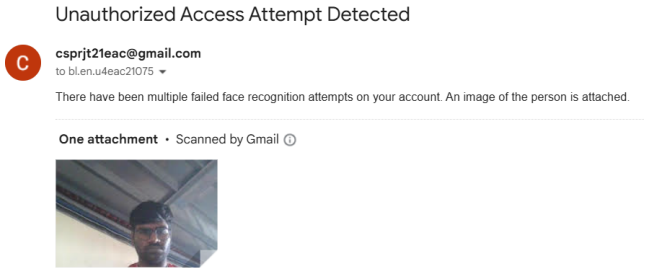

Fig. 7: Mail sent form Server

the evaluation metric. Table. VI presents a detailed comparison of both datasets. The CMU dataset comprises data from 51 users, each typing 400 times, while our dataset consists of 81 participants, each typing 30 times. Despite the smaller size of our dataset, the models demonstrated comparable performance to the benchmark dataset, indicating their strong and optimal effectiveness.

Finally the performance of the Fcerecognition model is also compared with the SOTA models as shown in the Table. VII.

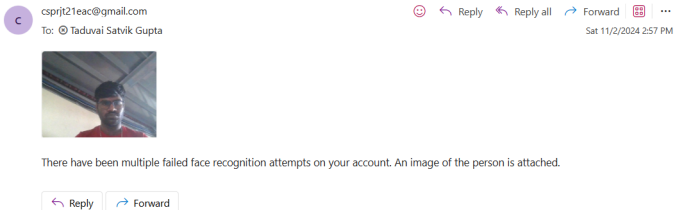

Fig. 8: Mail Received by the user

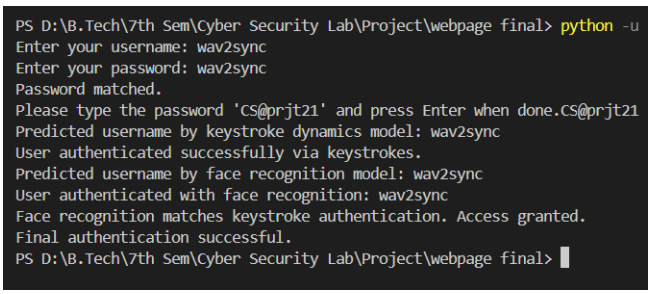

Fig. 9: Login in by the correct User

TABLE VI: Comparison of Model Performance on Classroom Dataset vs. CMU Dataset

Model	Our Dataset (%)	CMU Dataset (%)
KNN	81.8	73.3
SVM	87.5	87.6
Logistic Regression	73.8	83.1
Random Forest	93.4	93.5

TABLE VII: Comparison of Face recognition Model with SOTA

Author(Year)	Model	Accuracy
Lin zhi-heng et al.(2019) [24]	Aritificial Neural Networks	85%
P. A. Kumar et al.(2022) [25]	Haar Cascade, LBPH	85%
S Geerthik et al.(2024) [26]	KNN	94.32%
R. K. Reddy et al. (2024) [27]	Deep Face Learning	95%
Proposed Model (2024)	**Resnet**	**96%**

V. Conclusion And Future Scope

This study develop a multi-model user authentication technique by leveraging both the keystrokes and biometrics of the user. By using the machine learning techniques such as KNN, SVM, Random Forest and Logistic Regression foe the keystroke detection and the Deep learning model Resnet for the facial recognition. This study also proposes a algorithm to create a classroom dataset for the keystroke dynamics. The model performs more optimal by achieving a 93.4% accuracy for the keystroke detection and 96% accuracy for the facial recognition. The proposed models are also performing better compared to the SOTA model.

Future improvements for the authentication system could involve using advanced deep learning models such as RNNs or LSTMs to enhance keystroke recognition accuracy, especially for large datasets. Integrating CNNs or transfer learning techniques could optimize feature extraction and training efficiency. Facial recognition can be made more robust by employing GANs for data augmentation and Vision Transformers (ViTs) to handle occlusions like masks or sunglasses. Combining keystroke and facial data through multi-modal deep learning frameworks and feature fusion would strengthen overall authentication reliability. Implementing encryption methods such as homomorphic encryption and differential privacy will secure user data while adhering to evolving cybersecurity regulations. Lastly, continuous authentication can be added to monitor user behavior throughout a session and detect anomalies in real time.

References

[1] TechTarget, "What is user authentication?," SearchSecurity, 2021. https://www.techtarget.com/searchsecurity/definition/user-authentication

[2] G. D. Maayan, "User Authentication Methods & Technologies to Prevent Breach," ID R&D, Feb. 07, 2020. https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/

[3] "Identity Theft Resource Center 2023 Annual Data Breach Report Reveals Record Number of Compromises; 72 Percent Increase Over Previous High," ITRC, Jan. 25, 2024. http://surl.li/izzyxm

[4] Verizon, "2023 Data Breach Investigations Report: frequency and cost of social engineering attacks skyrocket," Jun. 06, 2023. https://www.verizon.com/about/news/2023-data-breach-investigations-report

[5] N. Hegde and S. Sankaran, "Toward an Adversarial Model for Keystroke Authentication in Embedded Devices," Lecture notes in electrical engineering, pp. 29–40.

[6] P. Kumar, S. Seth, K. Bajaj and S. Rawat, "Diverse Security Practices and Comparison on Key Stroke Dynamics," 2019 8th SMART, Moradabad, India, 2019, pp. 305-309.

[7] A. Maalej and I. Kallel, "Does Keystroke Dynamics tell us about Emotions? A Systematic Literature Review and Dataset Construction," 2020 16th IE, Madrid, Spain, 2020, pp. 60-67.

[8] B. Ayotte, M. Banavar, D. Hou and S. Schuckers, "Fast Free-Text Authentication via Instance-Based Keystroke Dynamics," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 2, no. 4, pp. 377-387, Oct. 2020.

[9] R. Toosi and M. A. Akhaee, "Time–frequency analysis of keystroke dynamics for user authentication," Future Generation Computer Systems, vol. 115, pp. 438–447, Feb. 2021.

[10] Z. Chen, H. Cai, L. Jiang, W. Zou, W. Zhu and X. Fei, "Keystroke Dynamics Based User Authentication and its Application in Online Examination," 2021 IEEE 24th CSCWD, Dalian, China, 2021, pp. 649-654.

[11] Y. Gu et al., "Secure User Authentication Leveraging Keystroke Dynamics via Wi-Fi Sensing," in IEEE Transactions on Industrial Informatics, vol. 18, no. 4, pp. 2784-2795, April 2022.

[12] P. Panda, A. Tripathy and K. C. Bhuyan, "Detecting Fraudulent Pattern Through Key Stroke Dynamics Using Machine Learning Algorithm," 2024 ASSIC, Bhubaneswar, India, 2024, pp. 1-4.

[13] Arnoldas Budžys, O. Kurasova, and V. Medvedev, "Integrating deep learning and data fusion for advanced keystroke dynamics authentication," Computer Standards & Interfaces, vol. 92, pp. 103931–103931, Sep. 2024.

[14] Y. Lin and H. Xie, "Face Gender Recognition based on Face Recognition Feature Vectors," 2020 IEEE 3rd ICISCAE, Dalian, China, 2020, pp. 162-166.

[15] S. Alfattama, P. Kanungo and S. K. Bisoy, "Face Recognition from Partial Face Data," 2021 APSIT, Bhubaneswar, India, 2021, pp. 1-5.

[16] S. P. Nair, K. Abhinav Reddy, P. K. Alluri, and S. Lalitha, "Face recognition and tracking for security surveillance," Journal of Intelligent & Fuzzy Systems, pp. 1–9, May 2021.

[17] A. Kumar, S. Samal, M. S. Saluja and A. Tiwari, "Automated Attendance System Based on Face Recognition Using Opencv," 2023 9th ICACCS, Coimbatore, India, 2023, pp. 2256-2259.

[18] A. Kumari Sirivarshitha, K. Sravani, K. S. Priya and V. Bhavani, "An approach for Face Detection and Face Recognition using OpenCV and Face Recognition Libraries in Python," 2023 9th ICACCS, Coimbatore, India, 2023.

[19] . M. Opanasenko, Sh. Kh. Fazilov, S. S. Radjabov, and Sh. S. Kakharov, "Multilevel Face Recognition System," Cybernetics and Systems Analysis, vol. 60, no. 1, pp. 146–151, Jan. 2024.

[20] "How To Choose a Strong Password : TechWeb : Boston University," www.bu.edu. https://www.bu.edu/tech/support/information-security/security-for-everyone/how-to-choose-a-strong-password/

[21] S. Lalitha, T. S. Gupta, A. Thelu, V. K. Reddy and V. C. Reddy, "Predictive Modeling for Real-Time Customer Lifetime Value," 2024 15th ICCCNT, Kamand, India, 2024, pp. 1-6.

[22] P. G. Sathvik, M. R Kumar, G. H Neeli, I. Y. Narasimha, T. Singh and P. Duraisamy, "RESNET-50, CNN and HNN Medical Image Registration Techniques For Covid-19, Pneumonia and Other Chest Ailments Detection," 2022 13th ICCCNT, Kharagpur, India, 2022, pp. 1-7.

[23] "Keystroke Dynamics - Benchmark Data Set," www.cs.cmu.edu. https://www.cs.cmu.edu/ keystroke/

[24] Z. -h. Lin and Y. -z. Li, "Design and Implementation of Classroom Attendance System Based on Video Face Recognition," 2019 ICITBS, Changsha, China, 2019, pp. 385-388.

[25] R. Azhaguraj, P. A. Kumar, S. Kadalarasan, K. Karthick and G. Shunmugalakshmi, "Smart Attendance Marking System using Face Recognition," 2022 6th ICOEI, Tirunelveli, India, 2022, pp. 1784-1789.

[26] A Senthil G, S Geerthik, R. Karthikeyan, and G Keerthana, "Face Recognition based Automated Smart Attendance using Hybrid Machine Learning Algorithms and Computer Vision," Jun. 2024, pp.606-611.

[27] J. Srikanth, R. K. Reddy, P. J. Reddy, K. Rahul and C. Bharath, "Artificial Intelligence based Multi-Face Recognition and Attendance Marking System," 2024 ICIPCN, Dhulikhel, Nepal, 2024, pp. 47-51.