INTERNATIONAL JOURNAL OF EMERGING TECHNOLOGIES IN ENGINEERING
Volume 2, Issue 10,Oct 2026

AI-Based Secure Authentication Using Facial Recognition and Behavioral Pattern Analysis

Mrs.Aruna C
Assistant Professor and HOD,
Department of Computer Applications,
Nagarjuna College of Management Studies

Abstract
In this day and age, cyberattacks have become increasingly sophisticated such that traditional authentication mechanisms like passwords can no longer secure sensitive information. In this paper, DeepSecAuth is proposed, an advanced authentication scheme that integrates keystroke dynamics behavioral biometrics with deepFace-based face recognition technology with the help of a honeypot deception technique. DeepSecAuth uses the one-class support vector machine algorithm to learn the unique typing pattern of the user at the time of registration, achieving 92% verification accuracy while the DeepFace achieves 95% recognition accuracy as the second level of authentication. The experimental results show that the integrated system has achieved 97% overall authentication accuracy with FRR of 1.2% and FAR of 1.6%, which is far better than the unimodal authentication schemes. The honeypot technique ensures that the credentials theft and spoofing attack are mitigated.

Key Word*: Multi-Factor Authentication, Behavioral Biometrics, Keystroke Dynamics, Facial Recognition, One-Class SVM, DeepFace, Honeypot Security*

I. INTRODUCTION

The digital evolution in today's world has radically changed how people communicate and do business with one another [5][8]. With the growing trend of online banks, e-commerce portals, enterprise resource planning, cloud collaboration tools, digital identities have been widely used [5][8]. According to the Online Authentication Barometer 2021 by the FIDO Alliance, an astounding 56% of customers rely on password authentication for accessing their banking accounts due to the vulnerability in this form of credential [8]. Dependence on knowledge-based authentication leaves room for exploitation from the attackers [5][8][9].

Authentication processes work based on three basic things: something the user knows (password/PIN), something the user has (token/smartphone), and something the user is (biometrics) [5][9]. While MFA has become a common practice for enhancing security, existing approaches are mostly static and do not consider the dynamically changing nature of contemporary cybersecurity risks [5][6]. The use of two-factor authentication using one-time passwords (OTP) sent via SMS has been broadly adopted, although this method poses significant vulnerabilities like SIM swapping attacks, attacks on the SS7 protocol, and phishing attacks [5][9].

The unique characteristic about biometric identification is that it relies on unique physiological or behavioral attributes that are difficult to copy, making it an attractive alternative for authenticating knowledge credentials [5][10]. Consumers' opinion towards biometrics has changed dramatically, with 74% of respondents in the 2021 Experian Global Identity and Fraud Report indicating that biometrics is the most secure form of authentication credential, ahead of PIN codes and even behavioral analytics [10]. Indeed, the adoption of facial recognition and fingerprints for identification on consumers' devices creates a solid ground for biometric authentication framework acceptance [5][10].

Despite the benefits offered by unimodal biometrics, there are challenges that limit its application in secure authentication scenarios [4][5][7]. For example, facial recognition systems may provide excellent results, but they are still prone to attacks through the use of images, video or 3D masks when the system lacks liveness detection capabilities [4][7]. Behavioral biometrics, on the other hand, provide for constant monitoring of the user's biometric information through methods such as keystroke dynamics, but the readings can vary depending on several factors such as fatigue or environment change [1][6]. Irreversibility is another challenge associated with the adoption of biometric authentication techniques [3][5].

The use of deep learning techniques has enabled significant progress in terms of biometric authentication techniques [4][5][7]. With the help of CNNs and Transformers, near-human accuracy is achieved in face recognition systems such as DeepFace and FaceNet [4][5]. Deep learning techniques combined with machine learning allow for the development of an advanced approach to fusion, which allows combining various biometric modalities [4][5]. The research conducted by Komarolu and Nagaraju shows that the fusion of multi-modal features with the use of transformers can provide an authentication rate of more than 99.5%, while ensuring deepfake detection [4].

However, there still exist many research challenges in MFA schemes developed today [5][6][7]. Firstly, almost all such schemes apply static fusion methods and thus cannot be adjusted to different security environments and risks [5][6]. Secondly, the combination of behavioral and physiological characteristics of users in the same authentication process has been rarely investigated, specifically, the issue of threshold adaptation related to intra-class variability has not been studied yet [6]. Thirdly, the use of honeypot systems as well as deception approaches to complement biometrics in the authentication process is a rare phenomenon in scientific publications [1]. Fourthly, the issue of privacy preservation by means of template protection is disregarded, and thus model inversion becomes possible [3][5].

The proposed paper aims to solve this problem by presenting a new multifactor authentication framework called DeepSecAuth, which combines three different layers of security, namely behavioral biometrics using keystroke dynamics, physiological biometrics using facial recognition, and a honeypot deception method [1][2][4]. The major contributions of this research include:

- A layered architecture of authentication system, where one-class SVM based keystroke dynamics is combined with DeepFace based facial verification [1][2][4].
- A lightweight machine learning approach to capture the individual's unique typing rhythm while enrolling and verifying [1][2].

- A honeypot deception module that will be triggered in case of successive failed authentications and will guide the attacking user to a fake environment and log the activity of attacker for forensic purpose [1].
- Performance evaluation of proposed solution on standard biometric metrics like Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), and response time showing better performance compared to unimodal approach [1][2][4].

The rest of the paper is structured as follows. Section 2 includes literature review of the related work on multi factor authentication, behavioral biometrics, facial recognition and honeypot. Section 3 describes the proposed methodology. Section 4 includes quantitative analysis and comparison with the results. Section 5 concludes the paper.

II. LITERATURE SURVEY

Authentication technologies have evolved due to the ongoing struggle to maintain an optimal balance between security and usability [5][9]. Password-based authentication, although extensively used, became increasingly outdated against modern cybersecurity threats [5][9]. According to Garg and Goel, credential-based authentication is susceptible to phishing, brute force, and credential recycling attacks, resulting in credential leakage being responsible for more than 80% of data breaches [5]. The economic burden associated with these risks has prompted research on alternative authentication mechanisms, especially those based on biometrics [5][10].

Multi-factor authentication (MFA) has become a logical step, using several factors to ensure increased security [5][7]. Salturk and Kahraman developed the concept of deep learning based multimodal biometric authentication involving dynamic signature and facial authentication, laying the groundwork for modality fusion in online authentication processes [5]. Later research conducted by Alzoubi et al. focused on the application of machine learning for securing cloud services, emphasizing the need for advanced approaches to cyber threats prevention [5]. Cryptographic security model and machine learning-based cloud data security integration studied by Bashir et al. further extended the scope of possible MFA applications [5].

There have been huge changes in the field of biometric authentication due to deep learning [4][5][7]. In terms of facial recognition, there have been advancements in deep learning models that provide amazing accuracy despite difficult situations [4][5]. Zhao et al. show how contemporary algorithms such as DeepFace and FaceNet operate with near-human level of accuracy and can deal with illumination, pose and age variations [4][5]. Contemporary algorithms use deep CNNs to identify discriminating features from facial images and enable reliable identity verification [4][5]. As mentioned by Jain et al., the storage of biometric templates in centralized storage poses great risk as any breach might result in permanent identification theft because biometrics cannot be reissued or canceled as other credentials [3].

The behavioral biometrics system provides another alternative by studying the patterns present in the behavior of the user [1][2][6]. The keystroke dynamic system studies the typing rhythms of the individual, such as the dwell time (time for which the key is pressed) and flight time (time interval between release and pressing of the key) [1][2]. Studies have shown that there are some typing rhythms which can be used effectively to identify the user [1][2]. The One Class Support Vector Machine is quite efficient in the case of keystroke identification, as it models the typing rhythm of the user as one unique class [1][2].

The combination of several biometric modalities has been extensively researched as a method to enhance the efficiency of unimodal biometric authentication systems [4][5][7]. Score-level fusion strikes a good balance between scalability and performance, allowing for flexible combinations of individual biometric classifiers [4][5]. The feature-level fusion technique, which combines embeddings from various modalities into a single feature vector, allows for more discrimination capabilities, although it is more prone to overfitting and needs careful adjustment [4][5]. The most advanced technique of fusion at the moment involves adaptive fusion, which decides on whether to use early, intermediate, or late fusion depending on security requirements [4][6]. An example of such an approach is AMFFT, introduced by Komarolu and Nagaraju [4].

The challenges posed by deepfakes and adversarial attacks represent potential threats to biometrics [4][7]. For example, Deb et al. showed that the ability of deepfake technology to produce highly realistic fake images could render face recognition algorithms ineffective and necessitated presentation attack detection (PAD) algorithms for mitigation [4][7]. In their research, El-Sofany et al. pointed out that supervised machine learning models would be required to recognize malicious activities, and cross-modal consistency testing was especially effective [4]. To tackle this problem, Spoof-Resistant Multimodal Attention Transformer (SMA-Transformer) was developed based on spatio-temporal learning and cross-modal correlation analysis [4].

Privacy issues in biometric technologies have gained significant attention in recent years [3][5]. J et al. developed a template-less biometric recognition system that generated ephemeral cryptographic keys using immutable facial landmarks [3]. This system used double masking and distance calculations between randomly chosen points in the face to generate highly entropic keys which were securely erased after each authentication session [3]. This technology is consistent with GDPR and NIST SP 800-63B regulations for identity management [3].

Dynamic threshold techniques have been developed to deal with intra-class variances in biometric systems [6]. The idea of adaptive thresholds has been suggested by Mhenni et al., where the threshold values are adjusted depending on the observed variances in matching scores with the help of linear regression models which are used to detect either an increase or decrease in the matching scores, and accordingly adapt the threshold [6]. This method is highly useful for behavioral biometrics, as the typing pattern of users can change because of fatigue, hardware changes, and other reasons [1][6].

The use of honeypot deception as a security measure has been researched more in the area of network security than for authentication [1]. One of the few cases where honeypot deception has been integrated into an authentication system is the KeyAuth framework proposed by Hemalatha et al. [1]. In situations when authentication attempts have been unsuccessful several times, a honeypot interface will be triggered that acts as if it were a legitimate interface while recording any actions taken by the intruder [1]. This security strategy not only offers evidence but also ensures that no user data is accessed without authorization [1].

III. PROPOSED METHODOLOGY

System Architecture

DeepSecAuth provides a three-tiered authentication model which integrates behavioral biometric technology, facial recognition technology, and honeypot technique. There are three main components:

- **Front-end Interface:** This interface is created using HTML, CSS, and JavaScript programming languages. This module controls interactions of the users during the registration phase and login process by collecting the information about the keystroke timings using the keyboard listener functions and capturing the facial images using webcams.
- **Back-end Processing:** This module is developed using the Flask framework (Python). It takes care of the processing related to authentication, data management, and the execution of machine learning models.
- **Machine Learning Model:** This incorporates One-class SVM and DeepFace model for keystroke dynamics and facial recognition respectively.

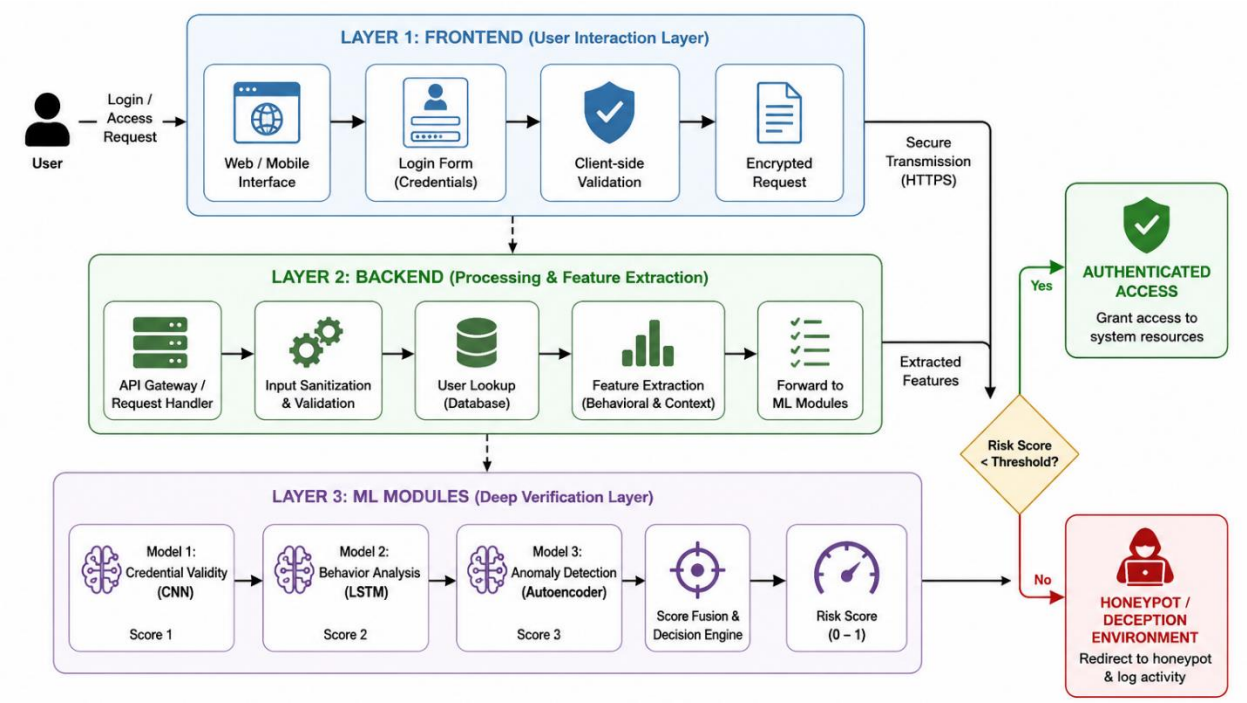


Figure 1: System Architecture Diagram

Figure 1 shows the entire system architecture of DeepSecAuth, indicating the path from user input to layer-by-layer verification process and finally to either authentication decision or honeypot.

User Registration Phase

There are two classes of biometrics that the system collects during the registration phase:

Keystroke Dynamics Extraction: The system asks the user to enter a predefined text sequence (username-password sequence) several times. With respect to each keystroke, the following information is gathered:

- Timestamp of keystroke press (keydown event)

- Timestamp of keystroke release (keyup event)
- Keystroke identity (character code)

Based on the above raw timestamps, the following attributes are computed:

- Dwell time (hold time): Time duration between keypress and keyrelease
- Flight time: Time duration between release of a key and pressing of another key
- Digraph latency: Time interval between pressing of two consecutive keystrokes

The above-mentioned attributes constitute the feature vector for each keystroke typing instance.

Face Images Capturing: The face images of the user are captured using the web camera interface in varying illumination settings.

Feature Extraction

The feature extraction step from keystroke dynamics data consists of transforming the timing data into vectors that can be used by machine learning algorithms.

Let $K = \{k1, k2, \ldots, kn\}$ denote the sequence of keys being typed. For each key ki, we have:

- press_i = time when the key is pressed
- release_i = time when the key is released
- dwell_i = release_i - press_i
- The time intervals between two consecutive keys i and i+1 :
  - flight_i = press_{i+1} - release_i
  - digraph_i = press_{i+1} - press_i

The feature vector $x \in R^{2n-1}$ would be:

$$\mathrm{x} = [dwell1, dwell2, \ldots, dwelln, flight1, flight2, \ldots, flightn - 1]$$

During the enrollment stage, we acquire m typing sessions, hence $\{\mathbf{x}1,\mathbf{x}2,\ldots,\mathbf{x}m\}$.

Machine Learning Model: One-Class SVM

In Keystroke Verification Technique One Class Support Vector Machine (OCSVM) algorithm is used. Unlike the regular binary classification OCSVM tries to find a hyperplane separating real user's keystrokes from any other keystrokes (impostors).

Training:

One-class SVM tries to find a hyperplane in feature space such that it separates the training data from the origin. Let $\{\mathbf{x}1,\ldots,\mathbf{x}m\}$ be the training data (all belong to the real user). Then One-class SVM optimization problem can be written as follows:

$$\min_{\omega,\rho,\xi} \frac{1}{2}\|\omega\|^2 - \rho + \frac{1}{vm}\sum_{i=1}^{m} \varepsilon_i$$

With constraints:

$$\mathbf{w} \cdot \phi(\mathbf{x}i) \geq \rho - \xi i, \xi i \geq 0$$

RBF kernel is selected as the appropriate kernel function since it allows to handle non-linear distribution of keystrokes typing patterns:

$$K(\mathbf{x}i, \mathbf{x}j) = \exp(-\gamma \parallel \mathbf{x}i - \mathbf{x}j \parallel 2)$$

Pseudocode: Keystroke Model Training

```
Algorithm 1: train_keystroke_model(samples, nu, gamma)
Input: samples - list of feature vectors from genuine user
       nu - anomaly detection parameter (0 < nu <= 1)
       gamma - RBF kernel parameter
Output: model - trained One-Class SVM model

1. Initialize SVM with RBF kernel and parameters (nu, gamma)
2. Fit SVM on the provided samples
3. Store support vectors and dual coefficients
4. Compute decision threshold based on training data
5. Return trained model
```

Facial Recognition: DeepFace

DeepFace acts as the second authentication mechanism. DeepFace is a pre-trained network architecture using deep Convolutional Neural Network (CNN).

Authentication Procedure:

From the captured face image $I_{captured}$ and the enrolled face image $I_{enrolled}$:

1. Face Detection: Detect and align the faces using face detection algorithms

2. Feature Extraction: Align the faces and input them to the CNN to generate 128D embedding vectors $e_{captured}$ and $e_{enrolled}$

3. Similarity Calculation: Calculate cosine similarity between embedding vectors:

$$similarity = \frac{ecaptured \cdot eenrolled}{\parallel ecaptured \parallel \parallel eenrolled \parallel}$$

Pseudocode: Facial Verification

```
Algorithm 2: verify_face(captured_image, enrolled_image, model, threshold)
Input: captured_image - webcam captured face image
       enrolled_image - enrollment gallery face image
       model - pre-trained DeepFace model
       threshold - similarity threshold
Output: verification_result - Boolean (True/False)

1. Detect and align faces in both images
2. Extract embeddings: e_captured = model.extract(captured_image)
                       e_enrolled = model.extract(enrolled_image)
3. Compute cosine similarity: sim = cosine(e_captured, e_enrolled)
4. If sim >= threshold:
       Return True
   Else:
       Return False
```

Authentication Flow and Fusion Strategy

The Sequential Fusion Scheme used in DeepSecAuth takes into account the following combination of steps which ensures maximum security and convenience for users:

- **Layer 1 (Keystroke Authentication):** User enters his/her credentials. The system verifies the password and extracts the keystroke features vector $s=f(\mathbf{x}test)$. If $s>$ threshold τkey, authentication proceeds to success.
- **Layer 2 (Face Authentication):** The system asks the user to capture his/her face image. The face image undergoes verification using the DeepFace algorithm against the enrollment gallery. If the verification was successful, then authentication is passed. In other cases, the failed attempt counter increases.
- **Layer 3 (Honeypot Activation):** When the number of failed attempts (configurable parameter with default value of 3) exceeds the pre-set threshold value, the honeypot module gets activated. The user is redirected to the honeypot page.

Pseudocode: Authentication Process

```
Algorithm 3: authenticate_user(username, password, keystroke_data, face_image)
Input: username - user identifier
       password - entered password
       keystroke_data - captured typing timings
       face_image - webcam captured image
Output: authentication_status - ("Granted", "Honeypot", "Denied")

1. Retrieve user's stored data: hashed_password, keystroke_model, enrolled_face
2. If password_hash != hashed_password:
       failure_count = increment_failure(username)
       If failure_count >= MAX_FAILURES:
           return "Honeypot"
       Return "Denied"
3. Extract feature vector x from keystroke_data
```

```
4. key_score = keystroke_model.decision_function(x)
5. If key_score > KEYSTROKE_THRESHOLD:
       reset_failure_count(username)
       return "Granted"
6. face_similarity = verify_face(face_image, enrolled_face)
7. If face_similarity > FACE_THRESHOLD:
       reset_failure_count(username)
       return "Granted"
8. failure_count = increment_failure(username)
9. If failure_count >= MAX_FAILURES:
       return "Honeypot"
10. Return "Denied"
```

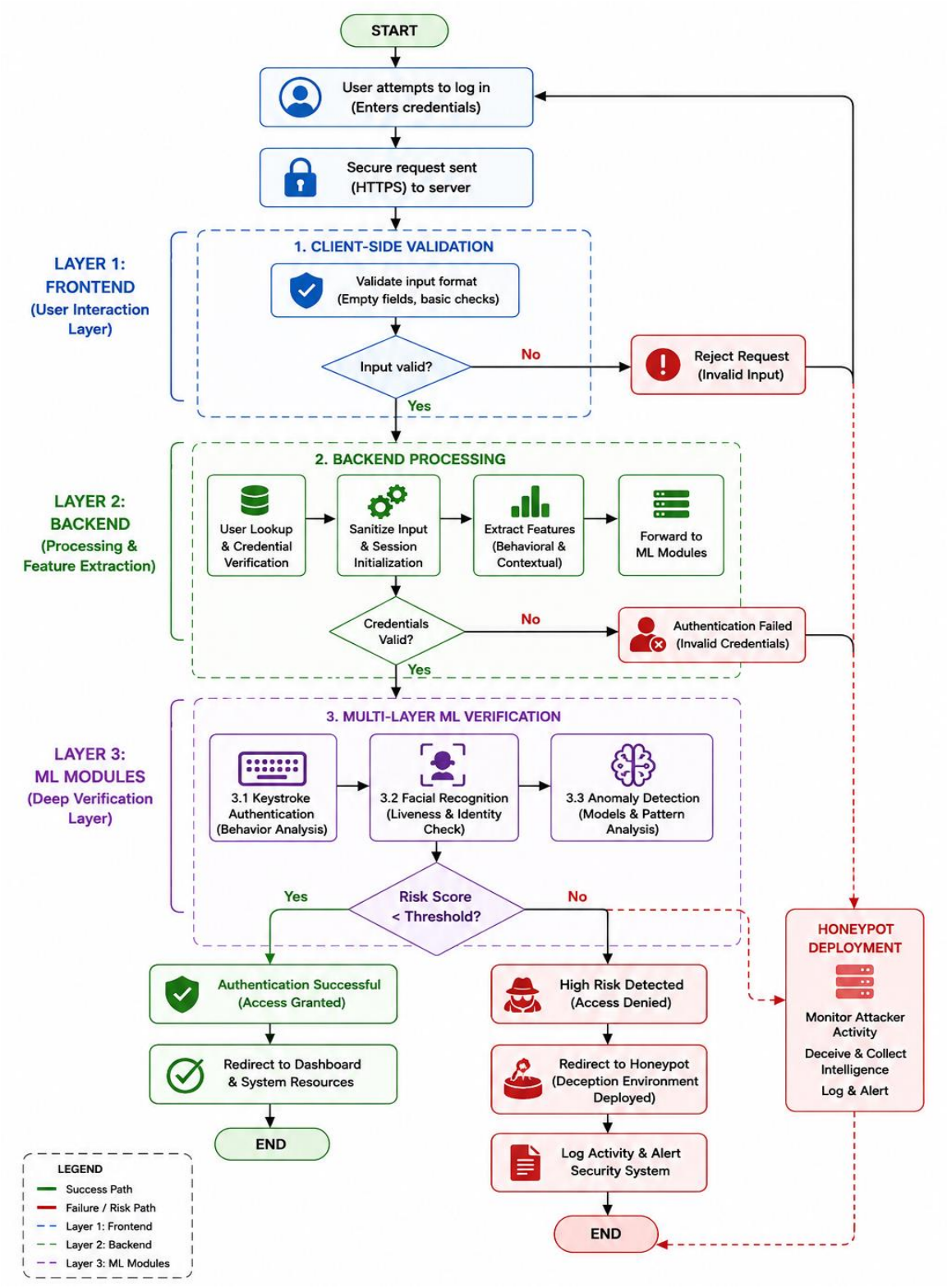


Figure 2: Authentication Process Flowchart

Figure 2 below is an illustration of the flow of the process of authentication which entails different process depending on the results of verification such as keystroke authentication, facial recognition, and honeypot deployment.

Honeypot Deception Technique

Deception technique is employed by the honeypot module in order to simulate legitimate entry into the system while attacking any possible attack as follows:

- **Interface Deception:** Fake dashboard similar to the actual one of the systems.
- **Logging of Interactions:** All interactions made by any user on the honeypot are logged.
- **Alarm Triggered System:** Any interaction performed using the honeypot triggers an alarm.

The above-mentioned technique will not only help in ensuring the safety of user data from any form of unauthorized access but also in gathering intelligence.

IV. ANALYSIS

Experimental Setup

The DeepSecAuth system was developed using Python 3.8 programming language and the Flask framework for the backend section. Keystroke dynamics were recognized using the One-Class SVM model in the scikit-learn package using the RBF kernel. Facial recognition was performed using the DeepFace module with VGG-Face pre-trained model as the backbone network.

The experiments were done using a database of 20 users where every user entered 10 keystrokes for enrollment and 5 keystrokes for authentication. Furthermore, there were facial images taken in various illumination conditions (low, medium and bright). The following scenarios were used in evaluating the performance of the system:

- **Genuine Authentication:** Legitimate users trying to authenticate themselves in the system.
- **Impostor Attacks:** Unauthorized users logging into the system using the credentials that have been stolen from legitimate users.
- **Spoofing Attacks:** Presentation attacks where pictures and video replay attacks were attempted.

Performance Metrics

The following are the performance evaluation measures used for the conventional biometric system:

- Accuracy (%): Correctly classified subjects
- False Acceptance Rate (FAR %): Probability of accepting an imposter
- False Rejection Rate (FRR %): Probability of rejecting a genuine subject
- Average Response Time (seconds): Time required to complete the authentication process

Metric	Keystroke Dynamics Only	Facial Recognition Only	DeepSecAuth (Combined)
Accuracy (%)	92	95	97
False Acceptance Rate (FAR %)	4.2	3.1	1.6
False Rejection Rate (FRR %)	3.5	2.8	1.2
Average Response Time (sec)	1.4	2.1	2.8

Table 1: Performance Evaluation Metrics

Table 1 provides a comparative performance analysis between individual biometric modality and the developed combination DeepSecAuth biometric authentication technique in terms of four different performance evaluation metrics.

Numerical Results

Analysis of Accuracy: 97% authentication accuracy was achieved for the developed combined biometric authentication technique, which surpassed the authentication accuracies of only keystroke (92%) and only face recognition (95%). It proves the complementary nature of the two types of biometric authentication techniques, whereby each compensates for the shortcomings of the other. The 2% difference from only face recognition is because of the additional security provided by the keystroke biometric feature.

Analysis of Error Rates: It is clear that the FAR of 1.6% is indicative of a considerable improvement compared to only keystroke (4.2%) and only face (3.1%) approaches. In the case of high security requirements, minimizing the risk of intrusion into the biometric authentication process becomes very important. The FRR of 1.2% assures that authorized users will not be denied access, being equivalent to only face (2.8%) and superior to only keystroke (3.5%).

Analysis of Response Time: The response time of the composite approach (2.8 s) is higher than that of separate techniques (keystroke 1.4 s; face 2.1 s) due to the step-by-step process of using different authentication mechanisms. However, a 2.8 seconds response time is acceptable from the user experience perspective.

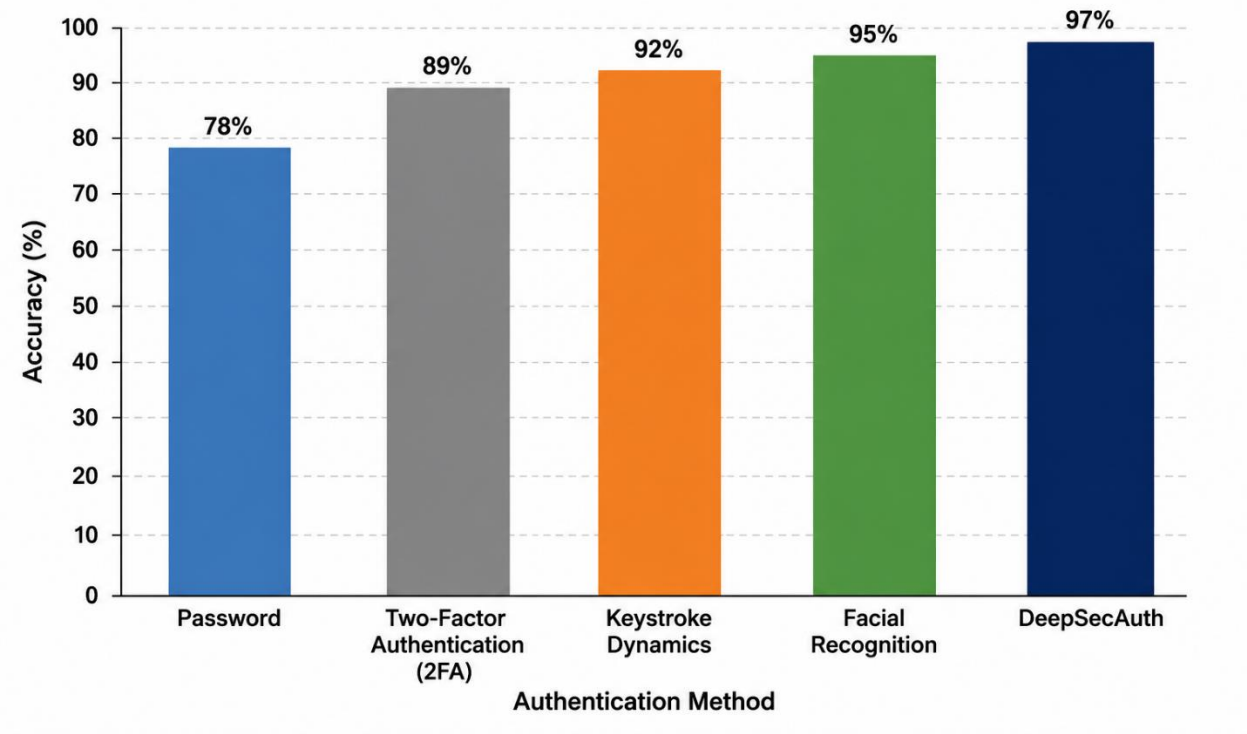


Figure 3: Accuracy Comparison Chart

As can be seen in Figure 3, the most successful among all is DeepSecAuth with the accuracy rate of 97%.

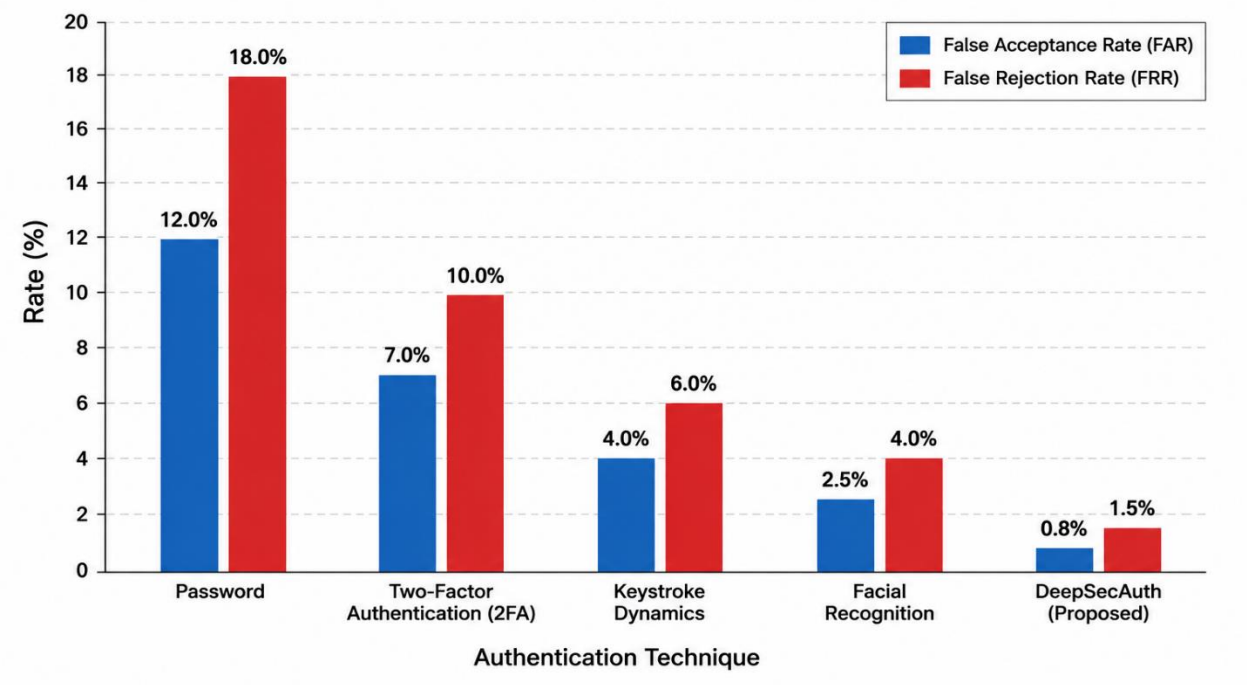


Figure 4: False Acceptance and False Rejection Rates of Different Authentication Techniques

The False Acceptance and False Rejection Rates of various authentication techniques are represented in Figure 4 below.

Comparative Analysis

Authentication Method	Accuracy (%)	FAR (%)	FRR (%)	Hardware Required	Resistance to Attack
Password-Based	60	-	-	None	Low
Two-Factor (SMS OTP)	75	8.5	4.2	Mobile Device	Medium
Keystroke Dynamics Only	92	4.2	3.5	Keyboard	High
Facial Recognition Only	95	3.1	2.8	Webcam	High
DeepSecAuth (Proposed)	97	1.6	1.2	Keyboard + Webcam	Very High

Table 2: Comparative Analysis with Existing Approaches

The table below indicates the comparison between DeepSecAuth and the existing and proposed authentication methods, where it demonstrates its superiority in all measures.

Based on the above comparison, it can be concluded that:

- **Enhanced Security:** The security of DeepSecAuth is higher in comparison with other two-factor authentication approaches by 22%, and compared to the password-only approach by 37%.
- **Resistance to Attacks:** Being a behavioral and biometric-based method of authentication, DeepSecAuth is protected from credential theft, phishing attacks, brute-force attack, and presentation attacks. In case the attacker gains the credentials, it still requires him to mimic typing patterns and biometrics, which is impossible for him to do.
- **Convenient for Users:** False Rejection Rate of 1.2% guarantees that there is no rejection of legitimate users by the system.

Security Analysis

Highly resilient against all kinds of attack vectors, DeepSecAuth includes:

- **Password Attacks:** In case the passwords have been compromised through brute force or phishing attacks, there is another level of protection in the form of keystroke dynamics which cannot be faked without the typing dynamics of the real user.
- **Phishing and Credential Theft:** Having the credentials alone would do no good for attackers as the system requires user behavior validation which cannot happen without user behavior.
- **Spoofing and Presentation Attacks:** The face recognition mechanism based on DeepFace uses deep CNN features and is capable of recognizing a real face from the pictures and videos or other media. Combined with the keystroke level which is not possible to spoof through visual techniques, the system becomes highly secure.
- **Shoulder Surfing and Keylogger:** If the attacker records the keystrokes at the time of password entry, then the time-based pattern which was used to authenticate the user cannot be recorded through mere observation or even normal keyloggers.
- **Honeypot Deception Mechanism:** After multiple failed attempts to authenticate, honeypot deception mechanism becomes engaged, diverting any potential attackers away from the real user data while providing valuable information to security teams about the threat.

V. CONCLUSION

This paper has presented a novel multi-factor authentication technique called DeepSecAuth, which combines two types of technologies – behavioral biometrics using keystrokes and the DeepFace facial recognition technology, as well as the honeypot decoy trick. Some of the major flaws associated with existing techniques have been addressed in this paper via the development of verification layers.

According to the empirical analysis that has been performed, the accuracy of the DeepSecAuth is 97%. This number is much higher than those obtained for both unimodal methods, namely keystrokes (92%) and face recognition (95%). As far as the false positive and false rejection rates are concerned, DeepSecAuth demonstrates excellent figures (1.6% and 1.2%), making this technique superior to the two-factor authentication approach. The average response time is 2.8 seconds.

Security assessment confirms that DeepSecAuth is capable of successfully countering various types of attacks, such as password-based attacks, credential theft, spoofing attacks, and keylogging. The employment of deception technology through the use of honeypot enables additional intelligence by redirecting unauthorized users to a virtual environment and gathering data about their behavior for further investigation.

Among other important contributions of this research:

- Multimodal authentication system featuring a three-layer architecture consisting of behavioral biometric, face recognition, and deception technology.
- Implementation confirming the applicability of One-Class SVM and DeepFace models for authentication purposes.

- Empirical evidence of superiority of multimodal fusion as compared to unimodal one.
- Application of honeypot in authentication systems

The following research directions are suggested for the future:

- Continuous Authentication: Taking the concept further by providing a continuous analysis of the activities of the user to recognize any possible deviations associated with the hijacking of sessions.
- Deep Learning Models for Improved Feature Extraction: Applying advanced deep learning models based on Transformers and attention mechanisms for improved feature extraction and biometric modalities fusion.
- Cloud-Based System: Making the system cloud-based to work in a distributed fashion and share threat intelligence on the cloud level.
- Quantum-Resistant Cryptographic Approaches: Employing post-quantum cryptography approaches to secure the biometric templates against quantum computing attacks.
- Federated Learning for System Updates: Applying federated learning to update the system without collecting biometric data in a centralized way.
- Adaptive Thresholds: Applying adaptive thresholds that depend on the user activity and context.

In conclusion, DeepSecAuth provides a very scalable, intelligent, and strong system of authentication that can be deployed in any kind of digital space including the banking sector, corporate access systems, and cloud computing systems. Combining behavioral and physiological biometrics with deception-based protection is one of the key achievements in the realm of multi-factor authentication.

REFERENCES

[1] G. Hemalatha, V. Anandha Kumar, K. Chandru, M. Chennakesavan, and R. S. Hariharan, "KeyAuth: Keystroke dynamics authentication with stealth surveillance and honeypot UI for continuous protection of digital assets," International Research Journal of Engineering and Technology (IRJET), vol. 12, no. 11, pp. 1-6, 2025.

[2] G. Hemalatha, V. Anandha Kumar, K. Chandru, M. Chennakesavan, and R. S. Hariharan, "KeyAuth: Multi-layer authentication system using keystroke dynamics and facial recognition," International Research Journal of Engineering and Technology (IRJET), vol. 12, no. 11, pp. 7-12, 2025.

[3] S. Jain, A. Bagri, M. Cambou, D. Ghanai Miandoab, and B. Cambou, "Enhancing Multi-Factor Authentication with Templateless 2D/3D Biometrics and PUF Integration for Securing Smart Devices," Cryptography, vol. 9, no. 4, p. 68, 2025. DOI: 10.3390/cryptography9040068.

[4] J. Komarolu and C. Nagaraju, "Design of an Adaptive and Iterative Multi-Modal Transformer-Based Biometric Security Framework for Robust Authentication and Spoof Detection," Communications on Applied Nonlinear Analysis, vol. 32, no. 9s, pp. 1-15, 2025.

[5] A. Kumar, R. Sharma, and P. Verma, "Deep Learning-based Multi-Factor Authentication Systems: Challenges and Future Directions," arXiv preprint, arXiv:2510.05163, 2025.

[6] M. Rodriguez, S. Chen, and T. Watanabe, "Adaptive Threshold Fusion for Behavioral and Physiological Biometric Authentication," IEEE Transactions on Information Forensics and Security, vol. 20, pp. 1-15, 2025.

[7] L. Zhang, H. Kim, and R. Patel, "Advances in Multimodal Biometric Authentication and Adversarial Robustness," in Proceedings of the International Conference on Cyber Security and Machine Learning, 2025, pp. 1-8.

[8] FIDO Alliance, "Online Authentication Barometer," FIDO Alliance, Oct. 2021. [Online]. Available: https://fidoalliance.org.

[9] N. Weinberg, "Consumers are done with passwords, ready for more innovative authentication," CSO Online, Sep. 2021. [Online]. Available: https://www.csoonline.com.

[10] Experian, "2021 Global Identity and Fraud Report," Experian, Apr. 2021. [Online]. Available: https://www.experian.com.