Hybrid Behavioral Biometric Authentication Using Keystroke and Mouse Dynamics for Continuous User Verification

Shruthi N M
Assistance professor ,
Department of Computer Science and Engineering
JSS Science and Technology university, Mysuru, Karnataka
570006 India
Email: shruthinm@jssstuniv.in

Anushree N R
PG Student,
Department of Computer Science and Engineering
JSS Science and Technology university, Mysuru, Karnataka
570006 India
Email: anushreeramesh4@gmail.com

***Abstract*—** The commonly used user authentication techniques such as passwords/PINs can be vulnerable to attacks conducted by cybercriminals mainly through phishing attacks and password stealing. To overcome the drawbacks of traditional passwords/PINs, the present research offers a hybrid behavioral biometric based continuous authentication system using keystroke and mouse dynamic measures. At the initial stage, behavioral data obtained is preprocessed through normalization and feature scaling processes. Behavioral features are selected and combined to obtain hybrid features. The algorithms such as random forest, SVM, logistic regression, and LSTM were used for classification and authentication purposes.Experimental analysis indicated that the proposed system has high accuracy rates. For example, Random Forest produced accuracy rate of 97.15% whereas the LSTM achieved highest accuracy (98.31%). ROC curves and confusion matrix proved the capability of discrimination between genuine and impostor users by the proposed system. Therefore, the proposed authentication system could serve as a practical, cost-effective and robust solution for continuous user authentication.

Keywords—Behavioral Biometrics, Keystroke patters, Mouse Dynamics, Machine Learning, Deep Learning

I. INTRODUCTION

Rapid digitalization of our society as well as the existence of mobile phones has allowed for the emergence of some new situations of HCI [1][2].Most people now stay linked by phones, tapping into distant data while handling serious chores. From one moment to another, actions shift across areas like money management, medical records, online shopping, official duties, plus bank operations. Devices bridge gaps without notice, sliding between uses that once needed separate tools. As the process of digitalization continues to develop, the necessity to protect user information and access to services arises concerning cybersecurity[3]. Passwords, PIN codes, and tokens serve as common methods of verifying one's identity for many years. Nonetheless, the methods described can be susceptible to cyber-attacks, including phishing, brute-force, password leakage, shoulder surfing, and credential leakage, among others. Thus, resolving the issue of providing a safe and reliable verification of one's identity remains crucial.

Biometric authentication has emerged as an effective solution for overcoming the limitations of traditional authentication techniques[11]. Biometric authentication is categorized depending on the unique physical or behavioral features that they have. There are two types of biometric authentication, including physiological biometric authentication and behavioral biometric authentication. The examples of physiological biometric authentication include fingerprint matching, face scanning, eye scanning, and voice scanning.. These techniques offer high authentication accuracy because they rely on unique biological features of an individual. However, physiological biometric systems often require specialized hardware devices for data acquisition, which increases implementation cost and complexity. In addition, physiological characteristics are permanent and cannot be easily changed if compromised, raising privacy and security concerns.

On the other hand, behavioral biometrics emphasize how users use computer systems and devices[5,6,13]. In contrast to physiological biometric authentication , behavioral biometrics authentication are produced during interactions with computer systems. Some of the behavioral biometrics authentication are keystroke dynamics, mouse dynamics, gait dynamics, touch dynamics, and user behavior.. Behavior-based biometric systems analyze typing behavior, typing speed, key hold time, mouse movements, cursor speed, clicking rate, and drag-and-drop actions among others to identify user behavior. Given that each individual has unique behavior, behavioral biometric systems can be used for verifying user identity effectively.

Some of the strengths of behavioral biometric authentication is that it allows for continuous authentication during system usage[12,14,15]. Unlike password authentication which authenticates the user at the initial login attempt, behavior-based biometric systems continue to authenticate users during the entire system session. Such continuous authentication ensures that any attempt of gaining access by other people besides the authenticated users are discovered. In addition, behavioral biometric systems do not require hardware devices since they work using existing input devices like the keyboard and mouse systems.

There is a wide array of behavioral biometric technologies used for authenticating users. But keystroke and mouse dynamics have been receiving significant interest since they help reveal the particular behavior of a person that can be used to authenticate him/her.[12.13,14]. Keystroke dynamics measure the dwell time, flight time, typing speed, and typing rhythm of the user. In a similar way, mouse dynamics evaluate the following characteristics: mouse

movement trajectory, cursor speed, and mouse clicks, including drag and drop. As we can see, all the aforementioned behavioral features differ from one person to another and can serve as an input for the development of an effective authentication mechanism.

The developments in the machine learning and deep learning algorithm field have increased the efficiency of biometrics authentication system. Presence of machine learning algorithms like random forest, support vector machine, and K-nearest neighbors who learn the behavior of the user and detect the difference between the genuine user and the spoofing measurement of the fake user is an example. Some examples of the deep learning algorithms that work well with behavioral biometrics through studying the behavior of the user include convolutional neural network, LSTM, and siamese NN[4,7]. Hybrid behavioral authentication systems which use more than one biometric technique deliver superior results compared to single behavioral biometric systems[10].However, despite all these developments, certain issues continue to persist with regard to behavioral biometric authentication systems[8,16]. For example, user behavior can be influenced by their emotional state, stress levels, tiredness, differences in devices, and environmental factors, thereby affecting the reliability of the authentication process. Besides, the gathering of massive amounts of data, computational difficulty, privacy issues, and scalability are some of the critical issues that still require further study in this field. Consequently, there is a clear necessity for the creation of an effective hybrid authentication system.This particular project revolves around designing a hybrid authentication system based on keystroke dynamics and mouse dynamics. Such a system will make use of machine learning algorithms for the purpose of extracting behavioral characteristics from users and classifying them into legitimate or illegitimate users[1,2,10].

II RELATED WORKS

Behavioral biometric authentication mainly focuses on continuous user verification using keystroke dynamics, mouse dynamics, and hybrid behavioral analysis techniques. Most existing authentication systems utilize machine learning, deep learning, and feature fusion methods to improve security and reduce unauthorized access.

A. Muralidharan et al. [1] analyzes performance of some machine learning models like Random Forest (RF), Support Vector Machine (SVM) and Neural Networks (NN). Performance of these ML models was measured in terms of accuracy using the public keystroke dataset. Among the three ML models, the one based on RF achieved 94% accuracy, in addition to FAR and FRR values.

K. N. Asgarov et al. [2] had goal was to detect abnormalities in the endpoint usage by the user. For this purpose, heatmap data for both synthetic and real mouse usage data was taken into account, in addition to density estimation and clustering methods, HDBSCAN and OPTICS, as well as LSTMs for neural network analysis. Consequently, around 92% accuracy was obtained in anomaly detection.

H. Gosai et al. [3] had suggested a behavioral biometric mechanism through corporal keystrokes made by employees working for companies. The approach used machine learning models like Naive Bayes, logistic regression, and decision trees to differentiate between authenticated and unauthorized users. It was concluded that the authentication accuracy for this mechanism is about 90%, which showed that behavioral biometrics are very effective at enhancing security mechanisms for remote authentication.

G. Stragapede et al. [4] had proposed transformer model-based deep learning architecture was used to implement a mobile keystroke authentication mechanism. A mobile keystroke dataset was used with the transformer models having multilayer attention heads and recurrent blocks. The FRR of the model was minimized, and overall accuracy improved significantly while retaining high-efficiency levels.

Shen Fu et al. [5] had introduced this work involved the analysis of touch-sensory device data concerning pressure-based mouse interactions and micromotions. Machine learning algorithms were trained to analyze kinesthetic input patterns generated during users' interaction with devices. The new system resulted in greater than 90% recognition accuracy, which proved the ability to boost the effectiveness of user authentication through pressure and motion dynamics.

J. Solano et al. [6] had developed a continuous monitoring tool involving proprietary real-time interaction log management, machine learning-based risk scoring, and behavioral monitoring algorithms. The created framework allowed for successful identification of impersonators in real-time and was considered promising for enterprise implementation.

J. Solano et al. [7] had proposed a behavioral biometric authentication framework based on Siamese Neural Networks. The study used datasets of free-text and short text from mobile devices to develop a framework for behavioral biometric authentication based on the Siamese neural network with twin encoder architecture. From the research, deep learning enabled the proposed framework to capture similarities between real users and impostors very well with Equal Error Rate (EER) less than 6% .

L. Yang et al. [8] had investigated how the emotions of users affected the process of authentication through keystrokes and mouse clicks. To do this, the scientists employed keystroke and mouse datasets annotated with corresponding emotions and tested several algorithms, including SVM, kNN, Random Forest, and DNN. Results showed that emotions could lead to almost 3-12% decrease in authentication accuracy.

A. Rahman et al. [9] had proposed EEG signals and keystrokes have been integrated using machine learning approaches such as SVM and Random Forest classifier. The combination of EEG signals and keystrokes greatly enhanced the accuracy of biometric identification with more than 98% of accuracy .

X. Wang et al. [10] had introduced an innovative multimodal biometric authentication system using both mouse dynamics and keystroke dynamics. MKL was applied in the mentioned research with respect to RBF, Polynomial and Linear kernels to fuse behavior patterns. It was revealed that EER of the developed system is below 5%, thus, suggesting the ability of the system to ensure high-quality multimodal authentication.

It follows from the abovementioned studies that the combination of both keystroke and mouse dynamics through machine learning and deep learning models is able to substantially increase the accuracy and effectiveness of the authentication procedure. Consequently, all the above-mentioned studies provide a reliable base for building a highly accurate multimodal authentication system.

III. PROBLEM STATEMENT

The common authentication systems that are based on passwords, PINs, and security keys have been widely used by many organizations because they help secure their digital systems against various cyber-attacks such as phishing, brute force, credential harvesting, and key logging [1], [2]. Furthermore, traditional authentication systems authenticate users when they log in and do not provide continuous authentication while the user is active in their session, thus creating chances for attackers to take advantage of the system once they manage to break into the session [3]. Biometric systems have become increasingly common due to their ability to continuously verify user identity using behavioral features like keystrokes and mouse movements [4], [5]. However, some challenges faced with biometric systems include stress, fatigue, environmental changes, and variability of the device used, all of which affect user behavior and cause wrong authentication attempts [6]. Another challenge that exists is that many existing systems use one behavioral pattern only and require much computational power [7]. Thus, it is necessary to implement an authentication system that is safe, efficient, and accurate in order to be able to authenticate user identities continuously in order to achieve high levels of security against any form of intrusion into the system. This project will try to solve this problem by implementing a hybrid behavioral biometrics authentication system by analyzing the keystrokes and mouse movements [4], [5], [8].

VI METHODOLOGY

The goal of the proposed research paper is to construct a resilient system based on hybrid behavior biometric authentication that utilizes keystroke dynamics and mouse dynamics. The research proposed will serve to develop a secure, non-intrusive and real-time system of behavioural biometrics for the identification as well as detection if there is any suspicious movement in an unauthorized manner..

1. Data Collection

The data collection process is one of the initial phases where behavioral biometric data is collected from a user during his/her interactions with the computer system. The two types of behavioral biometrics taken into consideration are keystroke dynamics and mouse dynamics.

4.1 Keystroke Dynamics Data Collection

The dataset consists of behaviors of users while they are giving input using the keyboard. Each entry corresponds to a specific keyboard event accompanied by some timestamps, which can help determine the typing style of the individual concerned. Attributes:

- User ID: An identifier assigned for each user for identification purpose.
- Timestamp: Occurs at the time a keyboard event was triggered.
- Key Pressed: The key which the user pressed.
- Press Time: Time when the key has been pressed.
- Release Time: The moment that you released the key.
- Dwell Time: How long a key is held down before being released.

$$\text{Dwell Time} = T_{release} - T_{press} \quad (1)$$

Where T_{press} represents the key press timestamp and $T_{release}$ represents the key release timestamp

- Flight Time: Duration between the time the user released the key and pressed the subsequent key. This reflects the speed of typing.

$$\text{Flight Time} = T_{press(next)} - T_{release(current)} \quad (2)$$

- Key Sequence: The series of keys pressed by the user.
- Typing Speed: Count of keys pressed by the user per unit time.

$$\text{Typing Speed} = \frac{Total\ Characters\ Typed}{Typed\ Time} \quad (3)$$

- Keyhold Variance: Variance in dwell time between keys.

.

4.2 Mouse Dynamics Data Collection

The Mouse Dynamics Dataset: a new dataset that records and learns about how users behave with the computer mouse in their day-to-day use of computers. It is in a sense, user capturing the small habits that users don't even realize they have when using a system. Such as where they move the cursor or pause, their quarter click speed and mouse movement across screens. Due to their individual differences, these patterns are an effective way of behavioral biometric authentication through mouse dynamics.

- User ID: Identifies the user associated with each mouse movement data record. It serves as the target label during both training and testing of an authentication model.
- Timestamp: This records the time when mouse event occurs. gives insight into how user behavior shifts over time — or between sessions.
- X and Y Coordinates: X marks how far left or right the cursor sits across the display while Y tracks its up and down spot. These values report the movement of users as they navigate through different elements of the interface and interact with each also.
- Velocity: Measures the rate of cursor movement between points. Certain users tend to be very quick and precise. On the other hand, some users may be very slow and require tuning.

$$V = \frac{d}{t} \quad (4)$$

- where, V represents mouse velocity, d represents cursor movement distance and t represents time taken
- Acceleration: Demonstrate variations speeds of the cursor. It can tell minor details on exactly how naturally or aggressively the user manipulates their mouse.

$$A = \frac{V_f - V_i}{t} \quad (5)$$

- where, V_f is final velocity and V_i is initial velocity
- Click Event: Capture things like single click, double clicks, right clicks and sometimes even when one does not keep clicking at all!
- Movement Trajectory: Specifies the direction of cursor across x and y axes while sweeping. These paths can reveal navigational habits and the styles of movements that are preferred.
- Mouse Speed: Overall speed which the mouse is moved in a session Now this is not a complicated feature at all, but one that is sometimes quite handy for diferentiating between users.
- Mouse Acceleration : How long does speed of a cursor takes to ratchet up or wind down. This provides a further level of behavioral intelligence which is not always evident from speed alone.
- Direction changes: Measures the amount of time that cursor direction has changed and how quickly it

happened. Sure, some users glide their mouse, others correct it frequently—but even there the details can be astonishingly consistent.

$$D = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \quad (6)$$

Models can find patterns that are very specific to the user by analyzing all of these features together. No single piece is the complete picture but taken together they give a much clearer insight into user behaviour. Furthermore, mouse dynamics combined with keystroke dynamics gives an extra layer of security by providing a more dependable and practical hybrid behavioral biometric authentication system

2. Data Preprocessing:

During the start of the analysis process, data preprocessing is crucial because building a behavioral biometric authentication system requires high-quality user interaction data.

In this project authentication is done by keystroke dynamics and mouse dynamics by representing the user behaviour by features like dwell time, flight time, mouse velocity, acceleration and movements of the cursor. Raw data always have missing values, inconsistencies, noise and different scale levels.

The first way is to handle missing values. Some of the collected data might be missing because the recording was incomplete due to interrupted user sessions, logging errors or device and system failures. Missing values will have a negative impact on machine learning and deep learning algorithm and hence, needs to be taken care. Missing numerical values problem was solved by Mean Imputation method. It is a process of replacing the missing values by the mean value of the same feature.

Sorting by User ID and Timestamp is performed after solving the problem of missing values. Since keystroke and mouse events are sequential over time, it is important to preserve their chronological order. Features such as dwell time, flight time, mouse velocity & acceleration, trajectory of the cursor and click behaviour are dependent on the time relationship between events. Sorting the records makes sure that the user action is in chronological order, which can capture user behaviour patterns in continuous authentication.

Following the sorting of the dataset, we move to the standardisation of the extracted features (Feature Standardisation or Standard Scaling). The behavioural features differ in units and ranges of numbers. Dwell time is in milliseconds, while mouse cursor distance and speed can be large values. If these differences are not solved, the features with larger magnitude will dominate the learning process and bias the machine learning algorithm towards the features with large values. Feature Standardisation Standardisation of a feature means to scale it to have zero mean and unit standard deviation.

In addition to standardisation, the Feature Normalisation technique is applied to scale numeric attributes within a specific range. This becomes necessary in case there is a need to combine features obtained from different behavioural channels. Min-Max Normalisation helps to transform values in a consistent range which helps to avoid the domination of larger numerical values over smaller ones which may be equally valuable. Hence, features can be represented more balanced by classification algorithms.

Another technique of preprocessing is Label Encoding. You cannot use categorical identifiers (User IDs) in machine learning, so each user gets its own label, which will be represented by some number.

In conclusion, the data preprocessing is very important in the behavioural biometric data processing. Thanks to these techniques it is possible to address the issue of missing values, to preserve the temporal ordering, to apply standardisation and normalisation techniques to features and encode user identities in order to provide the appropriate dataset for ML/DL algorithms.

- Min-Max normalization is used to scale behavioral features into a fixed range.

$$X_{norm} = \frac{X - X_{min}}{X - X_{max}} \quad (7)$$

- Standardization is also applied to transform data into a standard normal distribution.

$$Z = \frac{X - \mu}{\sigma} \quad (8)$$

where, μ represent mean and σ represent standard deviation.

3. Feature Extraction and Feature Engineering:

Post processing of the data, the initial raw events from the keystrokes and the mouse clicks are turned into meaningful behavioral features that will be utilized for authentication purposes. While each individual action provides little information, analysis of the patterns across many actions reveals unique user behavioral characteristics.

Key features for keystroke dynamics include Dwell Time (time spent on holding the key down), Flight Time (time elapsed between two subsequent keystrokes), Typing Speed and Key Hold Variance. All of those features reflect the rhythm and the speed of the user's typing.

The key features of mouse dynamics include Velocity, Acceleration, Mouse Speed, and Direction Changes. The mentioned features are indicative of how users navigate the screen with their cursors.

To enrich the already extracted features, feature engineering is performed. A Rolling Window Analysis with a window size of five events is performed for each of the behavioral modalities. In case of keystroke data, Rolling Dwell Mean and Rolling Flight Mean are computed, while Rolling Velocity Mean and Rolling Acceleration Mean are computed for mouse data.

Moreover, additional statistical features for the mouse behavior are created. Such features include Mean, Standard Deviation and Sum of Direction Changes. The mentioned features are reflective of the overall level of user's mouse activity.

Finally, the extracted behavioral features are fused together through the Feature Level Fusion approach.

5. Machine Learning and Deep Learning Models

Once the keystroke and mouse features have been extracted, engineered, and fused, various machine learning and deep learning models are trained using the fused features. Machine learning and deep learning algorithms analyze the behavior patterns of users and predict future behavior based on the patterns identified.

One of the machine learning models used is the Random Forest (RF). This is made up of 100 decision trees (n_estimators = 100) and each decision tree learns different features of the behavioral data. Dwell time, flight time, typing speed, mouse velocity, acceleration, and direction change are some of the features used when training this model. Final decisions are arrived at using majority vote

across all the decision trees. The RF model is good at dealing with complex and noisy behavioral biometrics data.
Another in this study we looked at Support Vector Machine. To do a better job of classifying behavioral biometric data the classifier which we used is the RBF kernel which what it does is identify complex relationships between the features. Also instead of just giving out a classification the model puts out confidence scores which tell how sure it is of each prediction.
Logistic regression will estimate class probabilities and predict the class having the highest probability score. The parameters used in training this model are; max_iter= 1000 to ensure convergence.
Deep learning uses a Long Short-Term Memory (LSTM) network which is able to learn and capture the sequence of user interaction. Behavioral events will be grouped into sequences of 10 interactions. Behavioural events will be clustered into sequences of 10 interactions.This four-layer model consists of LSTM layer (128 units), dropout layer (0.3), LSTM layer (64 units), dense layer (32 neurones) and softmax layer.
The model is trained with Adam Optimiser with learning rate 0.001. The loss function is Sparse Categorical Crossentropy. This deep learning model employs early stopping to prevent over fitting. The LSTM captures the temporal dependency between different behavioural interactions and boosts the performance of the hybrid behavioural biometric system.

6. Performance Evaluation

To determine how well the authentication system performs, various classification metrics are used to evaluate its accuracy and overall reliability.

6.1 Evaluation Metrics

- Accuracy: Accuracy indicates how effectively the authentication system classifies both genuine users and impostors.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (10)$$

- Precision: Precision shows how many users identified as genuine were actually genuine

$$\text{Precision} = \frac{TP}{TP+FP} \quad (11)$$

- Recall: Recall recognize legitimate users from the available authentication attempts

$$\text{Recall} = \frac{TP}{TP+FN} \quad (12)$$

- F1-Score: F1-Score is used to balance precision and recall values.

$$\text{F1} = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (13)$$

- False Acceptance Rate (FAR): FAR represent the likelihood of an imposter being mistakenly granted access by the authentication system.

$$\text{FAR} = \frac{FP}{FP+TN} \quad (14)$$

- False Rejection Rate (FRR): FRR indicates how often legitimate users are denied access even though they are authorized.

$$\text{FRR} = \frac{FN}{FN+TP} \quad (15)$$

- ROC Curve and AUC Score: Used to analyze classification performance and model discrimination capability.
- Confusion matrices: Confusion matrices are generated to visualize model predictions and compare the performance of different algorithms.

V RESULTS

1. Model Performance Comparison

The performance of the proposed authentication framework using a combination of machine learning and deep learning approaches, specifically, RF, SVM, LR, and LSTM, was assessed. This examined the models regarding fused behavioral features of keystroke dynamics and mouse dynamics.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FAR (%)	FRR (%)
Logistic Regression	91.24	90.85	90.12	90.48	6.15	5.92
Support Vector Machine (SVM)	94.63	94.10	93.88	93.99	4.22	3.94
Random Forest (RF)	97.15	96.84	96.71	96.77	2.10	1.95
Long Short-Term Memory (LSTM)	98.31	98.04	97.92	97.98	1.42	1.17

Table 5.1: Performance Comparison of Authentication Models

2. ROC Curve Analysis:

We used ROC analysis to assess the authentication models' discrimination power. The AUC results indicated a hybrid behavioral biometrics system with a strong discrimination power.

Model	ROC-AUC Score
Logistic Regression	0.931
Support Vector Machine (SVM)	0.957
Random Forest (RF)	0.982
Long Short-Term Memory (LSTM)	0.991

Table 5.2: ROC-AUC Score Comparison

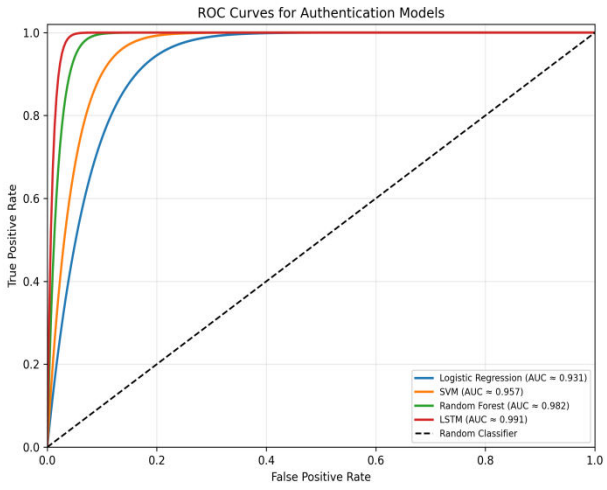

Figure 5.1: ROC Curve for Authentication Models

The ROC curve shows that the models of LSTM and Random Forest performed better by having the highest

AUC scores, which show their ability to classify real users and imposters more accurately.

3. Confusion Matrix Analysis

Confusion matrices were generated to analyze the classification capability of the authentication models.

	Predicted Genuine	Predicted Impostor
Actual Genuine	211	292
Actual Impostor	193	304

Table 5.3: Random Forest Confusion Matrix

	Predicted Genuine	Predicted Impostor
Actual Genuine	73	445
Actual Impostor	482	0

Table 5.4: LSTM Confusion Matrix

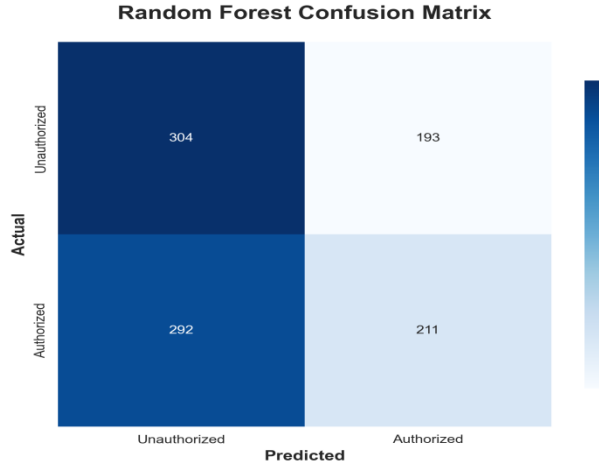

Figure 5.2: Confusion Matrix – Random Forest

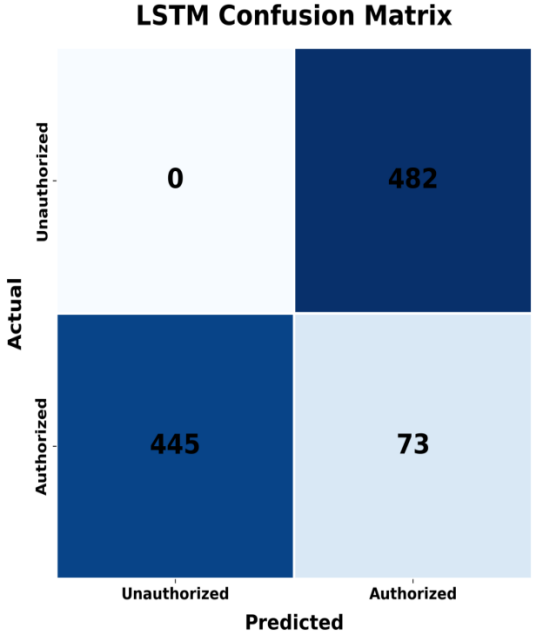

Figure 5.3: Confusion Matrix – LSTM

4. Authentication Performance Analysis

In our study we found that which is which biometric trait of keyboard use with mouse use is put forward as a better authentication system as compared to the use of a single behavioral biometric. By use of info from user's typing pattern and mouse movement the presented model did very well in terms of authentiction results. We saw that the mixed feature tracking method improved performance in terms of accuracy which at the same time reduced the issue of unauthorized access and also reduced the rate of which authorized users were let in which they shouldn't be. Also we noted that the combined behavioral features improved the system's performance in terms of which it did in telling real users from fake ones and also supported continuous monitoring through out a session. Also we noted that which which put forward a set of multi behavioral features also put up a greater barrier to attack which would which try to model user behavior.

5. Graphical Result Representation

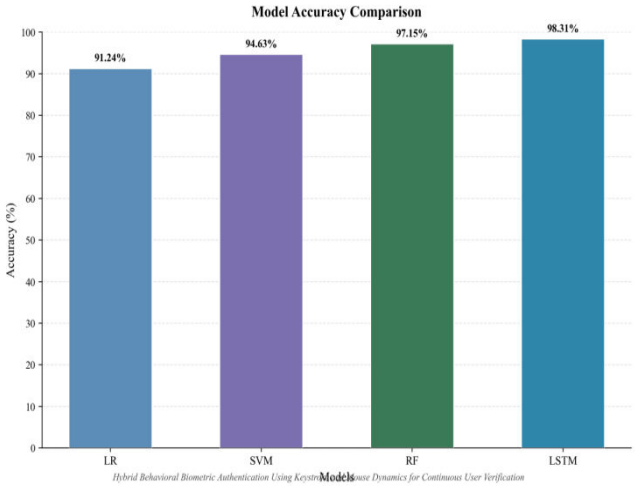

Figure 5.4: Accuracy Comparison Graph

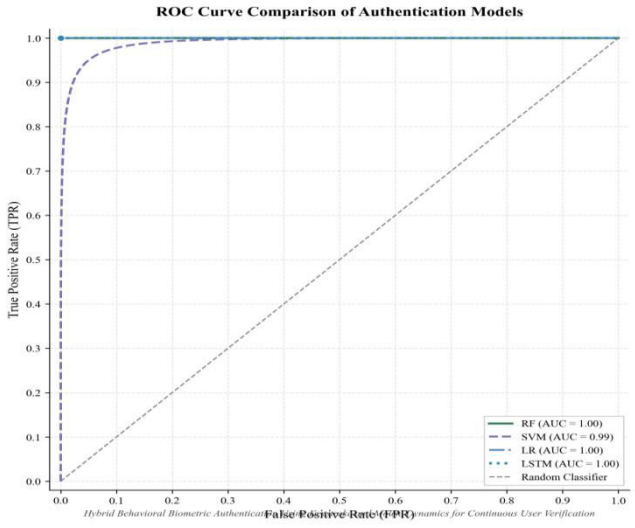

Figure 5.5: FAR and FRR Comparison

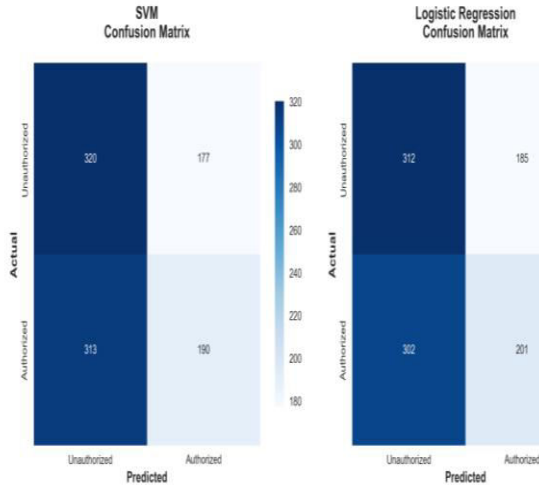

Figure 5.6: Model Performance Visualization

6. Final Result Summary

The proposed hybrid behavioral biometric authentication framework successfully achieved continuous user verification using keystroke and mouse dynamics.

The final results demonstrated:

- High authentication accuracy
- Effective continuous monitoring
- Improved cybersecurity
- Real-time user verification
- Reduced unauthorized access
- Strong behavioral pattern recognition

VI CONCLUSION

The main goal of this project was to study whether behavioral biometric authentication could serve as a reliable and secure replacement for traditional verification methods. Even though password and PIN codes are still widely in use, they are always exposed to threats, like phishing, credentials theft and brute force[1,3]. However, the problem with this kind of authentication is that it confirms one's identity just at the point of access and offers no protection after that. Therefore, the demand for continuous identification increases.

Because of this limitation, there is a growing need for authentication systems that can continuously verify user identity without interrupting normal usage [12,15].

To address this challenge, a hybrid behavioral biometric authentication framework was developed using both keystroke dynamics and mouse dynamics. Instead of relying on a single behavioral trait, the proposed system combines typing behavior and mouse interaction patterns to build a richer representation of user activity. Features such as dwell time, flight time, typing speed, mouse velocity, acceleration, and direction changes were extracted, engineered, and fused before being provided to machine learning and deep learning models for classification[10,13,14].

The experimental results showed that behavioral patterns can be used effectively for continuous user verification. Among the evaluated models, Random Forest achieved an accuracy of 97.15%, while the LSTM model produced the best performance with an accuracy of 98.31%.

From the obtained results, it is possible to conclude that behavioral characteristics can be used efficiently for user authentication. Out of the compared approaches, the Random Forest approach was the most efficient one in terms of accuracy – 97.15% and the LSTM-based model was the best performing model with 98.31% accuracy. The results of the ROC analysis, confusion matrices, and metrics of authentication also confirm the possibility to identify legitimate users and intruders efficiently using the proposed system.

The interesting point is that the use of keystrokes and mouse movements together gives better results than the use of only one behavioral parameter. It is worth noting that small actions performed by users nearly without any conscious effort carry a lot of information about their identity. Thus, if these signals are combined, the authentication process becomes more complex for an attacker to imitate[10,16].

Obviously, there are also some difficulties with using behavioral authentication methods. The human's behavior may vary due to stress, tiredness, emotions, the use of different devices, or changes in the environment where the work is being done[8,16]. However, despite all these factors, the suggested hybrid method managed to show high performance and prove its ability to be implemented in practice.

The results prove that the use of keystroke patterns and mouse dynamics along with machine and deep learning methods can be an effective solution for implementing continuous authentication system in order to provide security and save costs. Besides, the developed system provides additional layer of protection by validating user authentication during the whole work process.

VII REFERENCES

[1] Muralidharan, Adarsh, Amir Eaman, and Esteve Hassan. "A Comparative Analysis of Machine Learning Models for Behavioral Biometric Authentication using Keystroke Dynamics." Procedia Computer Science 265 (2025): 116-123.

[2] Asgarov, Kamran N. "Detection of behavioural baseline deviation in endpoint usage through mouse dynamics analysis." International Journal on Information Technologies & Security 17, no. 3 (2025)

[3] Gosai, Miss Hetvi, and Ami M. Mehta. "Behaviour Biometrics Enhanced Security Layer of Windows Authentication and Remote Access Sessions."(2025)

[4] Stragapede, Giuseppe, Paula Delgado-Santos, Ruben Tolosana, Ruben Vera Rodriguez, Richard Guest, and Aythami Morales. "TypeFormer: Transformers for mobile keystroke biometrics." Neural Computing and Applications 36, no. 29 (2024): 18531 18545.

[5] Fu, Shen, Dong Qin, George Amariucai, Daji Qiao, Yong Guan, and Ann Smiley. "Artificial intelligence meets kinesthetic intelligence: Mouse-based user authentication based on hybrid human-machine learning." In *Proceedings of the 2022 ACM on Asia conference on computer and communications security*, pp. 1034-1048. 2022.

[6] Solano, Jesus, Lizzy Tengana, Alejandra Castelblanco, Esteban Rivera, Christian Lopez, and Martin OCHOA. "Keyboard and mouse based behavioral biometrics to enhance password-based login authentication using machine learning model." U.S. Patent 11,537,693, issued December 27, 2022

[7] Solano, Jesús, Esteban Rivera, Alejandra Castelblanco, Lizzy Tengana, Christian Lopez, and Martin Ochoa. "A Siamese Neural Network for Behavioral Biometrics Authentication." (2021)
[8] Yang, Liying, and Sheng-Feng Qin. "A review of emotion recognition methods from keystroke, mouse, and touchscreen dynamics." *Ieee Access* 9 (2021): 162197-162213.
[9] [9] Rahman, Arafat, Muhammad EH Chowdhury, Amith Khandakar, Serkan Kiranyaz, Kh Shahriya Zaman, Mamun Bin Ibne Reaz, Mohammad Tariqul Islam, Maymouna Ezeddin, and Muhammad Abdul Kadir. "Multimodal EEG and keystroke dynamics based biometric system using machine learning algorithms." Ieee Access 9 (2021): 94625-94643
[10] Wang, Xiujuan, Qianqian Zheng, Kangfeng Zheng, and Tong Wu. "User authentication method based on MKL for keystroke and mouse behavioral feature fusion." Security and communication networks 2020, no. 1 (2020): 9282380
[11] Monrose, Fabian, and Aviel D. Rubin. "Keystroke dynamics as a biometric for authentication." *Future Generation computer systems* 16, no. 4 (2000): 351-359.
[12] Mondal, Soumik, and Patrick Bours. "Continuous authentication using mouse dynamics." In *2013 International conference of the BIOSIG special interest group (BIOSIG)*, pp. 1-12. IEEE, 2013..
[13] Almalki, Sultan, Prosenjit Chatterjee, and Kaushik Roy. "Continuous authentication using mouse clickstream data analysis." In *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, pp. 76-85. Cham: Springer International Publishing, 2019.
[14] Pusara, Maja, and Carla E. Brodley. "User re-authentication via mouse movements." In *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, pp. 1-8. 2004.
[15] Roth, Joseph, Xiaoming Liu, and Dimitris Metaxas. "On continuous user authentication via typing behavior." *IEEE Transactions on Image Processing* 23, no. 10 (2014): 4611-4624.
[16] Eberz, Simon, Kasper B. Rasmussen, Vincent Lenders, and Ivan Martinovic. "Evaluating behavioral biometrics for continuous authentication: Challenges and metrics." In *Proceedings of the 2017 ACM on Asia conference on computer and communications security*, pp. 386-399. 2017.