Smartphone-based Gait Authentication for Health Insurance Incentives: A Data-Driven Approach to Verify Walking Compliance

Sandip Dutta
Department of Computer and System Sciences, Visva-Bharati
Santiniketan, 731235
West Bengal, India

Soumen Roy
Department of Computer Science, Bagnan College
Bagnan, Howrah 711303
West Bengal, India

Purba Banerjee
Department of Computer and System Sciences, Visva-Bharati
Santiniketan, 731235
West Bengal, India

Utpal Roy
Department of Computer and System Sciences, Visva-Bharati
Santiniketan, 731235
West Bengal, India

ABSTRACT

Some of few health insurance companies now offer lower premiums to people who walk 10,000 steps every day. The main problem in this plan is figuring out who qualifies. We suggest using data from smartphone sensors while people walk. This data can track steps and confirm who's walking. This could help prevent misuse of the program. In response to the aforementioned conundrum, we have procured and meticulously analysed the gait patterns of 87 volunteers. Our investigation has determined that the Scale Manhattan an efficacious anomaly detector, suitable for individual verification in active mode, achieving an equal error rate from 10.20% to 13.76%. Our proposed detection system has undergone validation procedures employing datasets gathered across multiple sessions and repetitions. Based on a judiciously conducted realistic appraisal of the proposed model for each subject, we assert that this method of individual authentication holds merit for the aforementioned campaign, engendering tangible benefits for prospective beneficiaries. Beyond the immediate insurance incentives, this approach possesses the potential to motivate individuals not only to procure insurance coverage but also to foster their physical and psychological well-being. Our innovative methodology provides a substantive solution for health insurance companies contemplating the implementation of analogous promotional endeavours.

General Terms

Biometrics, User authentication, Health insurance

Keywords

Human gait analysis, Human computer interaction, Gesture, Action recognition, Anomaly detection, User authentication, Scaled manhattan

1. INTRODUCTION

Aditya Birla Health Insurance offers a reimbursement of up to 100% of the premium provided that the policyholder accumulates a sufficient number of 'Activ Dayz'. An 'Activ Day' is defined as achieving a daily target of 10,000 steps or engaging in any fitness activity stipulated by the insurer [1]. This policy introduces a critical challenge in verifying the eligibility of insurance holders who meet the specified requirements. To address this challenge, insurance holders can utilize a smartphone equipped with sensors and an application capable of tracking and quantifying physical activity. However, the potential for multiple users, such as family members, to share the device while maintaining the step count raises concerns about the authenticity of the recorded activity. Thus, ensuring continuous authentication of the user is imperative, highlighting the challenge of active user authentication via smartphones.

Active authentication involves the continuous measurement and analysis of biometric attributes and contextual data to verify the user automatically. It enables implicit recognition and ongoing re-authentication throughout the session with minimal user intervention [25]. This method, also referred to as continuous or transparent authentication, can be implemented both on-device and off-device. Key characteristics of active authentication include continuity and transparency. The process comprises two main phases: enrollment and identity verification, each involving steps such as data acquisition, feature extraction, data preprocessing, template formation, classification, decision-making, and re-authentication.

Traditional fixed-activity re-authentication methods often compromise usability. Studies have identified several desirable characteristics for effective authentication mechanisms: (a) implicit operation, (b) independence from user knowledge, (c) resistance to observation, and (d) fine-grained protection [16]. Additionally, goals for system design should include (a) implicit operation, (b) continuous engagement, (c) usability, and (d) cost-effectiveness [54]. Moreover, smartphone authentication should achieve (a) continuous operation, (b) unobtrusiveness, and (c) lightweight performance [43]. Designing a model that meets these criteria while ensuring robust security is crucial.

Modern smartphones are equipped with various sensors, including gyroscopes, accelerometers, and rotational sensors. Utilizing these sensory data streams presents an opportunity for continuous and implicit user validation. However, acquiring sensory data at high sampling rates significantly drains battery power, impacting device longevity [32]. For instance, measuring gyroscope and accelerometer data at 16 Hz incurs an energy overhead of 7.9% [70], and re-authentication can consume an additional 2.4% of battery life [41]. Therefore, prolonged sensory data acquisition results in substantial energy costs [75], with increased sampling rates exacerbating battery consumption and CPU usage [12]. To address these challenges, mobile applications must incorporate mechanisms to pause and resume sensor operation, optimizing battery usage while maintaining effective user authentication. Data augmentation methods, such as generating synthetic data from short-term real data, offer a potential solution [2].

Previous research has primarily focused on datasets collected during interactions like scrolling, typing, and swiping. However, there is a lack of open, standard datasets collected in realistic scenarios, such as when the phone is in the user's pocket. Most existing datasets are derived from specific, often homogeneous groups, limiting the generalizability of findings. For a robust authentication model, it is essential to develop datasets from diverse populations encompassing various age groups, genders, and other demographic factors. Moreover, acquiring a comprehensive dataset with advanced sensory features, including gyroscope, rotation, and acceleration, while walking, is necessary to design and evaluate effective authentication models.

The problem of user authentication in this context involves anomaly detection. Typical walking patterns, captured as sensory data, must be stored for reference, with new patterns compared against these stored templates during authentication attempts. If the current pattern matches the stored template, the user is recognized as genuine, allowing the continuation of step counting.

Developing a model with only user samples and using it to detect imposters through similarity measures or one-class classifiers is a feasible approach, given the impracticality of obtaining all potential imposter patterns. This approach, known as anomaly or novelty detection, is less explored in continuous domains with smartphone sensory data. Implementing anomaly detection techniques for advanced sensory features remains a research gap.

The selection of anomaly detectors is crucial, as performance varies significantly across datasets. For example, one-class SVM applied to touch-interaction datasets yielded a 4.68% false acceptance rate (FAR) and a 1.17% false rejection rate (FRR) [69], while the same detector on PIN typing datasets showed a higher equal error rate (EER) of 7.89% [37]. Other studies reported variable FAR and FRR rates for different input types [6, 78]. These variations underscore the need for further research on the effectiveness of anomaly detection methods in diverse scenarios.

The key contribution of this study is to design an implicit and active smartphone user authentication system using sensory data captured during walking and to compare various anomaly detectors. This study focuses on evaluating technologies by comparing the performance of different detectors.

2. LITERATURE REVIEW

Research in the realm of active user authentication utilizing smartphone sensors has explored a plethora of features encompassing image, touch sensors, location, accelerometer, gyroscope, WiFi, app usage, as well as texture and shape features, yielding diverse performance outcomes [3, 4, 15, 48, 76]. The rich multisensory data emanating from sensors integrated into smartphones furnishes a fertile ground for continuous authentication, with datasets such as *HMOG* and *Touchalytics* capturing nuanced patterns associated with holding, tapping, swiping, and scrolling activities [9, 21, 64]. Despite challenges related to intra-class variation and data quality, the covert data capture capabilities of keystroke dynamics (KD) during routine user interactions render it a promising attribute for active authentication. To surmount accuracy limitations, the research community has proposed multi-modal approaches integrating contextual factors and harnessing an array of pattern recognition methodologies, encompassing traditional statistics, deep learning, and binary classifiers [19, 26, 46, 74].

Recent efforts have delved into the realm of binary classifiers for mobile terminal identity authentication, with classification methods being applied across various studies [10, 29, 46, 66, 67, 72]. An emerging trend revolves around the utilization of anomaly detectors as one-class classifiers for implicit and active authentication of smartphone users, with studies underscoring the necessity for a robust comparison framework that encompasses diverse datasets and characteristics [3, 8, 14, 15, 17, 44, 47, 68, 77]. The intricacies inherent in these methodologies, coupled with the variances observed in datasets, underscore the evolving landscape of active user authentication on smartphones, thereby necessitating continued research efforts aimed at refining and optimizing these approaches.

A study [34] developed CMU dataset and found Scaled Manhattan is the suitable detectors among fourteen detector. They used huge training set to develop user's template. It takes large data acquisition time. Therefore, a study [58] used common nine anomaly detectors on CMU dataset and found Scaled Manhattan is suitable detector which is achieved 9.6% of EER similar to previous study. However, they used synthetic data and same detector to reduce the training time and observed the same results. In their observation Outlier-count achieved the lowest EER in case of considering synthetic data and reduced the EER to 8.3%. Another study [49] applied the same dataset and achieved 5.1% of EER using feature-engineering approach. They compared their approach with other fourteen detectors in same setting. Another study [36] proposed a deep learning based detector and found impressive results using the same dataset and compare their approach with other seventeen detectors. Similar study [45] achieved impressive results with the CMU dataset and compared with sixteen detectors. Another recent study [22] used the same dataset but found 4.9% of EER using neural network method. The above studies used only one dataset for their model evaluation and found the EER 4% to 10% while using CMU dataset.

Another dataset GREYC2009 has been used by a study [23] and found 15.28% of EER bit larger than previous. They used support vector-based detector. A study [65] used two datasets for their model evaluation and found around 9% of EER. Another study [56] used two datasets and found impressive results. Whereas, a study [53] used three datasets and found more accurate results using similarity-based detector.

A summary of recent approaches is shown in Table 1 conducted by researchers in the development of authentication models.

Table 1. : Latest Anomaly Detectors and Their Performances

Study	Year	Approach	Features	EER (%)
[30]	2018	OCSVM	T	Accuracy 90
[28]	2018	One class Naïve bayes	T	7, 4
[33]	2018	Scaled Manhattan distances	T	7.7
[58]	2018	Euclidean, Manhattan, and more	T	8.3
[55]	2018	Cosine similarity	T	FAR 0
[39]	2018	Euclidean, Manhattan distance	T, G, A, R, TP, S	7.89
[40]	2018	OCSVM	T, G, A, R	0 to 30
[30]	2018	OCSVM	T	Accuracy 99
[37]	2018	Distance-based, OCSVM	T, G, A, R, TP, S	7.89
[42]	2018	DTW	G, A, R	Accuracy 91.4
[57]	2019	Autoencoder	T	6.51
[50]	2019	GA-KNN	T	5.3, 2.3
[52]	2019	GA-KNN	T	5
[51]	2019	KNN	T	5.3
[13]	2019	Similarity	T	4
[63]	2019	OCSVM	T	FAR 10.32, FRR 29.99
[60]	2019	OCSVM	T	FAR 2.8 and FRR 8.1
[59]	2019	OCSVM	T	5.22, FAR 0.2 and FRR 10.24
[27]	2019	Scaled Manhattan, and more	T	AUC 0.937, 0.923, 0.920, and 0.919
[24]	2019	Siamese network	T	09:01
[20]	2019	Statistical measure	T	FRR 2.54 FAR 0
[62]	2019	Statistical measure	T	10.5
[38]	2019	Manhattan distance, Scaling	T, G, A, R, TP	6.48 to 8.18
[75]	2019	Support Vector Regression	T, P, G, A	0.1266
[22]	2020	Feed forward multilayer neural network	T	4.9
[7]	2020	Manhattan distance	T	FAR 1.7 FRR 4.3
[61]	2020	Similarity measure	T	7.176
[18]	2020	Gaussian Mixture Models	T	11.7
[73]	2020	DTW and Wigner distribution	T	2.8 and 3.2
[35]	2020	Manhattan	T, G, A, R, TP, S	13.44
[31]	2020	Gaussian mixture	T, G, A, TP	9.23, 2.34, 3.63

T− >Timing, DTW− >Dynamic Time Wrapping
G− >Gyroscope, A− >Accelerometer, R− >Rotation
TP− >Touchpoint, S− >Statistical features, P− >Pressure, FTA− >Finger Tips Area

3. PROPOSED AUTHENTICATION FRAMEWORK

User authentication systems generally comprise two core phases: registration and authentication. However, our proposed model introduces a novel framework segmented into three distinct phases, as depicted in Figure 1. These phases include: the registration or training phase, the testing phase, and the reauthentication phase. This tripartite structure facilitates the implementation of active user authentication.

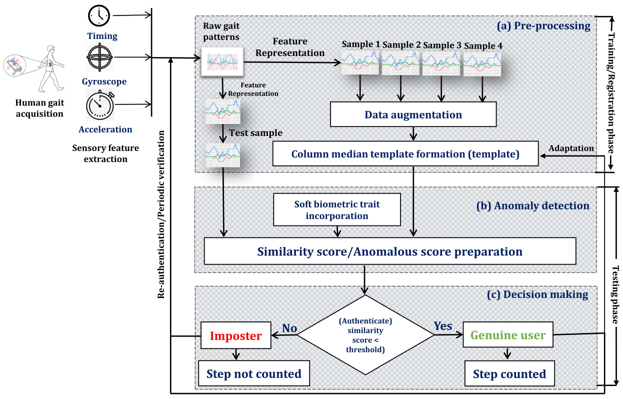


Fig. 1: Representation of the proposed framework for active user authentication.

3.1 Registration / Training Phase

In the registration or training phase, human gait patterns are captured through advanced smartphone sensors and subsequently preprocessed to construct a user-specific gait template and to train an anomaly detection model. Sensory measurements, which serve as raw features for gait pattern representation, are sampled at a rate of 2 Hz to optimize energy efficiency. The processed gait data are then condensed into a compact format for use in authentication and retraining. Multiple repetitions over time are aggregated to ensure the model's long-term reliability.
The specific steps involved in this phase are as follows:

(1) **Data Acquisition:** Human gait patterns are acquired from smartphone sensors, including accelerometers, gyroscopes, and timing devices, through a user-friendly interface during walking.

(2) **Feature Representation:** Continuous sensory data are partitioned into small intervals for alignment and ordering. Gait patterns are segmented into fixed-size samples using a sliding window technique with a time-domain-specific window length of 5 seconds. This yields discrete sensor values represented as averages, organized into a tabular structure where rows correspond to individual samples and columns represent data points within each sample. This structured approach facilitates consistent similarity assessment and aggregates multiple feature tables into a comprehensive input table for model development or template creation.

(3) **Data Augmentation:** Uniform random noise is introduced to each base sample to create synthetic variations, thereby enhancing its suitability for template formation. Noise values, uniformly distributed within the range of -0.5 to 0.5, are added to each element of the base gait sample. This controlled perturbation, executed using the 'runif' function in the R statistical environment, enriches the dataset and potentially improves model performance and robustness.

(4) **Template Formation and Adaptation:** Constructing an AI/ML model for gait-based authentication that integrates both user and impostor data presents significant challenges due to the impracticality of capturing all potential impostor patterns. Instead, the system constructs a template exclusively from the user's gait patterns and employs a similarity metric to identify impostors. The column median method is used to generate a dynamic gait template, where the median values from augmented gait samples form a representative instance of the user's gait pattern, as shown in Figure 3. This approach enhances model adaptability by addressing temporal variations and data uncertainties more effectively than traditional methods such as the column mean or Gaussian mixture model. The gait template evolves with each successful authentication, integrating new data to refine future templates and improving accuracy over time.

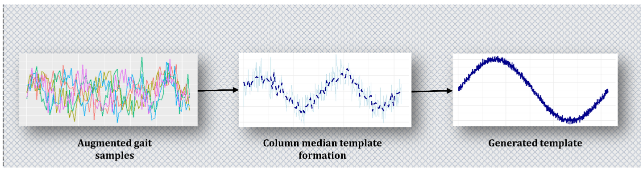


Fig. 2: Human gait template formation using the column median approach.

3.2 Authentication / Testing Phase

During the authentication or testing phase, a gait sample, termed as a test or claim sample, is captured within a brief time frame using the same methodology and sampling rate as in the registration phase. Anomalous scores are computed using anomaly detection algorithms to assess the similarity between the stored template and the claim sample. A threshold value of 0.5 is employed to classify the sample as either Access/Genuine or Denied/Imposter. Personalized thresholds can be set for each user to adjust the system's level of strictness. This threshold influences the False Acceptance Rate (FAR) and False Rejection Rate (FRR), which can be tailored according to application requirements and gait pattern consistency. The specific steps involved in this phase are:

(1) **Similarity Score Preparation:** Various anomaly detection algorithms are systematically evaluated to determine the most suitable method for the domain. This involves a comprehensive exploration of methodologies considering data distribution, feature space complexity, and computational efficiency. The chosen anomaly detector generates a similarity score by comparing the test gait sample with the generated template as shown in fig 3.

(2) **Soft Biometric Traits Incorporation:** Soft biometric attributes such as gender, age group, and educational qualification are incorporated to enhance the efficacy of the selected anomaly detection algorithm, as indicated by previous studies [71, 5, 11].

(3) **Decision Making:** Based on the anomaly score generated by the selected anomaly detector, a decision is made. If the score

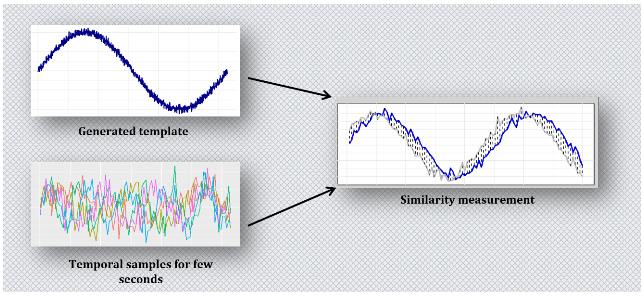


Fig. 3: Similarity score generation

is below the default threshold of 0.5, the claim sample is authenticated as genuine; if it exceeds this threshold, the sample is identified as an impostor. Authentic users' step counts are recorded, whereas impostors' attempts are not recorded.

3.3 Re-authentication / Periodic Verification

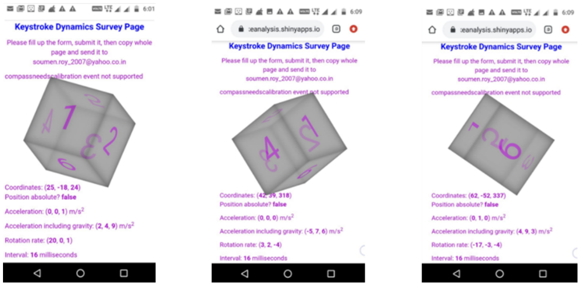
To implement active user authentication, the periodic verification phase is introduced. This process ensures user legitimacy by periodically restarting the authentication phase at intervals determined by the required security level. The duration of the authentication phase depends on the specific security requirements of the device or application. Effective management of this phase is crucial for balancing system usability with security.

4. DATASET PREPARATION

The gait dataset has been meticulously curated to ensure high fidelity, applicability, and relevance for studying gait dynamics in the context of active user authentication. This was achieved through the use of advanced, validated data acquisition systems and a comprehensive array of attributes.

4.1 Data Acquisition Application

The data acquisition application, designed for touchscreen smartphones, is accessible at `https://keystrokeanalysis.shinyapps.io/project/` under the 'Data Acquisition' tab. Developed using HTML and JavaScript, this application leverages the Sensors API for seamless integration and efficient capture of a diverse range of sensor-based gait patterns. The interface of the application is shown in Figure 4.



6:01

Keystroke Dynamics Survey Page

Please fill up the form, submit it, then copy whole page and send it to soumen.roy_2007@yahoo.co.in

compassneedscalibration event not supported

Coordinates: (25, -18, 24)
Position absolute? false

Acceleration: (0, 0, 1) m/s^2

Acceleration including gravity: (2, 4, 9) m/s^2

Rotation rate: (20, 0, 1)

Interval: 16 milliseconds

6:09

:eanalysis.shinyapps.io

Keystroke Dynamics Survey Page

Please fill up the form, submit it, then copy whole page and send it to soumen.roy_2007@yahoo.co.in

compassneedscalibration event not supported

Coordinates: (42, 39, 318)
Position absolute? false

Acceleration: (0, 0, 0) m/s^2

Acceleration including gravity: (-5, 7, 6) m/s^2

Rotation rate: (3, 2, -4)

Interval: 16 milliseconds

6:09

:eanalysis.shinyapps.io

Keystroke Dynamics Survey Page

Please fill up the form, submit it, then copy whole page and send it to soumen.roy_2007@yahoo.co.in

compassneedscalibration event not supported

Coordinates: (62, -52, 337)
Position absolute? false

Acceleration: (0, 1, 0) m/s^2

Acceleration including gravity: (4, 9, 3) m/s^2

Rotation rate: (-17, -3, -4)

Interval: 16 milliseconds

Fig. 4: Data acquisition application for collecting human gait patterns.

4.2 Data Acquisition Device

Human gait patterns were captured using the web-based application on an Android 9.0 (Pie) smartphone, specifically the Samsung A50 model. This setup enhances ecological validity by accurately reflecting real-world usage conditions.

4.3 Features considered :

The sensory features considered for capturing human gait patterns accurately and efficiently include $\langle g_x, g_y, g_z \rangle$ representing the gyroscope readings and $\langle a_x, a_y, a_z \rangle$ representing the accelerometer values, and so on as depicted in Figure 5. These advanced sensory features are monitored and recorded at a reduced sampling rate of 2Hz. This lower sampling rate is implemented to minimize battery power consumption while effectively capturing and analysing human gait patterns.

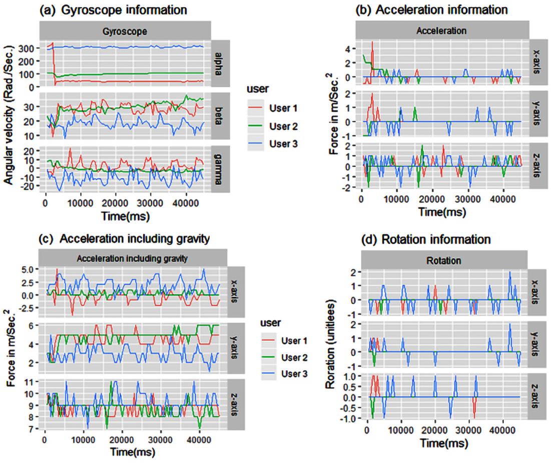


Fig. 5: Contrasting the sensory data from three randomly selected users involves examining Acceleration along the x, y, and z axes, Gyroscope data across alpha, beta, and gamma axes, Acceleration including gravity along the x, y, and z axes, and, Rotation along the x, y, and z axes.

4.4 Participants

The dataset comprises 87 participants, selected to provide a diverse representation across key demographic variables including age, gender, occupation, and educational background. The participant composition includes 48 males, 37 females, and 1 individual identifying with another gender, as illustrated in Figure 6. This diverse demographic coverage enhances the generalizability of the study's findings.

Participants were fully briefed on the data collection process, which included detailed information on data handling procedures, risks, confidentiality measures, and rights concerning their data and privacy.

4.5 Demographic Information

Data collection spanned 45 days and occurred at multiple locations, including the Visva-Bharati University campus, hostel facilities, and participants' residences in Bolpur and Bishnupur, West Bengal, India.

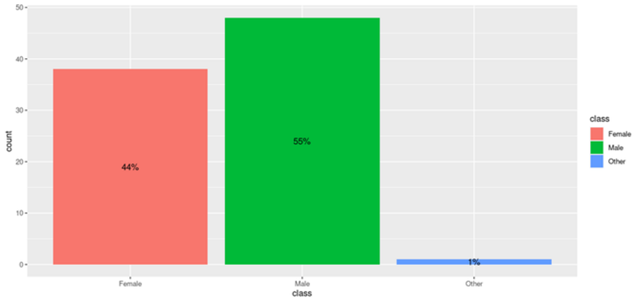


Fig. 6: Class distribution of volunteers.

4.6 Data Collection

Participants were instructed to carry the smartphone equipped with the web-based application in their pant pockets, as depicted in Figure 7. They were asked to walk on a flat surface in their normal manner for a duration of 1 minute and 30 seconds. Data was collected from each participant across two sessions, with each session consisting of two repetitions spaced 10 minutes apart. Sessions were separated by a 12-hour interval.

As participants moved, the smartphones in their pockets underwent positional shifts, leading to variations in sensor readings, including accelerometer, gyroscope, rotational, and gravity-augmented acceleration data. Consequently, the web-based application captured and recorded the sensory data reflecting these positional changes of the smartphone.

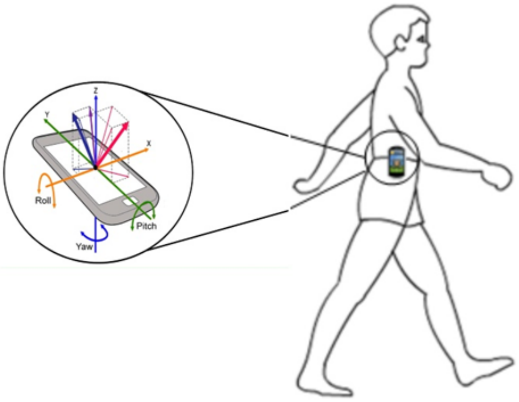


Fig. 7: Collection of human gait patterns through smartphone sensors.

5. MODEL IMPLEMENTATION AND EVALUATION

5.1 Performance Evaluation Metrics

The following metrics are employed to assess the performance of the anomaly detection algorithms:

(1) **Equal Error Rate (EER):** The EER represents the point at which the false acceptance rate (FAR) equals the false rejection rate (FRR), serving as an indicator of the balance between these two types of errors in the detection algorithm.

(2) **Standard Deviation (SD):** This metric quantifies the dispersion or variability of the error rates around their mean, providing insight into the consistency of the algorithm's performance.

(3) **95% Confidence Interval (CI):** The CI delineates the range within which the true mean of the error rate is expected to lie with 95% certainty, offering a statistical measure of the precision of the EER estimate.

(4) **p-Value from a One-Sample t-Test:** The p-value assesses the probability that the observed results are due to chance, thereby indicating the statistical significance of the algorithm's performance.

5.2 Model Implementation

(1) **Algorithm Selection:** For implementing human gait-based user authentication, selecting an optimal anomaly detection algorithm is crucial. This process involved an extensive evaluation of various anomaly detection techniques across diverse algorithmic families. These families include the L_p Minkowski distance family, the L_1 distance family, the Intersection distance family, the Squared-chord distance family, the Squared L_2 distance family, Shannon's entropy-based methods, as well as Support Vector-based, Probability Density-based, Statistics-based, Time Series Distance-based, and Logical Value Distance-based detectors. A total of 50 distinct anomaly detection algorithms from these families were tested. This rigorous selection process ensures that only the most effective and reliable algorithms are considered, establishing a benchmark for advanced performance in this field. The performances of a subset of these algorithms are summarized in Table 2.

(2) **Tools and Techniques:** The statistical programming language R (version 4.0.2) was utilized for implementing the proposed configurations and analyzing the results. All methodologies are accessible via the project page at `https://rstudio.cloud/project/4056744`, presented as interactive applications. This setup enables parameter variations and supports future deployment possibilities.

(3) **Model Evaluation:** Gait samples were collected from each participant across two sessions, with two repetitions per session, resulting in eight discrete samples per participant during the data augmentation phase. Four samples were allocated for template generation, while the remaining four were reserved for testing. Each participant's template was evaluated against an additional gait pattern to determine the FRR, followed by the assessment of FAR using gait patterns from eighty-six other participants. False acceptance and rejection rates were computed by comparing anomaly scores to personalized threshold values, based on gait consistency. This comprehensive evaluation methodology ensures thorough performance analysis of the model across diverse passwords and sessions, enhancing its capability to accurately distinguish legitimate user authentication attempts from potential unauthorized access.

6. RESULTS AND DISCUSSION

Table 2 presents the outcomes of Tukey's Honestly Significant Difference (TukeyHSD) analysis, which provides a detailed comparative evaluation of the selected anomaly detection algorithms. The table highlights the Estimated Equal Error Rates (AEERs) for each detector, along with their corresponding 95% Confidence Interval ranges (lower and upper EERs), standard deviations, and p-values derived from a one-sample t-test. This summary facilitates a comprehensive assessment of each algorithm's performance and the statistical significance of the observed differences.

6.1 Interpretation of the Results:

The symbols '+' and '-' in Table 2 represent deviations of each anomaly detector's performance relative to the proposed detector, indicating whether the parameter values are higher or lower, respectively. For instance, the One-Class Support Vector Machine (OCSVM) algorithm has an estimated Equal Error Rate (EER) of 14.32%, with a range from 16.01% to 17.86%, and a standard deviation of 0.1666. The Outlier Count algorithm presents an estimated EER of 14.53%, spanning from 11.03% to 18.02%, with a standard deviation of 0.0732. The Autoencoder algorithm shows an estimated EER of 14.79%, ranging between 10.95% and 18.62%, and has a standard deviation of 0.1801. These results are significant as the performances of these algorithms are closely comparable to that of the proposed detector, suggesting their potential utility as alternatives under certain conditions.
Conversely, algorithms such as Wave Hedges Distance and Canberra Distance exhibit more substantial deviations. The Wave Hedges Distance algorithm has an estimated EER of 19.69%, with a range from 16.09% to 23.29%, and a standard deviation of 0.1690. Similarly, the Canberra Distance algorithm shows an estimated EER of 19.76%, ranging from 16.25% to 23.42%, with a standard deviation of 0.1683. These detectors demonstrate greater performance variability compared to the Scaled Manhattan algorithm.

6.2 The Proposed Anomaly Detector

The Scaled Manhattan anomaly detector exhibited superior performance, achieving the lowest AEER of 13.76% among all evaluated algorithms. This performance underscores its effectiveness in minimizing errors when distinguishing between normal and anomalous gait patterns. The 95% CI for the EER of the Scaled Manhattan detector ranges from 10.21% to 17.31%, indicating stable performance across various test samples. The standard deviation of 16.68% suggests a moderate degree of variability in the AEER across samples, demonstrating consistent results among individuals. These findings validate the Scaled Manhattan algorithm as a robust and effective solution for gait-based user authentication.

6.3 Scaled-Manhattan Algorithm

The Scaled Manhattan algorithm quantifies similarity between two vectors by computing the normalized absolute differences between their corresponding elements and summing them. Mathematically, this is expressed as:

$$D_{\text{scaled-Manhattan}}(x,y) = \frac{1}{n}\sum_{i=1}^{n}\frac{|x_i - y_i|}{\text{range}_i} \qquad (1)$$

where x_i and y_i denote the values of the i-th feature in vectors x and y, respectively, and range$_i$ represents the range of the i-th feature across all data points. The scaled Manhattan distance is particularly effective in high-dimensional spaces and demonstrates resilience to outliers and variations in feature scaling. This method was selected due to its balance of computational efficiency and robustness in high-dimensional data contexts, making it suitable for complex biometric data analysis.

7. PERFORMANCE EVALUATION USING ROC CURVES

Receiver Operating Characteristic (ROC) curves are essential for evaluating the performance of anomaly detection algorithms. These curves are constructed by plotting the False Acceptance Rate (FAR) against the False Rejection Rate (FRR) across various threshold settings. Figures 8, 9, and 10 display ROC plots for three selected algorithms, showcasing their performance differences on the gait dataset.

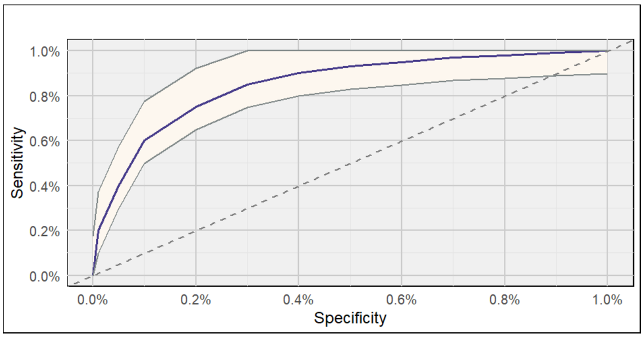


Fig. 8: ROC curve with 95% Confidence Interval (CI) for the Scaled Manhattan algorithm.

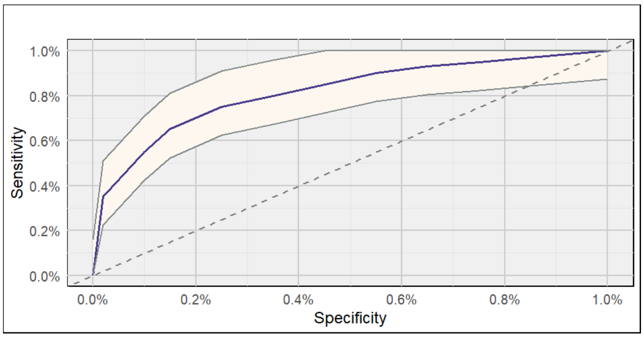


Fig. 9: ROC curve with 95% Confidence Interval (CI) for the Autoencoder algorithm.

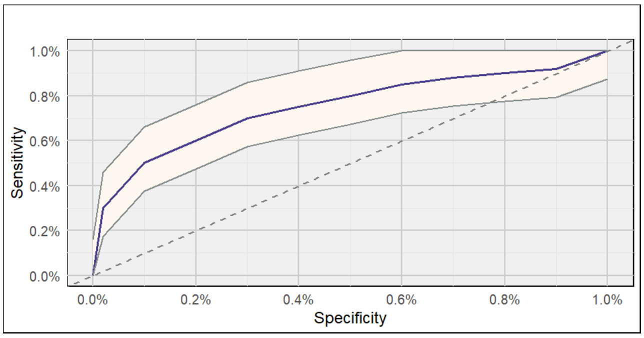


Fig. 10: ROC curve with 95% Confidence Interval (CI) for the Additive Symmetry algorithm.

Table 2. : TukeyHSD Analysis: Comparative performance of anomaly detectors on the gait dataset for active user authentication

Anomaly Detectors	**Estimated EER**	**Lower EER**	**Upper EER**	**Standard Deviation**	**p-Value**
highlightcolor **Scaled-Manhattan Distance (Proposed detector)**	**0.1376**	**0.1021**	**0.1731**	**0.1668**	**0.0002**
OCSVM	+0.0056	+0.0058	+0.0055	-0.0008	1.0000
Outlier-Count	+0.0077	+0.0082	+0.0072	-0.0024	1.0000
Autoencoder	+0.0103	+0.0074	+0.0131	+0.0133	0.9005
Bhattacharyya	+0.0124	+0.0116	+0.0133	+0.0039	0.8050
T-test	+0.0290	+0.0314	+0.0266	-0.0113	0.6770
Sorensen	+0.0568	+0.0575	+0.0560	-0.0036	0.3650
Soergel	+0.0568	+0.0575	+0.0560	-0.0036	0.1644
Kulczynski Distance	+0.0568	+0.0575	+0.0560	-0.0036	0.1644
Czekanowski Distance	+0.0568	+0.0575	+0.0560	-0.0036	0.1644
Motkya Distance	+0.0568	+0.0575	+0.0560	-0.0036	0.1644
Wave Hedges Distance	+0.0593	+0.0588	+0.0598	+0.0022	0.0084
Canberra Distance	+0.0607	+0.0604	+0.0611	+0.0015	0.0045
Jaccard Distance	+0.0611	+0.0625	+0.0598	-0.0063	0.0036
Dice Distance	+0.0611	+0.0625	+0.0598	-0.0063	0.0020
Chi Squared Distance	+0.0613	+0.0615	+0.0611	-0.0008	0.0001
Prob Symmetric	+0.0613	+0.0615	+0.0611	-0.0008	0.0001
Average Distance	+0.0638	+0.0648	+0.0644	-0.0013	0.0001
Manhattan Distance	+0.0646	+0.0648	+0.0644	-0.0010	0.0001
Gower Distance	+0.0646	+0.0648	+0.0644	-0.0010	0.0000
Additive Symmetry	+0.0654	+0.0677	+0.0632	-0.0107	0.0000

Figure 8 illustrates the ROC curve for the Scaled Manhattan algorithm, with the curve delineated by the 95% CI bounds. The curve's proximity to the top-left corner indicates a high true positive rate and a low false positive rate across different threshold settings. This positioning, coupled with the CI bounds, demonstrates that Scaled Manhattan achieves an optimal trade-off between FAR and FRR for the gait dataset, establishing it as the most effective algorithm in our comparison.

Figure 9 presents the ROC curve for the Autoencoder algorithm with its 95% CI bounds. Although the curve indicates reasonable performance, it does not reach the effectiveness of the Scaled Manhattan algorithm. The Autoencoder curve, while relatively favorable, shows a lower Area Under the Curve (AUC) compared to Scaled Manhattan, suggesting that it does not achieve the same level of accuracy and reliability in distinguishing authentic from anomalous gait patterns.

Figure 10 depicts the ROC curve for the Additive Symmetry algorithm with 95% CI ranges. This curve is situated further from the top-left corner, indicating inferior performance in terms of both FAR and FRR. The lower AUC for Additive Symmetry highlights its reduced efficacy in differentiating between authentic and imposter gait samples compared to Scaled Manhattan and Autoencoder, positioning it as the least effective among the tested algorithms.

8. BOX PLOT ANALYSIS OF ANOMALY DETECTION ALGORITHMS

Figure 11 provides a comparative analysis of the performance of ten selected anomaly detection algorithms through a box plot. Each point in the box plot represents the Equal Error Rate (EER) obtained from authenticating a single individual using the respective algorithm. Consequently, each box contains 87 data points reflecting the EER values for the 87 participants in the study. The boxes display the interquartile range (IQR), capturing the central 50% of the data where most EER values are concentrated, with the internal horizontal line representing the median EER. Additionally, the red dot within each box signifies the mean EER, providing a clear depiction of average performance across subjects. This visualization facilitates a comprehensive evaluation of the effectiveness and consistency of each anomaly detection method in the context of gait-based user authentication.

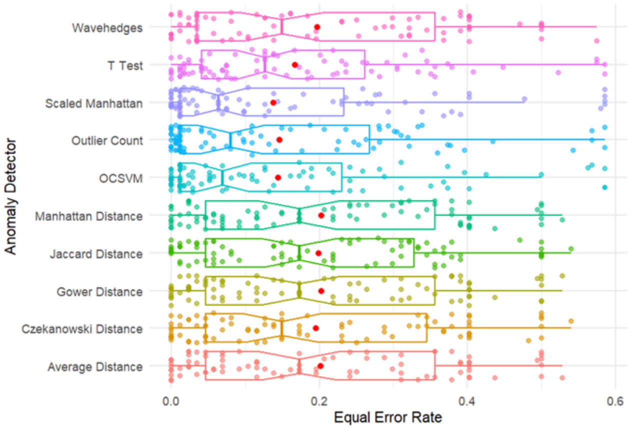


Fig. 11: Performance of selected anomaly detectors and associated risk.

Algorithms such as Scaled Manhattan, OCSVM, and Outlier Count exhibit not only lower mean EER values but also a significant concentration of data points near the zero EER line. This indicates high effectiveness in accurately authenticating individuals based on gait patterns, achieving minimal error rates in numerous cases.

In contrast, algorithms like Average Distance, Jaccard Distance, and Wave Hedges Distance show fewer data points clustered at zero EER. This suggests these methods are less effective in attaining low error rates for a substantial number of individuals. The lower density of data points at zero EER implies that these algorithms may not be as consistently reliable for gait-based authentication.

Furthermore, Figure 11 reveals that certain algorithms, particularly Average Distance and Gower Distance, have several data points significantly distant from the mean EER. This variability in performance may be attributed to the algorithm's sensitivity to gait pattern variations or less effective handling of outliers. Conversely, Scaled Manhattan, OCSVM, and Outlier Count display a more uniform distribution around the mean EER, reflecting more consistent performance with reduced extreme variability.

In summary, Scaled Manhattan, OCSVM, and Outlier Count are superior in both average performance and consistency. These algorithms demonstrate a high concentration of low EER values, making them robust choices for gait-based user authentication. The consistency and effectiveness of these methods highlight their suitability for reliable authentication applications, while algorithms with higher variability and fewer zero EER data points are less reliable for consistent performance, suggesting they may not be as effective for accurate gait-based authentication in diverse real-world scenarios.

9. STATISTICAL SIGNIFICANCE VALIDATION WITH ONE-SAMPLE T-TEST

The p-values listed in Table 2 are derived from a one-sample t-test. For the Scaled Manhattan detector, the p-value of 2.123e-11 indicates a statistically significant deviation from the assumed population mean of zero, as it is substantially below the significance threshold of 0.05. The t-statistic of 7.7008 indicates a significant deviation from the hypothesized mean, supporting the rejection of the null hypothesis. The 95% Confidence Interval (CI) for the true mean ranges from 0.1020512 to 0.1731496, reinforcing the conclusion that the population mean is significantly different from zero. Therefore, we accept the alternative hypothesis that the true mean of the algorithm's EER is significantly different from zero.

For other algorithms such as OCSVM and Outlier Count, the p-values of 1.0000 suggest their performance is statistically similar to that of the Scaled Manhattan detector. In cases of high feature dimensions or large numbers of gait samples, these algorithms could serve as viable alternatives. Conversely, algorithms such as Wave Hedges Distance and Jaccard Distance, with p-values of 0.0084 and 0.0036 respectively, do not meet the significance threshold. These lower p-values indicate significant performance differences from the Scaled Manhattan algorithm, suggesting they are less suitable as replacements in this context. Similarly, the Chi Squared Distance algorithm, with a p-value of 0.0001, cannot substitute the Scaled Manhattan detector due to its statistically significant deviation from the expected performance.

10. SOFT BIOMETRIC TRAIT INCORPORATION

Incorporating multiple soft biometric traits sequentially into the proposed anomaly detector results in a progressive improvement in EER, as illustrated in Figure 12. This cumulative effect underscores the benefit of integrating diverse biometric features to enhance the accuracy and effectiveness of the proposed detector.

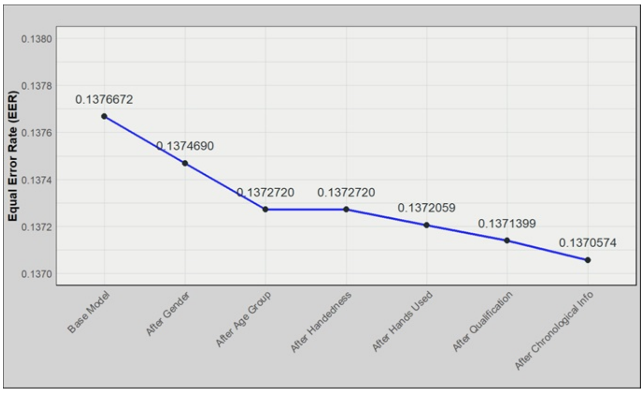


Fig. 12: Improvement in EER of the proposed detector due to the inclusion of soft biometric traits.

11. COMPARISON WITH EXISTING SYSTEMS

In comparing our results with state-of-the-art methodologies, the Scaled Manhattan anomaly detector achieved a mean EER of 13.76%, which does not surpass the most optimal performances reported in recent literature. For example, contemporary approaches such as GA-KNN and Autoencoder have demonstrated lower EER values of 2.3% and 4%, respectively. These methods utilize advanced techniques and feature combinations that contribute to their superior accuracy. Nevertheless, our system's performance remains commendable in terms of real-world applicability and practicality. The Scaled Manhattan detector's performance, with a range of 10.20% to 13.76% for individual gait verification, underscores its reliability and effectiveness. Our study, integrating sensory features from smartphones and employing a sophisticated web-based application, highlights a practical and scalable approach that meets contemporary needs for accessible and continuous user authentication. The inclusion of soft biometric traits into our model not only improves precision but also represents a novel application of smartphone sensors in health-focused authentication systems. Although not achieving the lowest EER reported, this integration advances gait-based authentication towards more feasible and user-friendly solutions, aligning with both security and wellness objectives.

12. CONCLUSION

Smartphone sensors offer invaluable tools for active user authentication, presenting a promising avenue for innovative gait-based authentication. Our study demonstrates the efficacy of the Scaled Manhattan algorithm as a top-tier anomaly detection method suitable for real-time applications. By employing Scaled Manhattan as a classifier alongside sensory features collected at a low sampling rate, we address the challenge of verifying insurance holders' eligibility for the 10,000 daily steps requirement, thereby mitigating the risk of fraudulent claims. Future research directions include optimizing battery consumption, enhancing anomaly detection performance under varied conditions, and improving verification across diverse environments. These efforts hold potential to further advance the efficacy and practical deployment of gait-based authentication systems in securing health and wellness initiatives.

13. ACKNOWLEDGEMENT

The authors wish to express their heartfelt thanks for the financial support received from DST-INSPIRE, which made this research project possible. They also deeply appreciate the contributions of the eighty-seven volunteers who generously provided their gait patterns for the study.

14. REFERENCES

[1] Aditya Birla Health launches new policy with up to 100% return of premium — Mint.

[2] Ala Abdulhakim Abdulaziz. *Features Extraction Scheme for Behavioural Biometric Authentication in Touchscreen Mobile Devices*. PhD thesis, Universiti Teknologi Malaysia, 2016.

[3] Alejandro Acien, Aythami Morales, Ruben Vera-Rodriguez, Julian Fierrez, and Ruben Tolosana. MultiLock: Mobile active authentication based on multiple biometric and behavioural patterns. In *Proceedings of the 1st International Workshop on Multimodal Understanding and Learning for Embodied Applications (MULEA 2019)*, pages 53–59, 2019.

[4] Jamil Ahmad, Muhammad Sajjad, Zahoor Jan, Irfan Mehmood, Seungmin Rho, and Sung Wook Baik. Analysis of interaction trace maps for active authentication on smart devices. *Multimedia Tools and Applications*, 76(2017):4069–4087, 2017.

[5] Md Liakat Ali, John V. Monaco, Charles C. Tappert, and Meikang Qiu. Keystroke biometric systems for user authentication. *Journal of Signal Processing Systems*, 86(217):1–16, 2016.

[6] Arwa Alsultan, Kevin Warwick, and Hong Wei. Free-text keystroke dynamics authentication for Arabic language. *IET Biometrics*, 5(3):164–169, 2016.

[7] Prince Yaw Owusu Amoako and Isaac Olusegun Osunmakinde. Emerging bimodal biometrics authentication for non-venue-based assessments in open distance e-learning (OdeL) environments. *International Journal of Technology Enhanced Learning*, 12(2), 2020.

[8] Noureddine Amraoui, Amine Besrour, Riadh Ksantini, and Belhassen Zouari. Implicit and continuous authentication of smart home users. In *Proceedings of the 33rd International Conference on Advanced Information Networking and Applications (AINA 2019)*, pages 1228–1239, 2020.

[9] Margit Antal, Zsolt Bokor, and László ZsoltSzabó. Information revealed from scrolling interactions on mobile devices. *Pattern Recognition Letters*, 56(2015):7–13, 2015.

[10] Tanapat Anusas-Amornkul. Strengthening password authentication using keystroke dynamics and smartphone sensors. In *Proceedings of the 9th International Conference on Information Communication and Management (ICICM 2019)*, ACM International Conference Proceeding Series, pages 70–74. Association for Computing Machinery, 2019.

[11] S. Ayeswarya and Jasmine Norman. A survey on different continuous authentication systems. *International Journal of Biometrics*, 11(1):67–99, 2019.

[12] Okan Engin Basar, Gulfem Alptekin, Hasan Can Volaka, Mustafa Isbilen, and Ozlem Durmaz Incel. Resource usage analysis of a mobile banking application using sensor-and-touchscreen-based continuous authentication. *Procedia Computer Science*, 155:185–192, 2019.

[13] Michael Boakye Osei, Enoch Opanin Gyamfi, and Mohammed Okoe Alhassan. Keystroke dynamics algorithm for securing web-based password driven systems. *Asian Journal of Research in Computer Science*, 4(4):1–26, 2020.

[14] A. Buriro, S. Gupta, B. Crispo, and F.D. D Frari. DIALERAUTH: A motion-assisted touch-based smartphone user authentication scheme. In *Proceedings of the 8th ACM Conference on Data and Application Security and Privacy (CODASPY 2018)*, pages 267–276, Tempe, AZ, USA, 2018. Association for Computing Machinery.

[15] Yufei Chen, Chao Shen, Zhao Wang, and Tianwen Yu. Modeling interactive sensor-behavior with smartphones for implicit and active user authentication. In *Proceedings of the IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2017)*, pages 1–6, 2017.

[16] Heather Crawford, Karen Renaud, and Tim Storer. A framework for continuous, transparent mobile device authentication. *Computers and Security*, 39(2013):127–136, 2013.

[17] Timothy Dee, Ian Richardson, and Akhilesh Tyagi. Continuous transparent mobile device touchscreen soft keyboard biometric authentication. In *Procedings of the 32nd International Conference on VLSI Design and 18th International Conference on Embedded Systems (VLSID 2019)*, pages 539–540. IEEE, jan 2019.

[18] Daniel Escobar Grisales, Juan. C. Vásquez-Correa, Jesús F. Vargas-Bonilla, and Juan Rafael Orozco-Arroyave. Identity verification in virtual education using biometric analysis based on keystroke dynamics. *TecnoLógicas*, 23(47):197–211, 2020.

[19] Tao Feng, Xi Zhao, Nick Desalvo, Tzu Hua Liu, Zhimin Gao, Xi Wang, and Weidong Shi. An investigation on touch biometrics: Behavioral factors on screen size, physical context and application context. *Proceedings of the IEEE International Symposium on Technologies for Homeland Security (HST 2015)*, 2015.

[20] Andrew Foresi and Reza Samavi. User authentication using keystroke dynamics via crowdsourcing. In *Proceedings of the 17th International Conference on Privacy, Security and Trust (PST 2019)*, pages 1–3, 2019.

[21] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Transactions on Information Forensics and Security*, 8(1):136–148, 2013.

[22] Ahmet Melih Gedikli and Mehmet Önder Efe. A Simple Authentication Method with Multilayer Feedforward Neural Network Using Keystroke Dynamics. In Chawki Djeddi, Akhtar Jamil, and Imran Siddiqi, editors, *Proceedings of the 4th Mediterranean Conference Pattern Recognition and Artificial Intelligence (MedPRAI 2020)*, volume 1144 of *Communications in Computer and Information Science*, pages 9–23. Springer, Cham, 2020.

[23] Romain Giot, Mohamad El-Abed, Baptiste Hemery, and Christophe Rosenberger. Unconstrained keystroke dynamics authentication with shared secret. *Computers and Security*, 30(6-7):427–445, 2011.

[24] Romain Giot and Anderson Rocha. Siamese networks for static keystroke dynamics authentication. In *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS 2019)*, pages 1–6, 2019.

[25] Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. Demystifying Authentication Concepts in Smartphones: Ways and Types to Secure Access. *Mobile Information Systems*, 2018.

[26] Eiji Hayashi, Sauvik Das, Shahriyar Amini, Jason Hong, and Ian Oakley. CASA: Context-aware scalable authentication. In *Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS 2013)*, pages 1–10, 2013.

[27] Itay Hazan, Oded Margalit, and Lior Rokach. Securing keystroke dynamics from replay attacks. *Applied Soft Computing Journal*, 85(2019):105798, 2019.

[28] Jiacang Ho and Dae Ki Kang. One-class Naïve Bayes with duration feature ranking for accurate user authentication using keystroke dynamics. *Applied Intelligence*, 48(6):1547–1564, 2018.

[29] Anbiao Huang, Shuo Gao, Junliang Chen, Lijun Xu, and Arokia Nathan. High security user authentication enabled by piezoelectric keystroke dynamics and machine learning. *IEEE Sensors Journal*, 20(21):13037–13046, 2020.

[30] Hani Jawed, Zara Ziad, Muhammad Mubashir Khan, and Maheen Asrar. Anomaly detection through keystroke and tap dynamics implemented via machine learning algorithms. *Turkish Journal of Electrical Engineering and Computer Sciences*, 28(2018):1698–1709, 2018.

[31] Himanka Kalita, Emanuele Maiorana, and Patrizio Campisi. Keystroke dynamics for biometric recognition in handheld devices. In *Proceedings of the 43rd International Conference on Telecommunications and Signal Processing (TSP 2020)*, pages 410–416, 2020.

[32] Hassan Khan, Aaron Atwater, and Urs Hengartner. Itus: An implicit authentication framework for android. In *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking (MobiCom 2014)*, pages 507–518. Association for Computing Machinery, 2014.

[33] Ali Khodabakhsh, Erwin Haasnoot, and Patrick Bours. Predicted templates: Learning-curve based template projection for keystroke dynamics. In *Proceedings of the International Conference of the Biometrics Special Interest Group (IOSIG 2018)*, pages 1–5, 2018.

[34] Kevin S. Killourhy and Roy A. Maxion. Comparing anomaly-detection algorithms for keystroke dynamics. In *Proceedings of the International Conference on Dependable Systems and Networks*, pages 125–134, 2009.

[35] Dong In Kim, Shincheol Lee, and Ji Sun Shin. A new feature scoring method in keystroke dynamics-based user authentications. *IEEE Access*, 8(2020):27901–27914, 2020.

[36] Gutha Jaya Krishna and Vadlamani Ravi. Keystroke based user authentication using modified differential evolution. In *Proceedings of the IEEE Region 10th Annual International Conference (TENCON 2019)*, pages 739–744. IEEE, 2019.

[37] Hyungu Lee, Jung Yeon Hwang, Dong In Kim, Shincheol Sung-Hoon Lee, Shincheol Sung-Hoon Lee, and Ji Sun Shin. Understanding keystroke dynamics for smartphone users authentication and keystroke dynamics on smartphones built-in motion sensors. *Security and Communication Networks*, 2018:1–10, 2018.

[38] Hyungu Lee, Jung Yeon Hwang, Shincheol Sung Hoon Lee, Dong In Kim, Shincheol Sung Hoon Lee, Jaehwan Lee, and Ji Sun Shin. A parameterized model to select discriminating features on keystroke dynamics authentication on smartphones. *Pervasive and Mobile Computing*, 54(2019):45–57, 2019.

[39] Shincheol Sung-Hoon Lee, Jung Yeon Hwang, Hyungu Lee, Dong In Kim, Shincheol Sung-Hoon Lee, and Ji Sun Shin. Distance-based keystroke dynamics smartphone authentication and threshold formula model. *Journal of the Korea Institute of Information Security and Cryptology*, 28(2):369–383, 2018.

[40] Sung Hoon Lee, Jong Hyuk Roh, Soo Hyung Kim, and Seung Hun Jin. Feature subset for improving accuracy of keystroke dynamics on mobile environment. *Journal of Information Processing Systems*, 14(2):523–538, 2018.

[41] Wei Han Lee and Ruby B. Lee. Implicit smartphone user authentication with sensors and contextual machine learning. In *Proceedings of the 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2017)*, pages 1–12, 2017.

[42] Wei Han Lee, Jorge Ortiz, Bongjun Ko, and Ruby Lee. Inferring smartphone users' handwritten patterns by using motion sensors. *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018.

[43] Lingjun Li, Xinxin Zhao, and Guoliang Xue. Unobservable re-authentication for smartphones. In *Proceedings of the 20th Annual Network and Distributed System Security Symposium*, pages 1–16. The Internet Society, 2013.

[44] Yantao Li, Hailong Hu, and Gang Zhou. Using data augmentation in continuous authentication on smartphones. *IEEE Internet of Things Journal*, 6(1):628–640, 2019.

[45] Md Liakat Ali and Charles C. Tappert. POHMM/SVM: A hybrid approach for keystroke biometric user authentication. In *Proceedings of the IEEE International Conference on Real-Time Computing and Robotics (RCAR 2018)*, pages 612–617, 2019.

[46] Xiaoshi Liang, Futai Zou, Linsen Li, and Ping Yi. Mobile terminal identity authentication system based on behavioral characteristics. *International Journal of Distributed Sensor Networks*, 16(1):1–12, 2020.

[47] X. Liu, C. Shen, and Y. Chen. Multi-source interactive behavior analysis for continuous user authentication on smartphones. In Jie Zhou, Yunhong Wang, Zhenan Sun, Zhenhong Jia, Jianjiang Feng, Shiguang Shan, Kurban Ubul, and Zhenhua Guo, editors, *Proceedings of the Chinese Conference on Biometric Recognition (CCBR 2018)*, volume 10996 of *Lecture Notes in Computer Science*, pages 669–677. Springer, Cham, 2018.

[48] Upal Mahbub, Sayantan Sarkar, Vishal M. Patel, and Rama Chellappa. Active user authentication for smartphones: A challenge data set and benchmark results. In *Proceedings of the IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS 2016)*, pages 1–8, 2016.

[49] Saket Maheshwary and Vikram Pudi. Mining keystroke timing pattern for user authentication. In Annalisa Appice, Michelangelo Ceci, Corrado Loglisci, Elio Masciari, and Zbigniew W. Raś, editors, *Proceedings of the International Workshop on New Frontiers in Mining Complex Patterns (NFMCP 2016)*, volume 10312 of *Lecture Notes in Computer Science*, pages 213–227. Springer, Cham, 2017.

[50] Abir Mhenni, Estelle Cherrier, Christophe Rosenberger, and Najoua Essoukri Ben Amara. Analysis of Doddington zoo classification for user dependent template update: Application to keystroke dynamics recognition. *Future Generation Computer Systems*, 97(2019):210–218, 2019.

[51] Abir Mhenni, Estelle Cherrier, Christophe Rosenberger, and Najoua Essoukri Ben Amara. Double serial adaptation mechanism for keystroke dynamics authentication based on a single password. *Computers and Security*, 83(2019):151–166, 2019.

[52] Abir Mhenni, Denis Migdal, Estelle Cherrier, Christophe Rosenberger, and Najoua Essoukri Ben Amara. Vulnerability of adaptive strategies of keystroke dynamics based authentication against different attack types. In *Proceedings of the International Conference on Cyberworlds (CW 2019)*, pages 274–278, 2019.

[53] Jugurta Montalvão, Eduardo O. Freire, Murilo A. Bezerra, and Rodolfo Garcia. Contributions to empirical analysis of keystroke dynamics in passwords. *Pattern Recognition Letters*, 52, 2014.

[54] Hebatollah Mostafa, Abeer Mohamed Elkorany, Mohammad El-Ramly, and Hassan Shaban. Behavio2Auth: Sensor-based behavior biometric authentication for smartphones. In *Proceedings of the ArabWIC 6th Annual International Conference Research Track (ArabWIC 2019)*, pages 1–6. Association for Computing Machinery, 2019.

[55] Masanori Nakakuni and Hiroshi Dozono. User authentication method for computer-based online testing by analysis of keystroke timing at the input of a family name. In *Proceedings of the International Conference on Computational Science and Computational Intelligence (CSCI 2018)*, pages 71–76, 2018.

[56] Ha Nguyen Ngoc and Ngoc Tran Nguyen. An enhanced distance metric for keystroke dynamics classification. *Eighth International Conference on Knowledge and Systems Engineering*, pages 285–290, 2016.

[57] Yogesh Patel, Karim Ouazzane, Vassil T. Vassilev, Ibrahim Faruqi, and George L. Walker. Keystroke dynamics using auto encoders. In *Proceedings of the International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2019*, pages 1–8, 2019.

[58] Shivani Payal, Bhushan Garware, and Shubhangi Kelkar. Towards designing a framework for practical keystroke dynamics based authentication. In *Advances in Intelligent Systems and Computing*, volume 614, 2018.

[59] Darpan Kumar Purwar, Deepika Vishwakarma, Neha Singh, and Vineeta Khemchandani. One v/s all SVM implementation for keystroke based authentication system. In *Proceedings of the 4th International Conference on Information Systems and Computer Networks (ISCON 2019)*, pages 268–272, 2019.

[60] Suhail Javed Quraishi and Sarabjeet Singh Bedi. On keystrokes as continuous user biometric authentication. *International Journal of Engineering and Advanced Technology*, 8(6):4149–4153, 2019.

[61] Siti Rahayu Selamat, Teh Teck Guan, and Robiah Yusof. Enhanced authentication for web-based security using keystroke dynamics. *International Journal of Network Security and Its Applications*, 12(4):1–16, 2020.

[62] Khandaker Abir Rahman, Deepak Neupane, Abdulrahman Zaiter, and Md Shafaeat Hossain. Web user authentication using chosen word keystroke dynamics. In *Proceedings - 18th IEEE International Conference on Machine Learning and Applications, ICMLA 2019*, 2019.

[63] Nataasha Raul, Royston D'mello, Mandar Bhalerao, Royston D'mello, and Mandar Bhalerao. Keystroke dynamics authentication using small datasets. In *Proceedings of the Security*

and Privacy: Second ISEA International Conference (ISEA-ISAP 2018), volume CCIS 939, pages 89–96, 2019.

[64] Aditi Roy, Tzipora Halevi, and Nasir Memon. An HMM-based behavior modeling approach for continuous mobile authentication. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2014)*, pages 1–5, 2014.

[65] Napa Sae-Baeid, Nasir Memon, Napa Sae-bae Id, and Nasir Memon. Distinguishability of keystroke dynamic template. *PLoS ONE*, 17(1):1–17, jan 2022.

[66] Baljit Singh Saini, Parminder Singh, Anand Nayyar, Navdeep Kaur, Kamaljit Singh Bhatia, Shaker El-Sappagh, and Jong Wan Hu. A three-step authentication model for mobile phone user using keystroke dynamics. *IEEE Access*, 8(2020):125909–125922, 2020.

[67] Asma Salem, Ahmad Sharieh, Azzam Sleit, and Riad Jabri. Enhanced authentication system performance based on keystroke dynamics using classification algorithms. *KSII Transactions on Internet and Information Systems*, 13(8), 2019.

[68] Chao Shen, Yuanxun Li, Yufei Chen, Xiaohong Guan, and Roy A. Maxion. Performance analysis of multi-motion sensor behavior for active smartphone authentication. *IEEE Transactions on Information Forensics and Security*, 133(1):48–62, 2017.

[69] Chao Shen, Yong Zhang, Zhongmin Cai, Tianwen Yu, and Xiaohong Guan. Touch-interaction behavior for continuous user authentication on smartphones. In *Proceedings of the International Conference on Biometrics (ICB 2015)*, pages 157–162, 2015.

[70] Zdenka Sitova, Jaroslav Sedenka, Qing Yang, Ge Peng, Gang Zhou, Paolo Gasti, and Kiran S. Balagani. HMOG: New behavioral biometric features for continuous authentication of smartphone users. *IEEE Transactions on Information Forensics and Security*, 11(5):877–892, 2016.

[71] Lichao Sun, Yuqi Wang, Bokai Cao, Philip S. Yu, Witawas Srisa-An, and Alex D. Leow. Sequential Keystroke Behavioral Biometrics for Mobile User Identification via Multi-view Deep Learning. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017.

[72] Yan Sun, Hayreddin Ceker, and Shambhu Upadhyaya. Shared keystroke dataset for continuous authentication. In *Proceedings of the 8th IEEE International Workshop on Information Forensics and Security (WIFS 2016)*, pages 1–6, 2017.

[73] Ramin Toosi and Mohammad Ali Akhaee. Time-frequency analysis of keystroke dynamics for user authentication. *Future Generation Computer Systems*, 115(2021):438–447, feb 2021.

[74] Tim Van hamme, Davy Preuveneers, and Wouter Joosen. Managing distributed trust relationships for multi-modal authentication. *Journal of Information Security and Applications*, 40(2018):258–270, 2018.

[75] Yuhua Wang, Chunhua Wu, Kangfeng Zheng, and Xiujuan Wang. Improving reliability: User authentication on smartphones using keystroke biometrics. *IEEE Access*, 7(2019):26218–26228, 2019.

[76] Guannan Wu, Jian Wang, Yongrong Zhang, and Shuai Jiang. A continuous identity authentication scheme based on physiological and behavioral characteristics. *Sensors*, 18(1):179, 2018.

[77] Yafang Yang, Bin Guo, Zhu Wang, Mingyang Li, Zhiwen Yu, and Xingshe Zhou. BehaveSense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics. *Ad Hoc Networks*, 84(2019):9–18, 2019.

[78] Enzhe Yu and Sungzoon Cho. Keystroke dynamics identity verification: Its problems and practical solutions. *Computers and Security*, 23(5):428–440, 2004.