International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 1, February 2022, pp. 802~815
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i1.pp802-815

Behavioral biometric based personal authentication in feature phones

Amitabh Thapliyal[1], Om Prakash Verma[1], Amioy Kumar[2]
[1]Department of Computer Science and Engineering, Delhi Technological University, Delhi, India
[2]Tech Lead, Data Science, Intel Corp, Bangalore, India

Article Info

Article history:

Received Mar 25, 2021
Revised Jul 17, 2021
Accepted Jul 30, 2021

Keywords:

Behavioral biometric
Feature phone
Fuzzy
Keystroke
Pattern recognition

ABSTRACT

The usage of mobile phones has increased multifold in the recent decades mostly because of its utility in most of the aspects of daily life, such as communications, entertainment, and financial transactions. Feature phones are generally the keyboard based or lower version of touch based mobile phones, mostly targeted for efficient calling and messaging. In comparison to smart phones, feature phones have no provision of a biometrics system for the user access. The literature, have shown very less attempts in designing a biometrics system which could be most suitable to the low-cost feature phones. A biometric system utilizes the features and attributes based on the physiological or behavioral properties of the individual. In this research, we explore the usefulness of keystroke dynamics for feature phones which offers an efficient and versatile biometric framework. In our research, we have suggested an approach to incorporate the user's typing patterns to enhance the security in the feature phone. We have applied k-nearest neighbors (k-NN) with fuzzy logic and achieved the equal error rate (EER) 1.88% to get the better accuracy. The experiments are performed with 25 users on Samsung On7 Pro C3590. On comparison, our proposed technique is competitive with almost all the other techniques available in the literature.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Amitabh Thapliyal
Department of Computer Science and Engineering, Delhi Technological University
Delhi, India
Email: amitabh.thapliyal@gmail.com

1. INTRODUCTION

In the last decade, the use of mobile phones and personal digital assistant (PDA) devices increased tremendously. The growth of mobile phones has increased over the period of time with tremendous improvement at technology side. Be it network growth from 2G to 5G and handset evolution from feature phone to powerful smartphones. As per the report from GSMA [1], there are 5.2 billion subscribers globally. However, the growth of mobile phones has also increased the mobile related thefts and fraud rates with 183 smartphones are stolen everyday between March 2015 and March 2016 in UK itself [2]. Mobile phones become potential targets as most of the transactions nowadays take place through them from the management of bank accounts to the buying and selling of stocks. This raises a potential question regarding the security of the mobile phone [3], [4]. Nowadays, different authentication approaches have been used on handheld devices to ensure the security of content [5], [6]. Some of them are password, fingerprint, iris, face, and pattern. These approaches are now the mainstream authentication techniques used across all the handheld and portable devices. The demerit of the existing approaches is that they are prone to shoulder surfing, guessing attacks, brute force attacks and dictionary attacks. Shoulder surfing is a password attack in which the user's password is compromised by peeping in the password entry screen while the actual user types in the password [7].

Relatively newer authentication method, that is pattern-based authentication in touchscreen devices, is also prone to the finger marks and smudges which can be used to lift the pattern sequence. As per recent report from counter point research, there is going to be a huge demand for the feature phone market as mentioned in [8]. Globally, the feature phone segment is forecast to generate around US $16 billion cumulatively in wholesale hardware revenues over the next three years. There affordability of feature phones is one of the major reasons why feature phones are the preferred mobile phone in many developing countries like India, Africa and Bangladesh. The market reports from counterpoint and shipment opportunity for feature phones there is a strong need to have robust security system [9], [10] without any additional hardware cost. In our proposed work, we have developed one of authentication solution based on behavioral keystroke dynamics from the user's learned machine learning model for feature phones.

To address the security issues in the feature phones, new age authentication technique uses biometrics as a means to identify the actual user. Biometric authentication [11] recognizes individuals by depending on their behavioral or physiological features like; fingerprints, iris, voice and signature. To deploy the fingerprint scanner or iris to the feature phone, it requires additional cost, memory and high computing power in the device which tend to increase the cost of the phone, therefore, such system is not feasible option in feature phone. Also, the conventional approaches are one-time authentication methods, in which a user can access the sensitive content if he or she logs the system with the correct password. Post acceptance of the password, there is no commercially available authentication system to ensure the continuity of security for that sensitive content in feature phones based on behavioral biometrics. Once the user is approved, there is no further screening of user which can help to detect if imposter is operating the device. Face, fingerprints and iris are examples of biometric solutions available in smartphones to offer high-end secure access control. In order to provide such biometric systems, it requires additional cost to mobile device because of additional equipment and hardware costs like fingerprint scanner, iris sensors requirement. Also, fingerprint and iris require high memory and computing power to perform and execute. Moreover, in case of feature phones which are low cost there is no support of biometric based authentication. To overcome this issue efficiently keystroke biometrics has been utilized in literature. Keystroke biometric authentication is behavioral based and it uses user's key input patterns and it based on the fact that each individual user's typing patterns are unique and consistent.

Many approaches to authenticate a device by keystroke biometrics have come in foreplay. Clarke and Furnell [12] analyzed user authentication based on keystroke input patterns on handset devices. They have utilized the key input of 11-digit phone numbers and 4-digit password to classify individuals. Their models were based on the generalized regression networks with accuracy of equal error rate (EER) ranging from 9% to 16%. Hwang *et al.* [13] achieved EER of 13% when applying the arthematics rhythms with Cues. They have utilized the key input 4-digit password to classify the users. Their models employed framework where only valid user's patterns are used for training purpose. In their work 25 users participated and they collected only 5 patterns from each user for enrollment.

Motwani *et al.* [14] in their work, the dataset was dynamically generated and the impostors were not involved during the enrollment phase, false rejection rate (FRR) was 3.2% with only 27 features. Stanciu *et al.* [15] focused on effectiveness of sensor-enhanced keystroke dynamics, they have utilized movement sensors that is accelerometer and gyroscope in their work. In their work 20 users participated and they gathered keystroke and sensor samples in controlled environment on Samsung Nexus S device. In their work results suggest that basic keyboard authentication is prone to attacks and when sensors are considered they obtained better results against statistical attacks. Huang *et al.* [16] achieved EER of 7.5% with their work for smartphone device on Android platform. They utilized statistical classification technique in their model. In their work client side, they developed Android application to capture the keystroke data, and server-side system database and authentication engine was developed as web service. The total of 40 users aged from 22 to 55 years old participated in their experiments.

It has been observed that existing security authentication mechanism in feature phones are based on personal identification number (PIN) or password characters. Current security authentication provided in feature phones are prone to the security attacks from imposters and fraudulent attackers. The basic concept with keystroke dynamics is the capacity of the method to understand the patterns like typing pattern during keyboard usage from the individual and then use this as a parameter to verify the user. A person typing on the mobile device will have the check if the time difference between typing of each of the letters of the password is similar to the owner's typing pattern. In the proposed work, the typing pattern (keystroke modality) of the user is learned with the k-nearest neighbors (k-NN) and fuzzy logic. The experimental data was collected on Samsung On7 Pro C3590 and the model was trained on the desktop PC Windows 10, by dividing the data into training and validation set. The next part of the paper is organized as follows section 2 explains our work keystroke dynamics-based authentication, section 3 explains results and discussion and future work and conclusion are discussed in section 4.

2. KEYSTROKE DYNAMICS APPROACH FOR FEATURE PHONES

The behavioral biometric [17], [18] technology proposed in the paper by analyzing the typing pattern of the user which is also known as Keystroke dynamics. Behavioral biometric is the field of study that uniquely measures patterns of human activities and thereby identifies the user. Behavioral biometric authentication methods include Keystroke dynamics, Touch dynamics, Voice, Signatures and Gait. Figure 1 shows the various known behavioral biometric methods. Behavioral biometrics provide secure authentication for banking and insurance applications, retail point of sales, and various other domain that need continuous authentication based on user's interaction with system. The block diagram of the proposed keystroke dynamics authentication system is shown in Figure 2. The whole process of keystroke dynamics is divided in to the following three steps: i) enrolment, ii) model training, and iii) authentication.

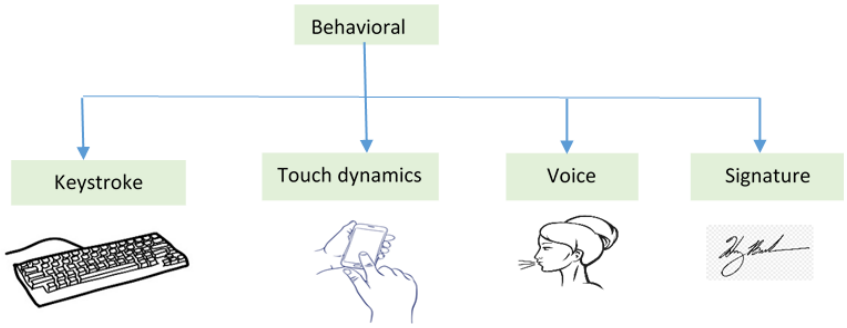

Figure 1. Behavioral biometrics

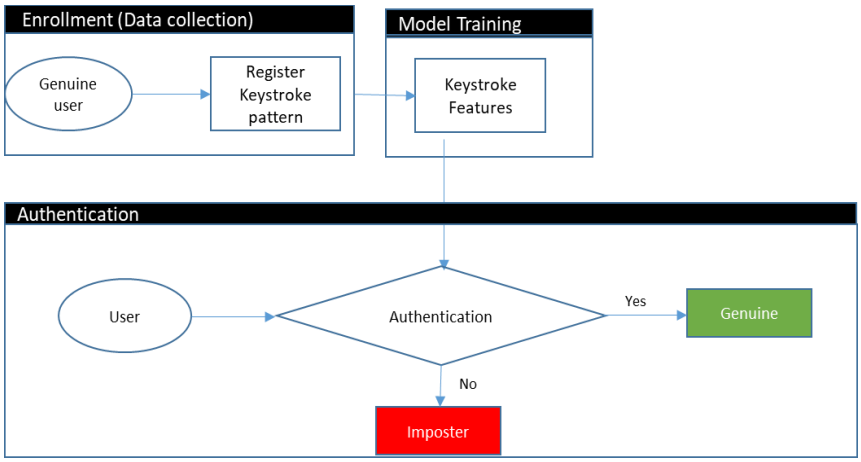

Figure 2. Basic steps for the authentication process

2.1. Enrollment (data collection)

In proposed work, a total of 25 users aged between 22 to 42 years, have participated in the experiment. In order to capture the keystroke data input from the users, we have developed mobile application on Samsung On7 Pro C3590. In our experiments, 4-digit password "1976" was used and users were asked to enter the password 60-times during enrollment phase at Samsung India Noida R&D center, where one of the author is working. The data collection was done in two separate sessions for each user. Entire enrollment process took one week to collect the sample data from all the users. The keystroke data acquisition step comprises of building a character transition lists for particular chosen keyword. The duration of key-presses between every two characters are stored. This proposed work was designed to classify the users in feature phone based on the typing patterns while entering the 4-digit personal identification number (PIN) key, which is based on the hold-time of key press, flight time and the total time entering the PIN. Our work utilizes the following mentioned parameters while capturing the data from the user: i) keystroke latency (flight time): time taken between two consecutive keystrokes, ii) hold-time: time to press and release a key, and iii) total time: time to press first key press and last key release. The components of features that are utilized in this work are shown in Figure 3.

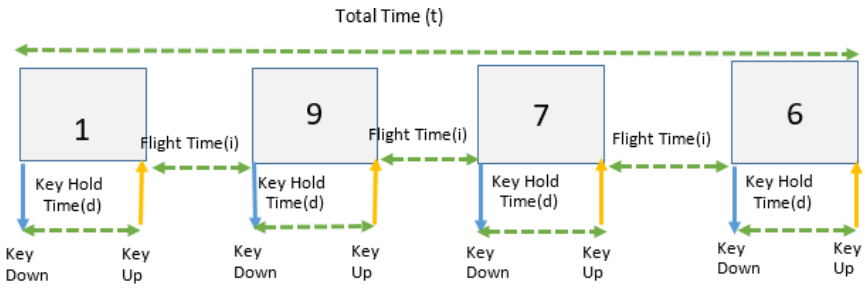

Figure 3. Keystroke dynamics features

The input captured during enrolment is in the following format for the keyword "1976" with 8 features [i_1, i_2, i_3, d_1, d_2, d_3, d_4, t]. Where:
d_k : Time of press for key (hold time in milliseconds)
i_k : Time between first key release and next key press (flight time in milliseconds)
t : Total time from first key press to last key release (in milliseconds)

2.2. Model training

In proposed work, with the help of data collected during enrollment phase typing pattern for a particular password is recorded and then model is trained with k-NN and fuzzy logic. Overall, 8 features are collected as shown in Figure 3 including hold time, flight time and total time from first key to last key release for the keyword "1976". The input features obtained are then passed through the k-NN model and the fuzzy training model separately and both the models are then trained using the given input features. The authentication values are obtained separately from both the models and final authentication value is returned as shown in Figure 4.

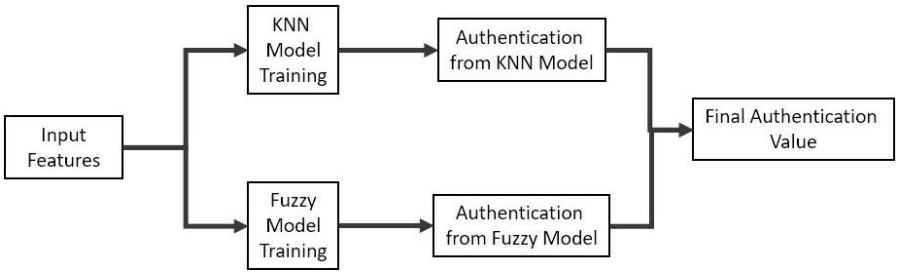

Figure 4. Proposed keystroke model architecture based on k-NN and fuzzy

2.2.1. K-NN model

We have used k-nearest neighbor (k-NN) as a classification method because of its key application in pattern recognition and prediction. k-NN uses the k nearest neighbors of the feature value, in our case we use 5-NN to search five nearest neighbors of user's typing patterns. In this algorithm, we make use of Euclidean distance to know the distance between the claimed user typing pattern and the actual user features.

Euclidean distance provides the direct distance between two points in space along the line joining the two points. It helps to find the shortest distance between two input feature vectors along the line segment joining the two input vectors. The Euclidean distance is calculated for all the points and then nearest points having the smallest distance are considered. Here is pictorial representation as shown in Figure 5 of how Euclidean distance is used in k-NN.

$$d(z,z') = \sqrt{(z_1 - z'_1)^2 + (z_2 - z'_2)^2 + \cdots + (z_n - z'_n)^2} \quad (1)$$

Where:
Z : Training sample value
z` : Test sample value
d(z,z`) : Computes the Euclidean distance

In nearest neighbor model, the number of characters in keyword decide the number of dimensions in a hyper dimensional space. Each set of typing pattern of that keyword among multiple iterations is one point in that hyper dimensional space. Since we have collected multiple inputs to train the model, we have multiple clouded points plotted for a particular keyword once the classifier training is complete as shown in Figure 6. In the proposed work we have hold time, flight time and total time as feature set which is captured from user and model is trained for the 4-digit keyword "1976". Refer Figure 7 shows the model is trained with data set which is comprised of training samples and genuine or accepted and the sample cases which are imposter.

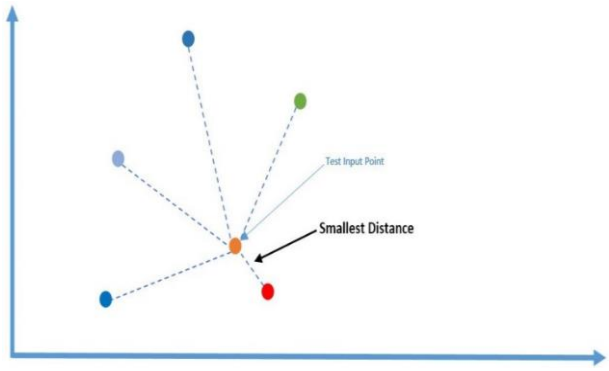

Figure 5. k-NN using Euclidean distance

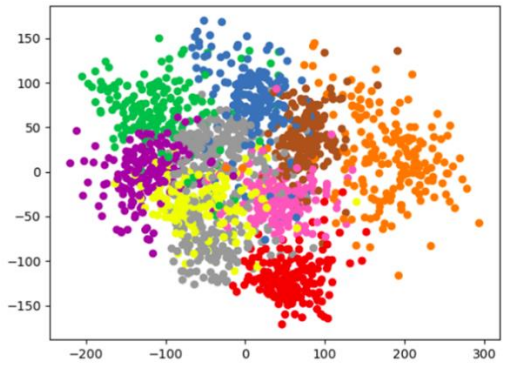

Figure 6. Plot of user data captured keystroke inputs

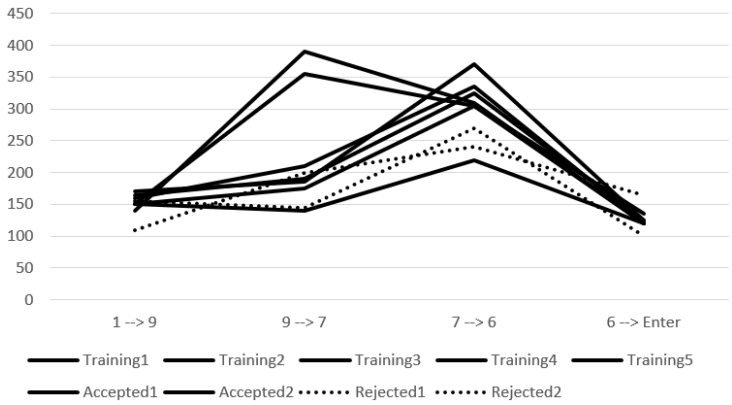

Figure 7. Plot of training data set of a user and the accepted and the rejected data

2.2.2. Fuzzy logic

Fuzzy means something that is not clearly defined or has crisp values. Fuzzy logic is used in the cases where a crisp definition cannot be provided for a quantity, such as the amount of hot or cold. In our case, a user when typing can have variable typing speeds, classified as fast, slow or normal. A crisp definition of the quantity where the value changes from fast to normal to slow cannot be defined in this case. Figure 8 shows frequency of typing speed timings graphically for a typical user, the normal typing speed has maximum frequency which occurs in day-to-day life while typing, while the frequency decreases as moving towards timings that are categorized as fast or slow. The actual values of timing will vary from person to person and a crisp range cannot be defined between the three values. Such values introduce a degree of fuzziness and using methods such as k-NN fail to classify two users with overlapping typing speed. Such fuzziness is solved by using the concepts of fuzzy logic. Fuzzy logic is used in authentication systems based on biometrics to provide enhanced security as in case of biometrics a lot of data from different users can be overlapping. In case of keystroke dynamics-based authentication system, the input features are keystroke timings which can have varying values for a single user which may or may not overlap with another user timings.

From Figure 8 we can see that it is not possible to define a single value as fast or slow typing speed for a given user. As explained in Figure 9 in the fuzzy logic model, inference engine which is responsible for

determining the output for a given input based on learned data, uses the input features of the keystroke timings which are first converted to the fuzzified input. Using the input keystroke timings, the rule base is generated which will be used to determine the timing similarities for a test input. Similarity gives a degree of closeness between one typing speed timing against the timings from learned users and is calculated by fuzzifying the test input first and based on the similarity values fuzzy output values are calculated. Finally, the fuzzy output can be converted to the crisp Authentication value using the available defuzzification functions such as centroid method, or normal max value, based on the current membership value, and center of sums.

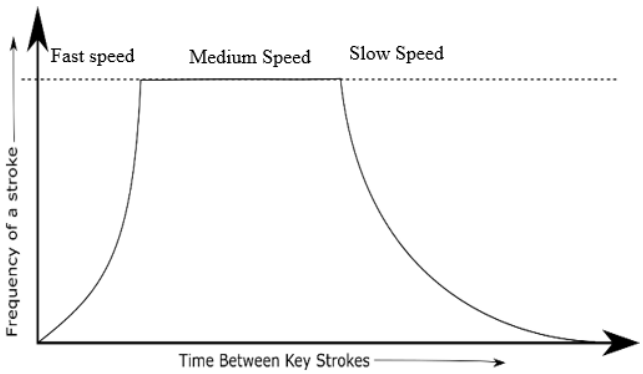

Figure 8. Timings between keystrokes of a participant

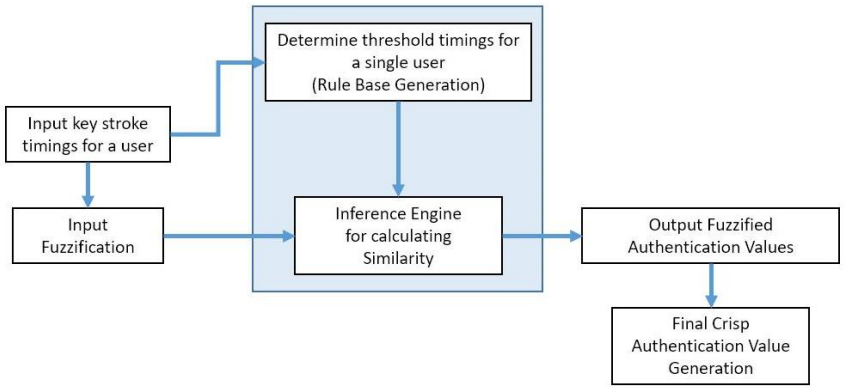

Figure 9. Working of the proposed fuzzy logic model for keystroke dynamics

A. Determining rule base for user classification

The input to the fuzzy system is the key stroke timings from a user collected over time or may be a test input typing pattern that needs to be authenticated yet, these inputs need to be converted to the fuzzy inputs before they are passed through the inference Engine for further processing, for both learning and test phase.

Following timings are taken into account when calculating the fuzzy membership input: i) time of press for key (hold time: d_k); ii) time between first key release and next key press (flight time: i_k); iii) total time from first key press to last key release (t).

The input is in the following format for the 4-character keyword "1976" with 8 features [i_1, i_2, i_3, d_1, d_2, d_3, d_4, t]. Note that this feature set is particular to 4-character keywords only and will change with the number of characters used for learning. Here, i_1, i_2, i_3 represent, Interval between releasing key and stroking next key (Milliseconds). Similarly, d_1, d_2, d_3, d_4 values represent Time period key during key remain pressed. Finally, last value represents, Time period first key press and last key release (Milliseconds)

Multiple feature set will be obtained for a given user during the learning phase. The values averaged to obtain an average typing time for a single user for all the three types of timings. We get the following 3 values for each input tuple for a single user.

$$(d, i, t) = (\sum_{k=1}^{4} d_k, \sum_{k=1}^{3} i_k, t) \quad (2)$$

To train the user,

$$d_{avg} = \frac{\sum_{k=0}^{n} d_k}{n} \quad (3)$$

$$i_{avg} = \frac{\sum_{k=0}^{n} i_k}{n} \quad (4)$$

$$t_{avg} = \frac{\sum_{k=0}^{n} t_k}{n} \quad (5)$$

where, n: total number of input timing feature set for a single user obtained while training.

Finally, we calculate an upper and lower limit of the typing speeds that can be used as rough estimate of the typing timing of a single user in day-to-day life. Threshold t_l and t_u are defined for each three inputs which give a rough estimate of minimum and maximum value of timing for a single user and is calculated as the mth standard deviation from the average value. This methodology helps to circumvent any outliers that may have occurred during data collection:

For d:

$$t_{ld} = d_{avg} - m * \sigma(d) \quad (6)$$

$$t_{ud} = d_{avg} + m * \sigma(d) \quad (7)$$

For i:

$$t_{li} = i_{avg} - m * \sigma(i) \quad (8)$$

$$t_{ui} = i_{avg} + m * \sigma(i) \quad (9)$$

For t:

$$t_{lt} = t_{avg} - m * \sigma(t) \quad (10)$$

$$t_{ut} = t_{avg} + m * \sigma(t) \quad (11)$$

where, generally, m is 3, but for our purpose we have taken value of m to be 1 as using 3 can sometimes allow outliers to be falsely accepted and in case of typing it is possible that multiple users may have very overlapping timings and may lead to false acceptance. Here, $m * \sigma(d)$ defines m^{th} standard deviation around the average value. t_{lk} and t_{uk} represents the lower and upper learned threshold timings for the user, where k is d, i, t. Finally, these values of threshold will be used during the input fuzzification phase to generate input membership function for a user input.

B. Input fuzzification

The obtained threshold values in the previous step are then used to generate an input membership function. The input membership function is defined as:

$$\mu_k = \begin{cases} \frac{0}{negative} + \frac{1}{normal} + \frac{0}{positive}, if\ t_{lk} \leq\ t_k \leq t_{uk} \\ \frac{\left(1-\frac{1}{|t_k - t_{lk}|}\right)}{negative} + \frac{\frac{1}{|t_k\ - t_{lk}|}}{normal} + \frac{0}{positive},\ if\ t_k < t_{lk} \\ \frac{0}{negative} + \frac{\frac{1}{|t_k - t_{uk}|}}{normal} + \frac{1-\frac{1}{|t_k - t_{uk}|}}{positive},\ if\ t_k > t_{uk} \end{cases} \quad (12)$$

where, k= d, i and t, respectively and the membership function is calculated for d, i and t respectively. The membership function calculations are partitioned based on the thresholds. The membership function will have degree 1 for normal when the timings are between upper and lower threshold value and zero for positive and negative. Similarly for cases when the timing is less than or greater than the threshold the degree of membership is calculated as shown in (12).

So, now we have three values defined for each timing. The membership graph for input is presented in Figure 10. The graph timings have been modified to allow for a range of user timings because a single user may have a varying range of timing from a general average. All the three keystroke timings will have a similar membership function.

For any incoming test input [t_{i1}, t_{i2}, t_{i3}, t_{d1}, t_{d2}, t_{d3}, t_{d4}, t_t], (d, i, t) is calculated as shown previously in (2). The membership values are calculated for three values d, i, t, using the membership function as mentioned in (12). For an incoming test input, we obtain three membership functions μ_d, μ_i, μ_t.

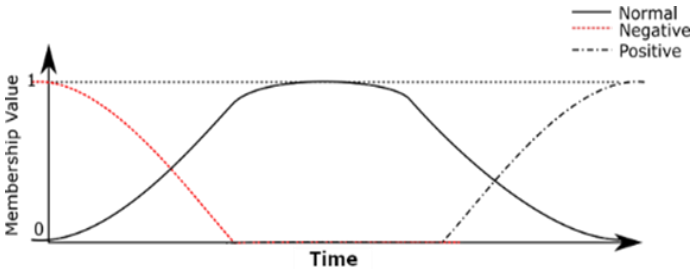

Figure 10. Fuzzy membership function for the input timings based on authenticated user input.

C. Calculating similarity for a test input using inference engine

After converting the input to fuzzified values the inference engine uses the rule base to determine the similarity for the input to the learned user timings. Based on the closeness of the features to the limits of the authentication values, similarity function can be defined as mentioned in (13), (14):

$$s = \left(\frac{(\Sigma(\mu_k))}{3}\right) \tag{13}$$

$$s_{norm} = (s/||s||)/\, normal \tag{14}$$

where,

μ_k : input membership function with k = d, i, t
normal : means that membership value of the normal is considered only for similarity.
S : represents the similarity, 0 <= s <=1.
s_{norm} : represents the normalized values

Here, summation is done separately for negative, normal and positive member values defined in the input membership function.

D. Obtaining output membership function

Finally, after applying keystroke dynamics timings and calculating the score the inference engine will calculate the possible authentication value based on the current learned preferences and based on a threshold of similarity 's_l', 's_u' the authentication values is generated. Where, s_l is the lower limit and s_u is the upper limit for similarity thresholds. A similarity value below 0.9 times s_l of means no authentication, while if similarity is greater than 1.1 times of s_u the user is fully authenticated. Using a range instead of strict values of s_l and s_u helps to achieve the desired fuzziness by removing any strict crispiness in the threshold values. For in-between values of similarity, authentication values are defined using the output membership function as shown in (15). Values for the s_l and s_u can be set based on the learning from the previous data. Typical values for s_l are 0.3-0.5 and for s_u are 0.6-0.8. Similar, to the input function an output function can be defined as shown in (15):

$$\mu_{op} = \begin{cases} \frac{0}{NoAuth} + \frac{1}{\partial Auth} + \frac{0}{FullAuth}, if(1.1 * s_l) < s \leq (0.9 * s_u) \\ \frac{1}{NoAuth} + \frac{0}{\partial Auth} + \frac{0}{FullAuth}, if s < s_l \\ \frac{0}{NoAuth} + \frac{0}{\partial Auth} + \frac{1}{FullAuth}, if s > s_u \\ \frac{\frac{s-s_l}{0.1*sl}}{NoAuth} + \frac{1-\frac{s-s_l}{0.1s_l}}{\partial Auth} + \frac{0}{FullAuth}, if s_l \leq s \leq 1.1s_u \\ \frac{0}{NoAuth} + \frac{1-\frac{s_u-s}{0.1s_u}}{\partial Auth} + \frac{\frac{s_u-s}{0.1*s_u}}{FullAuth}, if 0.9s_u \leq s \leq s_u \end{cases} \tag{15}$$

Based on the similarity value s, membership function for the output $\mu_{op,}$ is calculated as shown in (15). The graph for the output membership function is shown in Figure 11. Three values have been defined for authentication membership function: i) no authentication, ii) partial/strict authentication, and iii) full authentication.

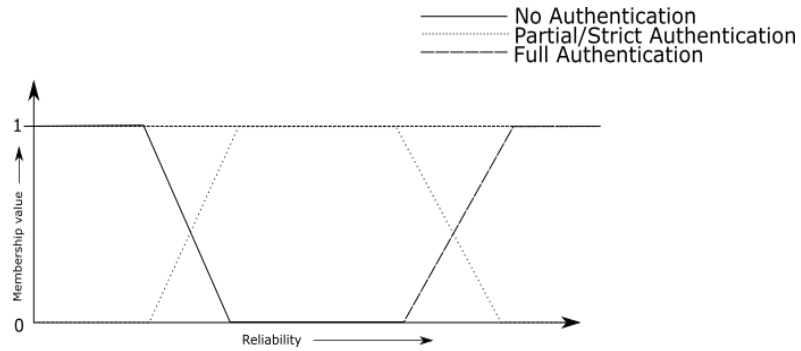

Figure 11. Output fuzzy function obtained from keystroke input after applying inferences

Instead of using crisp similarity thresholds for s_l and s_u the authentication membership values are generated by varying over a range which helps to achieve the desired fuzziness in the output membership function as shown in the Figure 10. The partial authentication decreases as the reliability/similarity increases while at the same time partial authentication membership increases, similar is the case of partial and full authentication the membership values change gradually over a range of similarity values.

E. Final crisp authentication value generation

From this approach, finally the output can be converted into de-fuzzified output by taking the max of the three outputs as defined in (16):

$$\text{Output} = \max(a, b, c) \quad (16)$$

where,
a : membership value for no auth
b : membership value for partial auth
c : membership value for full auth

2.3. Authentication

The final step post model training, is of authentication. Both the trained classifiers separately generate the authentication results which are then combined together generate the final authentication value. For k-NN the trained classifier is used to calculate the nearest distance of the test sample from all of the training samples in that hyper dimensional space. Once the nearest distance of the testing sample is calculated, it is checked with the permissible threshold value for that keyword and if the value is outside the limits of threshold, the test sample is marked as unrecognized typing pattern and the user is classified as imposter. When by recursive intruding the imposter matches the value within the permissible threshold, the imposter is falsely allowed the access. The permissible threshold solely depends on the duration between typing each consecutive letter. For the imposter to match the values in permissible threshold all these parameters should match the parameters that of the actual user.

For fuzzy model the similarity is calculated for user and output authentication values is generated for the user. The user is considered to be authenticated if the authentication value is obtained as full authentication. A value of no or partial authentication is considered as no authentication in this case. Figure 12 shows basic flow chart when unknown user tries to access mobile app or log in to the device, even when he knows the user password the proposed system checks the behavioural characteristics of user input pattern on keystroke and dis-allows access to the imposters. This way it provided the second level of security to the user in feature phone. There are basically two phases in the authentication system-enrolment and login phase. In the enrolment phase the user keystroke dynamics are learned by the classifier.

When setting a 4-digit PIN the timings for the user are captured feature vector is created with it. This Feature vector is then passed through the k-NN classifier for training. The fuzzy classifier also learns threshold

values for the lower and upper typing timings for the user. During the login phase when a test user actually enters the similar timing feature vector are obtained and passed through the learned classifier to obtain the k-NN authentication output. Similarly, the input is converted to a fuzzified input and then using the fuzzy inference converted to fuzzified output to finally obtain the crisp output result.

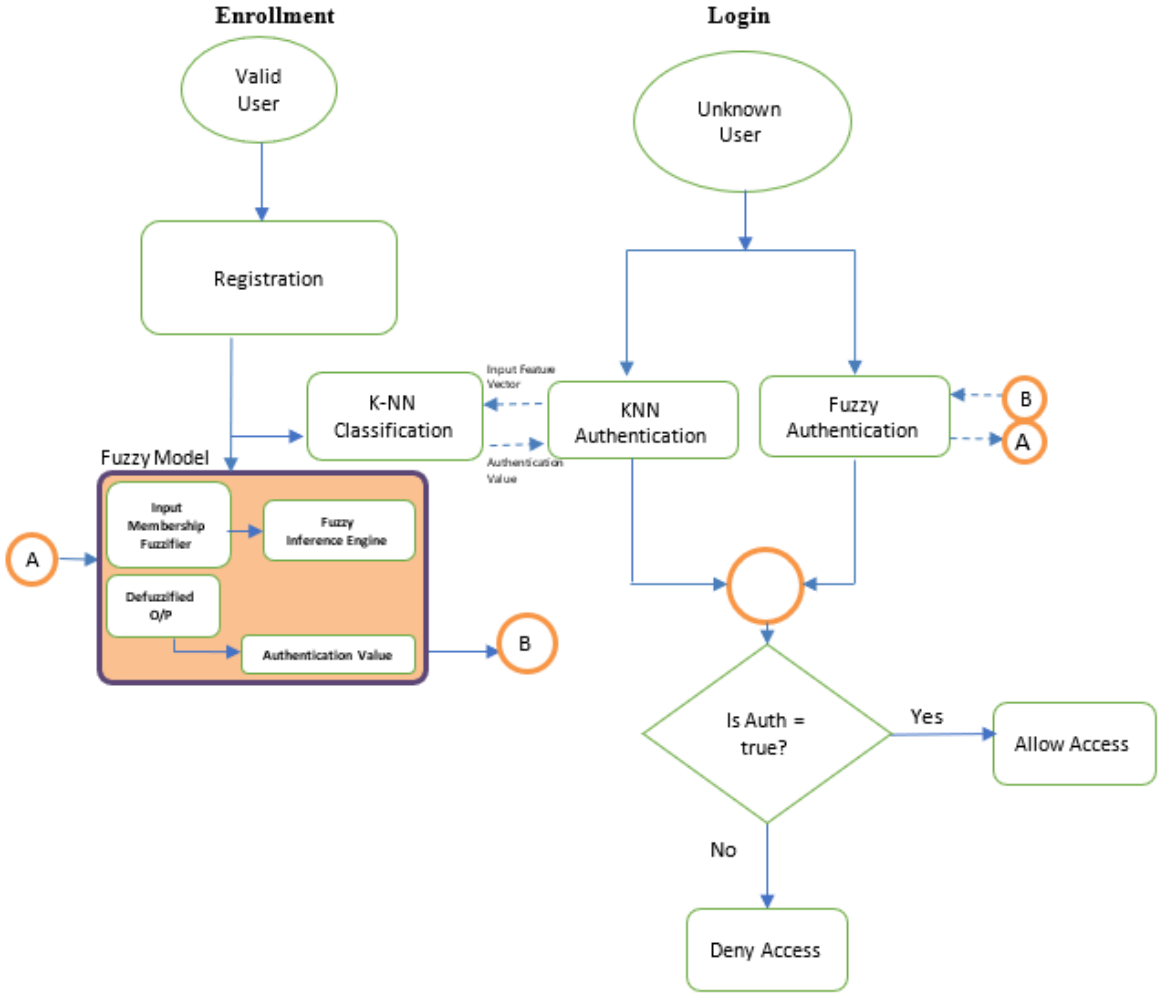

Figure 12. Basic flow diagram of proposed keystroke dynamics

3. RESULTS AND DISCUSSION

The accuracy of the keystroke dynamics system is measured on the following counts:

a) False rejection rate (FRR) is the measure of the percentage ratio between incorrectly reject authorized users against the total number of genuine users accessing the system. A lower false rejection rate means less reject cases and easier access by legitimate user.
b) False acceptance rate or FAR is measure of the percentage ratio between falsely accepted unauthorized users against the total number of imposters accessing the system. Terms such as false match rate (FMR) or type 2 error refers to the same meaning. A smaller FAR indicates less imposter accepted.
c) Equal error rate (EER) is used to determine the biometric system accuracy. When both FAR and FRR rates are equal that intersection point is EER. The lower the value of EER the higher the precision of the biometric system.

Based on an experiment conducted to find accuracy of keystroke analysis, FAR i.e. rate of system giving access to an imposter. Experiment has been performed for 25 different users for different acceptance threshold FRR i.e. rate of system denying access to authorized user has been taken for 25 different users for different acceptance threshold. To conduct this experiment fluently, the authorized user took 4-digit PIN as input. Now, to know the EER value, we plotted the graph between FAR and FRR value. The intersection point of this graph so plotted gives us the EER value as shown in Figure 13. More precisely the closest match of

FRR and FAR value is the EER. Table 1 represents a comparative evaluation of accuracy parameters performed between our proposed k-NN model and the improved version of our model when fuzzy logic is added alongside k-NN classifier to find the final authentication value.

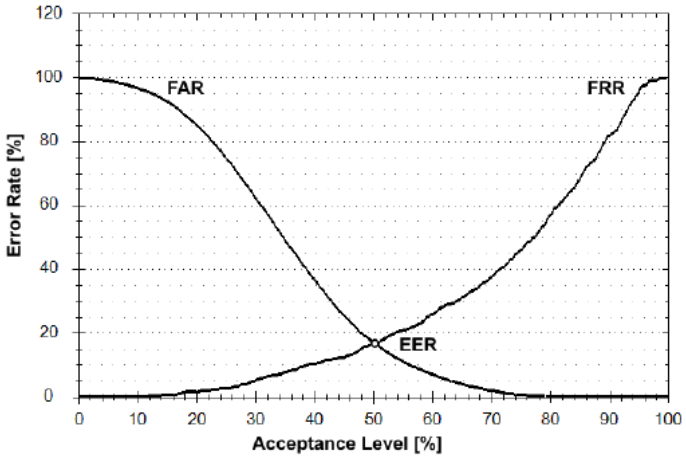

Figure 13. Relation between FAR and FRR

Table 1. A Comparison between simulations of different techniques

User	Age	Gender	k-NN			k-NN with Fuzzy		
			FAR	FRR	EER	FAR	FRR	EER
User1	27	Male	0.015	0.014	1.45%	0.017	0.015	1.6%
User2	32	Male	0.023	0.05	3.65%	0.012	0.017	1.45%
User3	27	Female	0.092	0.093	9.25%	0.013	0.017	1.5%
User4	24	Female	0.031	0.014	2.25%	0.021	0.018	1.95%
User5	28	Female	0.092	0.093	9.25%	0.01	0.011	1.05%
User6	31	Male	0.023	0.021	2.20%	0.015	0.015	1.5%
User7	42	Male	0.031	0.029	3.00%	0.013	0.015	1.39%
User8	25	Male	0.008	0.021	1.45%	0.01	0.010	1.00%
User9	29	Male	0.062	0.043	5.25%	0.010	0.019	1.44%
User10	22	Male	0.054	0.064	5.90%	0.012	0.015	1.35%
User11	22	Female	0.026	0.032	2.9%	0.020	0.019	1.95%
User12	23	Female	0.014	0.029	2.1%	0.010	0.012	1.1%
User13	24	Female	0.026	0.005	1.6%	0.010	0.014	1.20%
User14	25	Male	0.043	0.008	2.6%	0.018	0.020	1.90%
User15	22	Male	0.005	0.02	1.46%	0.009	0.013	1.1%
User16	23	Female	0.02	0.023	2.19%	0.012	0.020	1.6%
User17	24	Female	0.023	0.017	2.0%	0.027	0.012	1.95%
User18	23	Male	0.020	0.026	2.3%	0.020	0.020	2.0%
User19	22	Male	0.011	0.029	2.04%	0.057	0.027	4.2%
User20	23	Female	0.014	0.002	0.8%	0.034	0.035	3.45%
User21	22	Male	0.035	0.023	2.9%	0.037	0.033	3.5%
User22	22	Male	0.026	0.002	1.4%	0.021	0.025	2.3%
User23	27	Female	0.017	0.017	1.75%	0.01	0.020	1.5%
User24	25	Male	0.043	0.017	3.0%	0.025	0.03	2.75%
User25	27	Male	0.038	0.023	3.0%	0.022	0.025	2.35%

In this performance evaluation, we have found out that using only the k-NN model over the biometric input features had a limitation in that the model does not take into account the variance in the keystroke latencies among the multiple attempts of the single user. From the results, we can observe that k-NN model the average EER 3.03% and this is the best result we found with our experiments when the value of k was set to 5. We can observe that the EER has shown improvement and it's decreased from 3.03% to 1.88% when fuzzy was applied with k-NN. Out of 25 users we have observed that 12 users the EER results were less than 1.5%. Best results were observed for user5 (female) with EER 1.05% with k-NN and fuzzy combined model. In Figures 14, 15 and 16 we have analyzed the FAR, FRR and ERR for 25 users with k-NN, k-NN with fuzzy methods. It can be observed from our experiments that k-NN and fuzzy model when combined have performed better for most of users and its results are superior from k-NN.

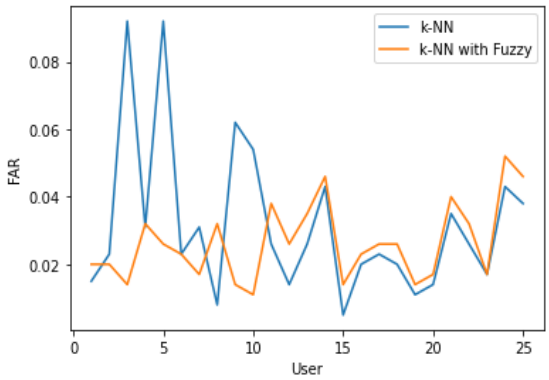

Figure 14. FAR with k-NN, k-NN with fuzzy for 25 different users

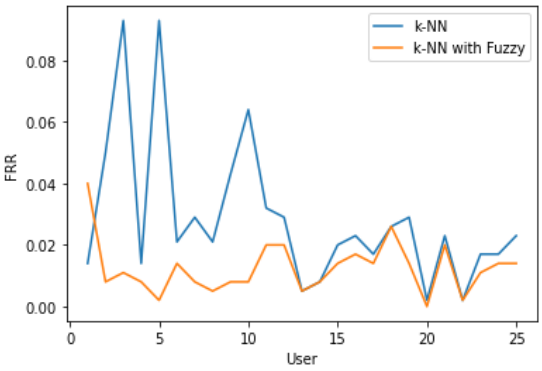

Figure 15. FRR with k-NN, k-NN with fuzzy for 25 different users

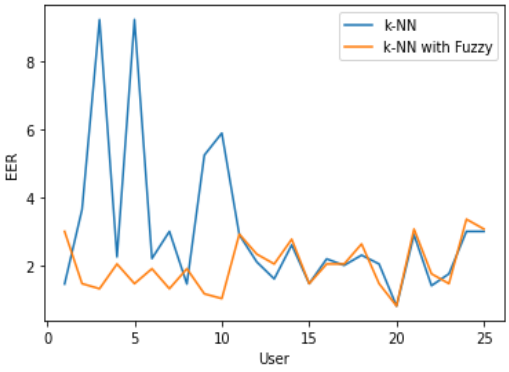

Figure 16. EER with k-NN, k-NN with fuzzy for 25 different users

In Table 2 we have shared the comparison of the proposed work with existing work in keystroke dynamics from other researches is covered. In the proposed work, we have considered 60 patterns from each user and 25-users participated in experiments. Our study is competitive as its network trained with combination of k-NN with fuzzy method with EER rate of 1.88% when experiments were performed with 25 participants on feature phone Samsung on 7 Pro at Samsung India labs.

Table 2. Comparison with existing work

Study	Input Data	# Of Participants	# of Inputs Training	Classifier	EER (%)
Clarke and Furnell [12]	4-digit PIN	32	30	Neural networks	12.8%
Hwang *et al*. [13]	4-digit PIN	10	5	Artificial rhythm with Cues	4% to 13%
Wang *et al*. [19]	4-digit PIN	104	20	Support vector machine (SVM)	8.70%
Chang *et al* [20]	200 words	114	3	Statistical classifier	7.89%
Mondal *et al* [21]	All keys of keyboard	53	$7*10^5$	ANN and CPANN	2.35%
Lee *et al*. [22]	6-digit PIN	22	100	Manhattan and Euclidean Distance	7.89%
Kim *et al*. [23]	6-digit PIN	6	100	Statistical classifier	13.44%
Frolova *et al*. [24]	alphanumeric	15	30	LOF, Manhattan and Euclidean ensemble	8.00%
Proposed Work	4-digit PIN	25	60	k-NN	3.07%
Proposed Work	4-digit PIN	25	60	k-NN with fuzzy	1.88%

In the litreture, there are many research works done for keystroke dynamics [25]-[36] from last three deacdes, however with the proposed keystroke dynmaics study for feature phones we have proposed k-NN classifier with fuzzy logic model to provide enhanced security when data from different users can be overlapping.

4. CONCLUSION AND FUTURE WORK

Behavior biometrics is the future of security domain, and using the keystroke modality can be a simplest way to achieve this efficiently and precisely. With the developed study the accuracy of EER 1.88% is achieved by training model with 60 samples with 25 users. With proposed study the accuracy rate is increased as we used combination of k-NN with fuzzy to improve the results with sufficient samples to train the model. Building multiple models for different keywords that are frequent in usage can help us to monitor the user while typing in a generic scenario of chatting platform and suspicious operation over the handheld device can be tracked and prevented. To increase the scope of this security, other modalities such as touch analytics, battery charging patterns and walking patterns of an individual can be explored as future research work for mobile phone security under behavioral biometric research scope. For future work we intend to increase the concept with smartphone devices and there we would like to develop multimodal framework based on keystroke dynamics and user swipe pattern to recognize the user. This can further be connected using cloud support to deploy the keystroke machine learning models with better internet connection which help to improve the security further by processing the data on the web servers and keeping client devices light and handy.

ACKNOWLEDGEMENTS

The authors would like to thanks Samsung Research Institute, Noida to conduct this research in their labs and providing the required development environment.

REFERENCES

[1] "The Mobile Economy." GSMA.com. https://www.gsma.com/mobileeconomy (accessed Mar. 2, 2021).
[2] C. Jarret and O. Shalofsky. "Apple products too a-peeling for thieves." Directlinegroup.co.uk. https://www.directlinegroup.co.uk/en/news/brand-news/2017/apple-products-too-a-peeling-for-thieves.html (accessed Mar. 15, 2021).
[3] L. Aron and P. Hanacek, "Overview of security of the mobile devices," *2015 2nd World Symposium on Web Applications and Networking (WSWAN)*, 2015, pp. 1-11, doi: 10.1109/WSWAN.2015.7210319.
[4] A. Lacerda, R. de Queiroz, and M. Barbosa, "A systematic mapping on security threats in mobile devices," *2015 Internet Technologies and Applications (ITA)*, 2015, pp. 286-291, doi: 10.1109/ITechA.2015.7317411.
[5] M. E. Fathy, V. M. Patel, and R. Chellappa, "Face-based active authentication on mobile devices," *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2015, pp. 1687-1691, doi: 10.1109/ICASSP.2015.7178258.
[6] Q. Tao and R. Veldhuis, "Biometric authentication system on mobile personal devices," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 4, pp. 763-773, 2010, doi: 10.1109/TIM.2009.2037873.
[7] L. Zhang, G. Zhang, and L. Zhang, "an overview of mobile devices security issues and countermeasures," *2014 International Conference on Wireless Communication and Sensor Network*, 2014, pp. 439-443, doi: 10.1109/WCSN.2014.95.
[8] V. Mishra, "More than a billion feature phones to be sold over next three years." Counterpointresearch.com. https://www.counterpointresearch.com/more-than-a-billion-feature-phones-to-be-sold-over-next-three-years (accessed Mar. 10, 2021).
[9] H. A. Shabeer and P. Suganthi, "Mobile phones security using biometrics," *International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007)*, 2007, pp. 270-274, doi: 10.1109/ICCIMA.2007.182.
[10] M. N. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 446-471, 2013, doi: 10.1109/SURV.2012.013012.00028.
[11] A. K. Jain and K. Nandakumar, "Biometric authentication: system security and user privacy," *Computer*, vol. 45, no. 11, pp. 87-92, 2012, doi: 10.1109/MC.2012.364.
[12] N. L. Clarke and S. Furnell, "Authenticating mobile phone users using keystroke analysis," *International Journal of Information Security*, vol. 6, pp. 1-14, 2007, doi: 10.1007/s10207-006-0006-6.
[13] S. Hwang *et al.*, "Keystroke dynamics-based authentication for mobile devices," *Computers & Security*, vol. 28, no. 1, pp. 85-93, 2009.
[14] A. Motwani, R. Jain, and J. Sondhi, "A multimodal behavioral biometric technique for user identification using mouse and keystroke dynamics," *International Journal of Computer Applications*, vol. 111, no. 8, pp. 15-20, 2015, doi: 10.5120/19558-1307.
[15] V. D. Stanciu, R. Spolaor, M. Conti, and C. Giuffrida, "On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks," *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, 2016, pp. 105-112, doi: 10.1145/2857705.2857748.
[16] X. Huang, G. Lund, and A. Sapeluk, "Development of a typing behavior recognition mechanism on android," *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 2012, pp. 1342-1347, doi: 10.1109/TrustCom.2012.127.
[17] R. Yampolskiy and G. Venu, "Behavioral Biometrics: A survey and classification," *International Journal of Biometrics*, vol. 1, no. 1, pp. 81-113, 2008, doi: 10.1504/IJBM.2008.018665.
[18] A. A. El Masri., "Active authentication using behavioral biometrics and machine learning," George Mason University, Thesis, 2016.
[19] Y. Wang, C. Wu, K. Zheng, and X. Wang, "Improving reliability: User authentication on smartphones using keystroke biometrics," *IEEE Access*, vol. 7, pp. 26218-26228, 2019, doi: 10.1109/ACCESS.2019.2891603.
[20] T.-Y. Chang, C.-J. Tsai, J.-Y. Yeh, C.-C. Peng and P.-H. Chen, "New soft biometrics for limited resource in keystroke dynamics authentication," *Multimedia Tools and Applications volume*, vol. 79, pp. 23295-23324, 2020, doi: 10.1007/s11042-020-09042-x.
[21] S. Mondal and P. Bours, "A study on continuous authentication using a combination of keystroke and mouse biometrics," *Neurocomputing*, vol. 230, pp. 1-22, 2017, doi: 10.1016/j.neucom.2016.11.031.
[22] H. Lee, J. Y. Hwang, D. I. Kim, S. Lee, S.-H. Lee, and J. S Shin, "Understanding keystroke dynamics for smartphone users authentication and keystroke dynamics on smartphones built-in motion sensors," *Security and Communication Networks*, vol. 2018, pp. 1-10, 2018, Art. no. 2567463, doi: 10.1155/2018/2567463.

[23] D. I. Kim, S. Lee, and J. S. Shin, "A new feature scoring method in keystroke dynamics-based user authentications," *IEEE Access*, vol. 8, pp. 27901-27914, 2020, doi: 10.1109/ACCESS.2020.2968918.
[24] D. Frolova, A. Epishkina, and K. Kogos, "Mobile user authentication using keystroke dynamics," *2019 European Intelligence and Security Informatics Conference (EISIC)*, 2019, pp. 140-140, doi: 10.1109/EISIC49498.2019.9108890.
[25] D. Stefan, S. Xun, and D. Yao, "Robustness of keystroke-dynamics based biometrics against synthetic forgeries," *Computers and Security*, vol. 31, no. 1, pp. 109-121, 2012, doi: 0.1016/j.cose.2011.10.001.
[26] C. Giurida *et al*., "I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics," *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, vol. 8550, 2014, pp. 91-111, doi: 10.1007/978-3-319-08509-8_6.
[27] C.-J. Tasia, T.-Y. Chang, P.-C. Cheng, and J.-H. Lin, "Two novel biometric features in keystroke dynamics authentication systems for touch screen devices," *Security and Communication Networks*, vol. 7, no. 4, pp. 750-758, 2014, doi: 10.1002/sec.776.
[28] R. Napier, W. Laverty, D. Mahar, R. Henderson, M. Hiron, and M. Wagner, "Keyboard user verification: toward an accurate, efficient and ecologically valid algorithm," *International Journal of Human-Computer Studies*, vol. 43, no. 2, pp. 213-222, 1995, doi: 10.1006/ijhc.1995.1041.
[29] S. Cho, C. Han, C. Han, D. Hee, and H.-Il Kim, "Web based keystroke dynamics identity verification using neural networks," *Journal of Organizational Computing and Electronic Commerce*, vol. 10, no. 4, pp. 295-307, 2000, doi: 10.1207/S15327744JOCE1004_07.
[30] R. Giot, M. El-Abed, and C. Rosenberger, "Keystroke dynamics authentication for collaborative systems," *2009 International Symposium on Collaborative Technologies and Systems*, 2009, pp. 172-179, doi: 10.1109/CTS.2009.5067478.
[31] Y. Zhong, Y. Deng, and A. K. Jain, "Keystroke dynamics for user authentication," *2012 IEEE computer society conference on computer vision and pattern recognition workshops*, 2012, pp. 117-123, doi: 10.1109/CVPRW.2012.6239225.
[32] C. Jadhav, S. Kulkami, S. Shelar, K. Shinde, and N. V. Dharwadkar, "Biometric authentication using keystroke dynamics," *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, 2017, pp. 870-875, doi: 10.1109/I-SMAC.2017.8058304.
[33] K. Tse and K. Hung, "User behavioral biometrics identification on mobile platform using multimodal fusion of keystroke and swipe dynamics and recurrent neural network," *2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, 2020, pp. 262-267, doi: 10.1109/ISCAIE47305.2020.9108839.
[34] H. Gascon, S. Uellenbeck, C. Wolf, and K. Rieck "Continuous authentication on mobile devices by analysis of typing motion behaviour," *Sicherheit 2014-Sicherheit, Schutz und Zuverlässigkeit*, 2014.
[35] J. Kim, H. Kim, and P. Kang, "Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection," *Applied Soft Computing*, vol. 62, pp. 1077-1087, 2018, doi: 10.1016/j.asoc.2017.09.045.
[36] I. Lamiche, G. Bin, Y. Jing, Z. Yu, and A. Hadid, "A continuous smartphone authentication method based on gait patterns and keystroke dynamics," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 11, pp. 4417-4430, 2019, doi: 10.1007/s12652-018-1123-6.

BIOGRAPHIES OF AUTHORS

Amitabh Thapliyal received his Master's Computer Application from Jamia Hamdard, the Bachelor of Science with Physics Hons from Delhi University. Currently, he is working with Samsung Research Institute, Noida, India as Director R&D Mobile division. He has more than 2 decades of industry experience in the field of ICT. He is pursuing his PhD. Computer Engineering from Delhi Technological University, Delhi, India in the field of biometric authentication for mobile devices. He published more than 10 patents in the field of mobile technology while working for several research and innovation projects for Samsung R&D. His areas of interests include pattern recognition with emphasis on the behavioral pattern understanding on Mobile devices. He can be contacted at email: amitabh.thapliyal@gmail.com.

Om Prakash Verma received his PhD degree in Image processing from Delhi University, the MTech degree from Indian Institute of Technology, Delhi. He has vast research and academia experience of more than 28 years. He is presently working as Professor in Department of Computer Science and Engineering, Delhi Technological University, Delhi, India. His academics and research interests are image processing, soft computing, machine learning and evolutionary computing. He published more than 67 research papers in both conferences and journals. He can be contacted at email: opverma.dce@gmail.com.

Amioy Kumar received his PhD from Indian Institute of Technology, Delhi in 2013. His areas of expertise include Artificial Intelligence, Machine Learning, Biometrics, Pattern recognition and Image Processing. Currently, he is working with Intel Corp. Bangalore, India as Technical Lead and Solution Architect. He is leading advanced research and innovation activities at Client Computing Group. His expertise is to provide the cutting edge solutions to the diverse problems of Intel customers by employing the most recent academia research on artificial intelligence or advance machine learning. Amioy is a research scientist with perfect blend of industrial end to end deployment. He can be contacted at email: amioy.iitd@gmail.com.