IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 7, 2019, accepted March 25, 2019, date of publication April 9, 2019, date of current version April 22, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2909536

An Intelligent Scheme for Continuous Authentication of Smartphone Using Deep Auto Encoder and Softmax Regression Model Easy for User Brain

VISHNU SHANKAR AND KARAN SINGH
School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi 110070, India
Corresponding author: Vishnu Shankar (vishnu44_scs@jnu.ac.in)

This work was supported by Jawaharlal Nehru University, New Delhi, under Grant PAC-JNU-DST Purse-462 (Phase II)-2019.

ABSTRACT The smartphones are becoming more popular these days because of having more technologies in a smaller and slim-sized device. The people can get Internet connectivity and some other facilities, such as communication and storing data, with these smaller devices. It is necessary for securing personal data on smartphone devices with authentication techniques. In recent years, most of the static authentication techniques, such as password, patterns, and fingerprint, were used for securing smartphones. Most of the studies are focusing on a new method called continuous authentication for improving the security of smartphones. The continuous authentication techniques differ from other static authentication techniques by authenticating the smartphone user periodically. It uses behavioral features of users for authenticating the user. Continuous authentication is easy for the user's brain, as a user need not to memorize anything. In this paper, a continuous authentication technique is designed with the Deep Auto Encoder and Softmax Regression techniques (DAE-SR). The DAE-SR achieved 0.950% and 0.970% of accuracy on predicting the users on different states (walking and sitting) of users.

INDEX TERMS Brain signals of user, continuous authentication, smart phone security, deep learning, deep auto encoder, softmax regression, feature selection with BOA, smart phone authentication.

I. INTRODUCTION

In recent years, the world has changed due to the commencement of a revolution in the field of technology. One of the most prominent inventions in technology is the smartphone device [1]. The smartphones offer more convenient services to peoples such as email, online shopping, social networking services, and so on, at the same time, they also reveal valuable personal information to potential attackers [2]. Hence, it is essential to explore a more dependable and secure mechanism for user authentication. The most common authentication system follows knowledge-based mechanisms using PIN codes, passwords and graphical pattern as an inputs [3]. Though, user use small passwords or easy passwords are simple to remember, which will increase the risk of information theft by any unauthorized users. Unfortunately, even if composite passwords are used, they can also be obtained by sending the position of screen taps based on sensors readings [4], [5].

The authentication mechanisms widely use two different types of authentication methods, namely, passwords and PIN codes. Major problem in such authentication schemes are weak passwords that can be easily remembered by the people and it tends to decrease the security level [6]. Even the users used the difficult or large passwords which can also be identified with the help of accelerometer and gyroscope readings by detecting the location of screen taps. In the authentication of mobile users, some of the knowledge based techniques like PINs, patterns and passwords were used for authentication [7], [8]. Such techniques are much weak for various attacks and security threats like smudge attacks, brute force attacks and shoulder surfing. Basically, the usage time periods of mobile devices are much shorter and its authentication frequency is much higher when compared with the desktop computers. So, these traditional authentications schemes cannot be kept secure and effective for longer duration on mobile devices because of its mobility and ubiquity [9], [10].

The biometric based authentication technique is an alternative for passcode based authentication approaches.

The associate editor coordinating the review of this manuscript and approving it for publication was Victor Hugo Albuquerque.

This technique uses the physiological or behavioral features of persons for the authentication [11]. The physiological based biometrics is the stable and unique physical features from human body include iris pattern, fingerprint, and facial features. Another one is the behavior based biometrics, it uses the behavior or habits of humans such as voice, keystroke, signature, and gait [12], [13]. The biometrics-based authentication techniques are free from being stolen, carrying token and user memorization problem. So, it is considered as the highly secured authentication technique when compared with other authentication techniques. For effective biometrics based authentication techniques, the technique should be secure and usable. For increasing the security of these devices, the researchers gave more attention on developing biometric based intelligent authentication techniques in past few decades [14]. The authentication techniques which are based on the voice and iris biometrics are ranked higher on providing higher security and lower on usability [15].

The authentication techniques based on keystroke dynamics got more attention in past years, but it can't work with the smartphones which have the virtual keyboard [16]. In touch screen mobile phones, harmonized user authentication based on thumb stroke dynamics has taken positive dimensions of various mobile authentication schemes. It has better usability and more security from attacks. This method has given both the entry point and continuous authentication mechanism [17]. This has some problem that can be solved by creating a continuous authentication based system with biometric features by considering the usability and security. This continuous authentication never depend on any direct interaction of the user, at the same time it is related to the user's habits, behavior and living environment. This method has the ability to maximize the system security by identifying the identity of users continuously instead of identifying only at the entry point [18], [19]. In past years, various motion sensors were integrated with mobile devices including gyroscope, accelerometer and so on. During such case, in biometric authentication a new branch will be developed [20]. In most of the literature, such mechanisms are known as sensor based authentication and it works mainly based on the data acquired from the physical devices which are integrated with the body or the generated data during the interaction of machine and human.

The remainder of this work is organized as follows: Section 2 describes various related existing continuous authentication techniques, section 3 describes the proposed continuous authentication technique, section 4 describes the experimentation carried out with the presented approach, and finally the presented work is concluded in section 5.

II. RELATED WORKS

Some of the recent works related to continuous smart phone authentication using Behavioral Biometrics are listed below:

Ehatisham-ul-Haq *et al.* [21] presented a method for authenticating the smartphone users with continuous authentication using passive mobile sensing with the base of activity pattern recognition. The researches make this method to focus on performing various actions with behavioral patterns of different users while they are using their smart mobile devices. In the validation of users, there are six different activities of users were utilized, which includes, Walking, Walking Upstairs, Walking Downstairs, Running, Standing and Sitting. Users can be better recognized on the basis of their walking pattern if the phone is kept in their pant pocket. Placing the phone at the upper hand position makes it tough to recognize users on the basis of the walking activity. The main aim of this system is to identify the variations present in the behavioral patterns of various users on similar activities. To achieve this, the researchers tried to learn the behavioral patterns of different users for all the activities with the trained system. Based on the certain activity performed by the users the smartphone users are identified and authenticated by the system.

Meng *et al.* [22] proposed an authentication system based on touch gesture and it is said to as TouchWB. It contains 21 different features for verifying the users based on the web browsing behavior of users on their smartphones. Here, the multi-touch based operations are considered as a feature and best example for multi-touch operation is zoom-in and zoom-out. To identify the variations among the touch gestures of different users, additionally the Radial Basis Function Network (RBFN) and the Particle Swarm Optimization (PSO) were combined and utilized as a classifier. The results achieved on the experimentation of this system shown that, this system can reduce the touch behavioral deviation and the classifier outperformed than other touch based authentication with reduced error rate of 2.4%.

Kim *et al.* [23] presented an authentication method with the base of keystroke-dynamics and by utilizing the freely typed text by conducting the adaptive feature extraction and novelty detection. The difficulties rise during the extraction of features from the freely typed text, a user adaptive feature extraction and a novelty detection technique based method called keystroke dynamics-based authentication (KDA) were designed by the researchers. Every user has their own typing style and they can also make a keystroke features that are user dependent with the base of the typing speed of two sequential keys. To create a novelty score, the valid user's keystroke with some imposter data will be utilized and train the novelty detection algorithm. It identifies the user who is typing at current time is valid user or not. The researchers expected that this method can beats the performance in terms of accuracy with the user-adaptive feature set than other existing fixed feature sets based approaches. By using the keystroke data of all users, they trained the novelty detection algorithm and this can also be implement on other existing security system.

Lamiche *et al.* [24] proposed a method with the base of keystroke dynamics and gait patterns for continuous smartphone authentication. This system detect the gait patterns and keystroke dynamics with the accelerometer through the inputted text and walk without any continuous user

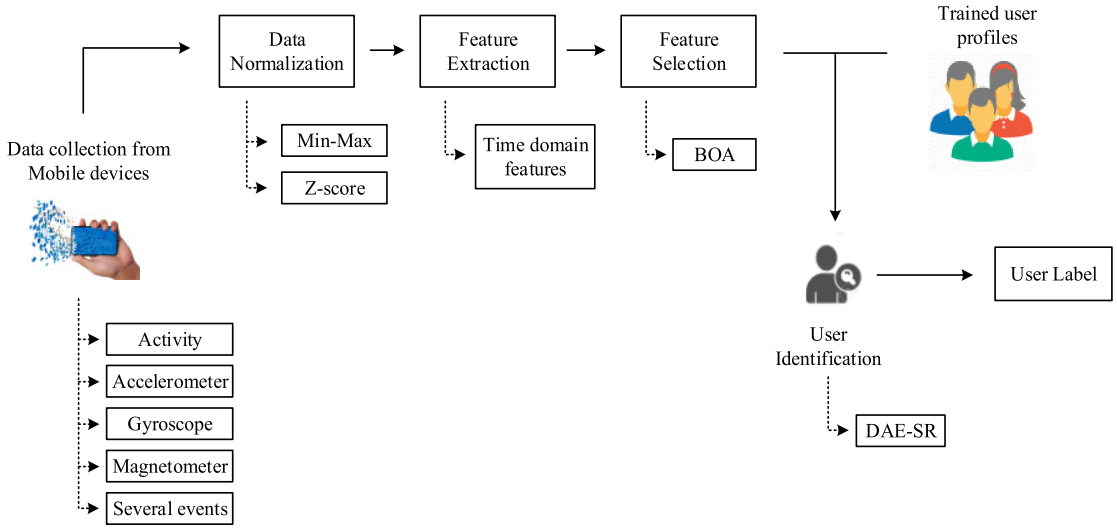

FIGURE 1. Proposed continuous user authentication scheme.

intervention. The process of feature extraction has been carried out from both modalities. The multimodal biometrics profile were constructed with the feature level fusion method for every user. The dimension and the computational complexity of fused feature vector will be reduced with an algorithm called sequential floating forward selection. The efficiency of this method is estimated by the researchers by using various machine learning classifiers with 20 real multimodal dataset collected from various scenarios. Here, two types of attacks were selected for evaluating the security strength of the system namely, minimal-effort mimicking attack and zero-effort attack.

Li *et al.* [25] presented a method with Kernel Ridge Regression for a sensor based continuous authentication. Here, the data augmentation method of the rotation was exploited by the researchers and it is applied on the raw data they already gathered. This process generates more data and increases the strength of the system. The sensor based features were extracted by the sensor CA along with the augmented data from both domains (time and frequency) within the time window. At last, the classifier is trained with KRR-TRBF and the current user was authenticated.

III. PROPOSED CONTINUOUS AUTHENTICATION SCHEME

Nowadays, the security of smart phone device is upgraded through continuous authentication of mobile users. Apart from static authentication, the continuous authentication process give probable solution to earlier security challenges faced by mobile users. In continuous authentication tap and keystroke dynamics features are utilized for authenticating the users. The proposed continuous authentication includes several steps: data collection from mobile devices, data normalization, feature extraction, feature selection, and user identification. At the data collection phase, different behavioral data from various users will be collected through mobile device for authenticating the user.

The data normalization phase, normalize the collected data by using different normalization techniques include, Min-Max and Z-score. The feature extraction phase is responsible for extracting various time domain features from normalized data. By using the Butterfly Optimization Algorithm (BOA) the extracted features will be optimized, and the optimal features are selected. Finally, with the selected features and by using the hybrid deep learning technique Deep Auto Encoder and Softmax Regression (DAE-SR) the user will be identified and labeled.

A. SMART PHONE DATA COLLECTION

The smart phone data is collected from http://www.cs.wm.edu/~qyang/hmog.html. It includes data of a smart phone (Samsung Galaxy S4) used by 100 different users at different time (both male and female). Here, every user answered three different questions while walking and sitting both. It is carried out with total 24 sessions and first 12 were done in walking state and others in sitting state. Here, readings of different sensors such as magnetometer, accelerometer, gyroscope, activity readings, and various events like, touch, key press, pinch, scroll, and stroke were collected for every user. Different orientation of smart phone (portrait and landscape) were allowed during the process of data collection and for experimentation the portrait data is used because of lower user data with landscape mode.

B. DATA NORMALIZATION

In this work, there are 10 different set of data from 10 users in 12 different scenarios was collected for identifying the users. So, numerous amount of data will be kept on the dataset and it need to be normalize. For that, here the data is normalized with two normalization techniques [26] namely, Min-Max and Z-score normalization. These normalization

$$\text{MinMax\_D}_{\text{Att}} = \frac{\text{D}_\text{v} - \text{MinD}_\text{v}}{\text{MaxD}_\text{v} - \text{MinD}_\text{v}} (\text{new\_MaxD}_\text{v} - \text{new\_MinD}_\text{v}) + \text{new\_MinD}_\text{v} \quad (1)$$

techniques will scale the features from a range of value to new range of value.

1) NORMALIZATION WITH MIN-MAX

In this process the data from mobile device with different users are scaled within the range of [0, 1]. The Min-Max method uses linear interpretation formula for scaling the data values and it is given as, On equation 1, D_{Att} represents the corresponding attribute of data, D_v represents the current data value of attribute, MinD_v represents the minimum data value on current attribute, MaxF_v represents the maximum data value of current attribute, and the new maximum and minimum data value is denoted as new_MaxD_v and new_MinD_v and its values are set to 1 and 0.

If any data value looks constant after the normalization process then it will be removed because it never provide any result with the classifier and it also reduce the accuracy of system (Zero is considered here as an constant value). At the result of Min-Max, it provides scaled values of data with same relationship in the data but it is also providing more outliers and ambiguity in data values. Thus, to remove the unwanted outliers in data here another normalization process is carried out with Z-Score normalization technique.

2) NORMALIZATION WITH Z-SCORE

In this technique, the normalization is taken place based on the mean and standard deviation (SD) achieved for every data. The Z-Score normalization is carried out by,

$$\text{ZScore\_D}_{\text{Att}} = \frac{\text{D}_\text{v} - \mu\text{D}}{\sigma\text{D}} \quad (2)$$

where, $\boldsymbol{\mu}\mathbf{D}$ and $\boldsymbol{\sigma}\mathbf{D}$ represents the mean and SD of all data values in corresponding attribute, n is all number of data values. The mean and SD were estimated by,

$$\mu\text{D} = \frac{\text{Addition of all data values in current attribute}}{\text{No of data values}} \quad (3)$$

$$\sigma\text{D} = \sqrt{\frac{\sum (\text{Every individual data values in attribute} - \mu\text{D})^2}{\text{n}}} \quad (4)$$

The outliers in the dataset will be removed with equation 2.

C. FEATURE EXTRACTION

Once the collected mobile data is normalized, the features available on the normalized data will be extracted. There are various time domain features are extracted during this process and it includes, maximum amplitude, minimum amplitude, variance, mean, median, first difference in absolute value of mean, second difference in absolute value of mean, minimum latency, maximum latency, peak-to-peak signal value, peak-to-peak time, peak-to-peak slope, skewness, kurtosis, and entropy. The time domain features can describes the accurate variation among the data from different users. The expression utilized for extracting features are described below:

Maximum amplitude: It is one of the time domain signal based feature, provides the highest amplitude signal value on every set of data. It is given by,

$$\text{Amp}_{\text{max}} = \max \{\text{D}_{\text{Att}}(\text{n})\} \quad (5)$$

where, $\text{D}_{\text{Att}}(\text{n})$ represents all the data values in corresponding attribute.

Minimum amplitude: It provides the lowest amplitude signal value on every set of data and it is given by,

$$\text{Amp}_{\text{min}} = \min \{\text{D}_{\text{Att}}(\text{n})\} \quad (6)$$

Here for estimating the maximum and minimum amplitude values, the event time among the sensors were utilized.

Variance: It estimates the zero variance among the values and removes all zero values and it is given by,

$$\sigma^2 = \frac{1}{\text{N}} \sum (\text{D}_{\text{Att}}(\text{n}) - \mu\text{D})^2 \quad (7)$$

Here, N represents the number of data values.

Mean: The mean value of data provides an average value among the data values and it is estimated with equation (3).

Median: The median describes the middle value of the dataset. Initially it rearranges the values in smaller to higher and find the middle value. The median value is estimated by,

$$\text{Med} = \{(\text{N} + 1) \div 2\} \quad (8)$$

First difference in absolute value of mean: The absolute value of mean describes the difference among the data values in corresponding attributes. Here, first and second difference was considered. The first difference of mean is estimated by,

$$\mu\text{D}_1 = \frac{1}{N} \sum |\text{D}_{\text{Att}}(\text{n}) - \text{D}_{\text{Att}}(\text{n} - 1)| \quad (9)$$

Second difference in absolute value of mean: The second absolute value of mean is estimated by,

$$\mu\text{D}_2 = \frac{1}{\text{N}} \sum |\text{D}_{\text{Att}}(\text{n} + 1) - 2\text{D}_{\text{Att}}(\text{n}) + \text{D}_{\text{Att}}(\text{n} - 1)| \quad (10)$$

Minimum latency: The latency provides time interval among the inputs from user. Here, minimum and maximum latency were considered. The minimum latency is estimated by,

$$\text{n}_{\text{Amp}_{\text{min}}} = \left\{\text{n} | \text{D}_{\text{Att}}(\text{n}) = \text{Amp}_{\text{min}}\right\} \quad (11)$$

Maximum latency: The maximum latency is estimated by,

$$\text{n}_{\text{Amp}_{\text{max}}} = \left\{\text{n} | \text{D}_{\text{Att}}(\text{n}) = \text{Amp}_{\text{max}}\right\} \quad (12)$$

Peak-to-peak signal value: The peak-to-peak features represents the variance among the maximum positive and negative rate of amplitudes from different sensors. Here, three

different peak-to-peak features were considered. The peak-to-peak signal value is estimated by,

$$PP_{sv} = Amp_{max} - Amp_{min} \tag{13}$$

Peak-to-peak time: The peak-to-peak time is estimated by,

$$PP_t = n_{Amp_{max}} + n_{Amp_{min}} \tag{14}$$

Peak-to-peak slope: The peak-to-peak slope is estimated by,

$$PP_s = \frac{PP_{sv}}{PP_t} \tag{15}$$

Skewness: It estimate the symmetry among the data values of corresponding data attributes. It is given by,

$$Skew = \frac{\sum_{i=1}^{N} (D_{Att}(n) - \mu D)^3 / N}{\sigma D^3} \tag{16}$$

Kurtosis: This feature describes that the data is either high or light tailed. High tailed data indicates the outliers and light tailed data indicates the lack of outliers. The kurtosis is estimated by,

$$Kurt = \frac{\sum_{i=1}^{N} (D_{Att}(n) - \mu D)^3 / N}{\sigma D^3} \tag{17}$$

Entropy: It partition the data based on its similarity and it is given as,

$$Ent = -\sum_{i=1}^{N} p_i(n) log_2 p_i(n) \tag{18}$$

where p represents the probability of events.

D. FEATURE SELECTION

After the extraction of features from different user's data the feature selection process will be initiated. The feature selection is carried-out by using the Butterfly Optimization Algorithm (BOA) [27]. This optimization technique was developed based on the food foraging process of butterflies. Different from other metaheuristic optimization techniques, the BOA contains fragrance and it has its own unique scent and personal touch. It initially identifies or emits some fragrance and finds the best one globally or locally and updates it to population.

Here, the set of extracted features should be in non-linear and it needs to covert it as linear for an effective feature selection. For converting the feature set into linear, the fisher score is estimated and rescaled.

The fisher score is determined by,

$$FS(f_i) = \frac{\sum_{D_{Att}=1}^{p} n_{D_{Att}} \left(\mu D_{f_i}^{D_{Att}} - \mu D_{f_i}\right)^2}{\sum_{D_{Att}=1}^{p} \left(f_i - \mu D_{f_i}^{D_{Att}}\right)^2} \tag{19}$$

where, $n_{D_{Att}}$ represents the number of data values in an attribute, f_i represents the feature, μD_{f_i} represents the mean of feature, and $\mu D_{f_i}^{D_{Att}}$ represents the mean of the feature in corresponding attribute.

The fisher score $FS(f_i)$ will be rescale at the range $[\varepsilon, 1, -\varepsilon]$ and the linear function $LF(FS(f_i))$ is described by,

$$LF(FS(f_i)) = \frac{1 - 2\varepsilon}{FS_{max} - FS_{min}} FS(f_i) + \frac{\varepsilon (FS_{max} - FS_{min}) - FS_{min}}{FS_{max} - FS_{min}} \tag{20}$$

On equation 20, ε indicates the smaller positive value, $0 < \varepsilon < 0.1$.

After the conversion of non-linear feature set, the feature selection is carried out with BOA. It initially generates fragrance for every butterfly on the solution space. Before that it needs to estimate the fitness function for all the butterflies in the search space. It has been estimated with two goals, selecting minimal features and getting higher accuracy.

The fitness function can be estimated with,

$$fit(f_i) = \alpha ER_C + \beta \frac{|F_{fs}|}{|N_{fs}|} \quad \alpha \in [0, 1] \tag{21}$$

where, $\beta = [1 - \alpha]$.

From equation 21, the α and β represents the quality and length of subset, the error rate of classifier is denoted as ER_C, the total number of features available for corresponding user is represented as $|N_{fs}|$, and the cardinality of selected feature set is described as $|F_{fs}|$. The fragrance of butterfly will be generated by,

$$Fr_{bf} = S_m S_i^b \tag{22}$$

In equation 22, S_m represents the sensory modality, S_i represents the stimulus intensity, and b represents the modality based power exponent. The value of b and S_m lies in [0, 1].

Once the fragrance is generated, it start to find the butterfly with more fragrance to get the optimal solution. The search process is carried out with its two key steps, global search and local search.

The global search is given as,

$$a_i^{it+1} = a_i^{it} + \left(rn^2 \times g_b - a_i^{it}\right) \times Fr_i \tag{23}$$

On above equation, the solution vector of butterfly a_i in current iteration **it** is represented as a_i^{it}, the best solution found in current iteration is described as g_b, Fr_i represents the fragrance of current butterfly, and rn represents the random number lies among [0, 1].

The local search is given as,

$$a_i^{it+1} = a_i^{it} + \left(rn^2 \times a_j^{it} - a_k^{it}\right) \times Fr_i \tag{24}$$

On above equation, the j^{th} and k^{th} butterflies in solution space is described as a_j^{it} and a_k^{it}.

After completing the searching process the algorithm will provide the best solution found with better fitness.

Algorithm 1 Feature Selection With BOA

Input: Set of extracted features
Output: Optimal features
Objective function f (x) , x = (x_1, x_2, . . . , x_n), n indicates the no. of dimensions
Generate the initial population of butterflies a_i, i = 1, 2, . . . , n
Stimulus intensity S_i at a_i
Define the parameters includes, S_m sensor modality, b power exponent,
and ρ switch probability
while stopping criteria not met
    do
    for each butterfly in population
        do
        Estimate fitness function with equation 21.
        Estimate fragrance with equation 22.
        Estimate randomly the position of butterfly based on fitness and
    fragrance
    end for
    Find best butterfly
    for each butterfly in population
        do
        Create a random number rn from [0, 1]
        if rn $< \rho$ then
            Move the current one to the position of best one with
    equation 23.
        Else
            Move randomly with equation 24.
        End if
    End for
    Update b
End while

E. CLASSIFICATION OF USER

In this work, the identification of right mobile user is identified by using the DAE-SR. The deep auto encoder [28] is an unsupervised learning method and it reduces the dimension of the inputted data. It can reduce the classification time and improve the accuracy of authentication system. The classification of users is carried out with softmax regression technique. We have used softmax regression as this is a multiclass classifier.

1) DIMENSION REDUCTION WITH DEEP AUTO ENCODER

The set of features selected with BOA is used as the input for the deep auto encoder and it is given as,

$$f = f_1, f_2, \ldots f_n \tag{25}$$

The reduced dimension of input layer is given as the hidden layer $h = h_1, h_2, \ldots, h_n$ and it is done with feed forward activation function. It is expressed as,

$$h = \sigma\left(W_1 \times f + B_1, W_2 \times f + B_2, \ldots, W_n \times f + B_n,\right) \tag{26}$$

where, W and B indicates the weight value and bias unit.

2) RECOGNIZING THE USER WITH SOFTMAX

The hidden units obtained from the training of auto encoder can be utilized and inputted to the softmax to classify the user. That means it uses the last encoded feature data.

The softmax classifier model training needs input data (data from hidden unit) $x = \left\{x^1, x^2, \ldots x^n\right\}$ and the labels of class $cl = \left\{cl^1, cl^2, \ldots, cl^n\right\}$.

The training process is initiated by estimating the probability of input data P(cl = j|x) and j = 1, 2, . . . , m. Based on the different possible value of m the probability will be estimated.

The hypothesis function is formed by,

$$\begin{aligned} HF_\theta\left(x^{(i)}\right) &= \begin{bmatrix} P(cl^i = 1|x^i; \theta) \\ P(cl^i = 2|x^i; \theta \\ \vdots \\ P(cl^i = m|x^i; \theta \end{bmatrix} \\ &= \frac{1}{\sum_{k=1}^{m} \exp\left(\theta^{(k)T} x\right)} \begin{bmatrix} \exp\left(\theta^{(1)T} x\right) \\ \exp\left(\theta^{(2)T} x\right) \\ \vdots \\ \exp\left(\theta^{(m)T} x\right) \end{bmatrix} \end{aligned} \tag{27}$$

TABLE 1. Performance on walking state with various classifiers.

Methods	*Accuracy*	*Precision*	*Recall*	*F-measure*	*Error rate*	*Equal Error rate*
KNN	*0.927*	*0.920*	*0.897*	*0.877*	*0.073*	*0.087*
SVM	*0.932*	*0.935*	*0.902*	*0.890*	*0.068*	*0.079*
DAE-SR	*0.950*	*0.978*	*0.918*	*0.900*	*0.050*	*0.050*

TABLE 2. Performance on sitting state with various classifiers.

Methods	*Accuracy*	*Precision*	*Recall*	*F-measure*	*Error rate*	*Equal Error Rate*
KNN	*0.916*	*0.930*	*0.926*	*0.917*	*0.064*	*0.091*
SVM	*0.942*	*0.943*	*0.942*	*0.930*	*0.058*	*0.073*
DAE-SR	*0.970*	*0.979*	*0.959*	*0.968*	*0.032*	*0.030*

where, the θ represents the parameters of softmax model, and the normalization of distribution is given as an expression $\frac{1}{\sum_{k=1}^{m} \exp(\theta^{(k)T} x)}$.

The input data from the user will be identified with the obtained hypothesis function.

IV. EXPERIMENTAL DATASET RESULT AND DISCUSSION

In this section the performance of proposed continuous authentication technique is evaluated. The proposed DAE-SR model is implemented in Python platform and the obtained results are compared with two other classifier KNN and SVM.

Here, the data of 10 different users were utilized during the evaluation with 12 sessions. There, 8 sessions are used for training the classifier (4 on sitting state and 4 on walking state) and other 4 sessions were used for testing the classifier (2 on sitting state and 2 on walking state). More details about dataset can be seen on the link http://www.cs.wm.edu/~qyang/hmog.html.

A. PERFORMANCE ANALYSIS

The performance obtained for different classifiers in both state is described on below tables.

From table 1 and 2, the performance of different classifiers on continuous authentication is compared in terms of accuracy, precision, recall, f-measure, error rate, and equal error rate. The performance with walking state is slight lower when comparing it with the performance obtained on sitting state. It is because of the varied timing of different events data collected on walking state. In walking state most of the users are pressing the keys with more differed or on a same timings.

The performance of various classifiers on recognizing the users are evaluated with several metrics and it is given below:

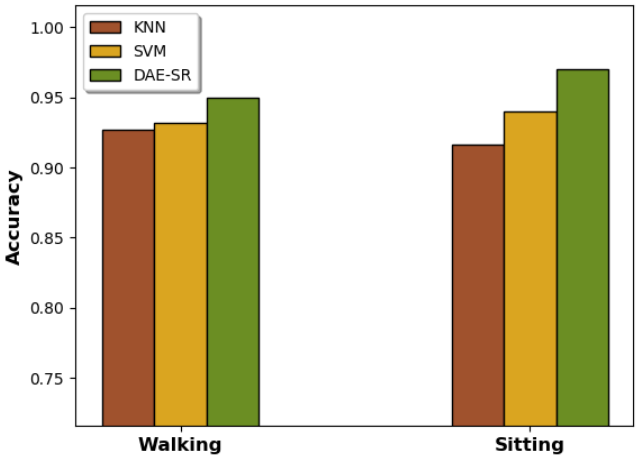

FIGURE 2. Comparison of accuracy on continuous authentication technique with various classifiers.

1) ACCURACY

The accuracy of continuous authentication technique with different classifiers is estimated with,

$$\mathrm{ACC} = \frac{t_p + t_n}{t_p + t_n + f_p + f_n} \tag{28}$$

The above figure describing the accuracy of different classifiers. It clearly shows that the proposed DAE-SR technique earned better results than the SVM and KNN. The DAE-SR got up to 0.950 % and 0.970 % on walking and sitting state.

2) PRECISION

The precision of continuous authentication technique with different classifiers is estimated with,

$$\mathrm{Pre} = \frac{t_p}{t_p + f_p} \tag{29}$$

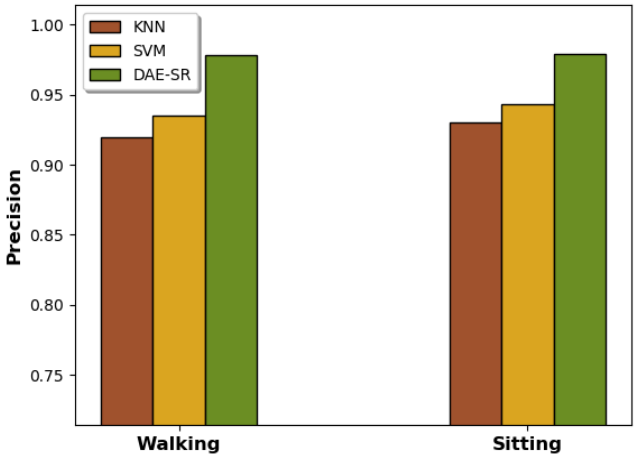

FIGURE 3. Comparison of precision on continuous authentication technique with various classifiers.

The comparison of precision on both state is described in above figure. Here, the DAE-SR earned 0.978 % and 0.979 % of precision and other classifiers KNN and SVM earned 0.920 %, 0.930 % and 0.935 %, 0.943 % of precision rate.

The performance of DAE-SR much better when compared with KNN and SVM.

3) RECALL

The recall rate of continuous authentication technique with different classifiers is estimated with,

$$\text{Re\_c} = \frac{t_p}{t_p + f_n} \tag{30}$$

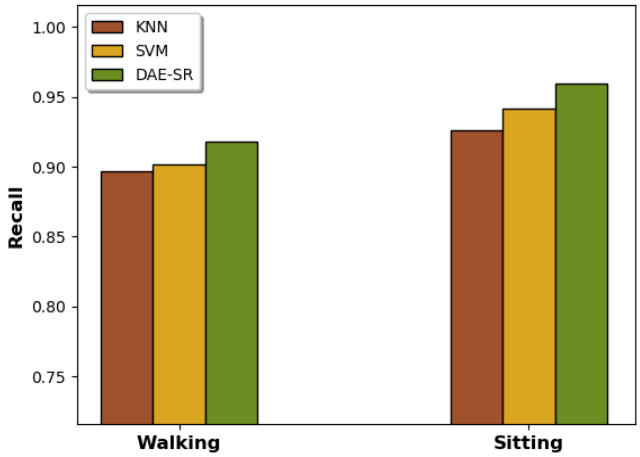

FIGURE 4. Comparison of recall on continuous authentication technique with various classifiers.

The above figure describes the comparison of recall on different classifiers. On recall rate, the DAE-SR got 0.918% and 0.959 %, it is better than the other two classifiers. The recall rate of KNN and SVM is 0.897 %, 0.926 % and 0.902 %, 0.942 % at sitting and walking state.

4) F-MEASURE

The f-measure rate on continuous authentication technique with different classifiers is estimated with,

$$\text{F} - \text{m} = 2\left(\frac{\text{Pre.Re\_c}}{\text{Pre} + \text{Re\_c}}\right) \tag{31}$$

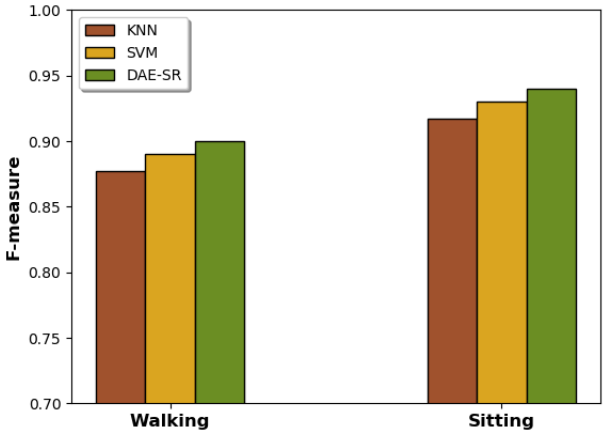

FIGURE 5. Comparison of f-measure on continuous authentication technique with various classifiers.

Above figure describes the comparison on different classifiers with their f-measure rate. While comparing the f-measure rate of different classifiers, it shown that the results of DAE-SR beaten the performance of KNN and SVM. The f-measure rate of DAR-SR is 0.900 % and 0.968 % on sitting and walking state.

5) ERROR RATE

The error rate on continuous authentication technique with different classifiers is estimated with,

$$\text{Err} = 1 - \text{Acc} \tag{32}$$

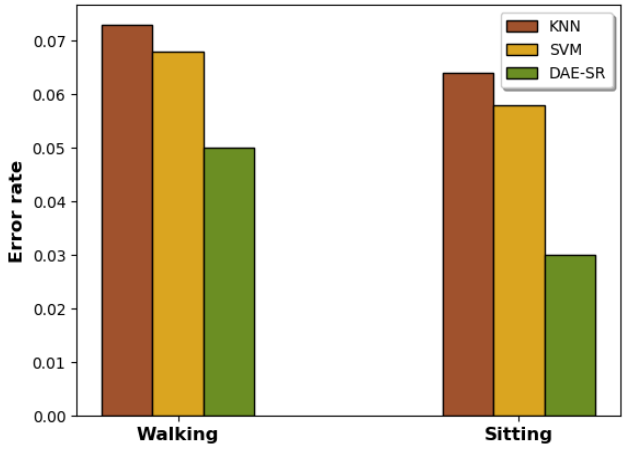

FIGURE 6. Comparison of error rate on continuous authentication technique with various classifiers.

The comparison of error rate on both state is described in above figure and it shows the proposed DAE-SR achieved much lower error rate on both state than other classifiers. The proposed technique got the lowest error rate of 0.050 % and 0.032 % on walking and sitting state.

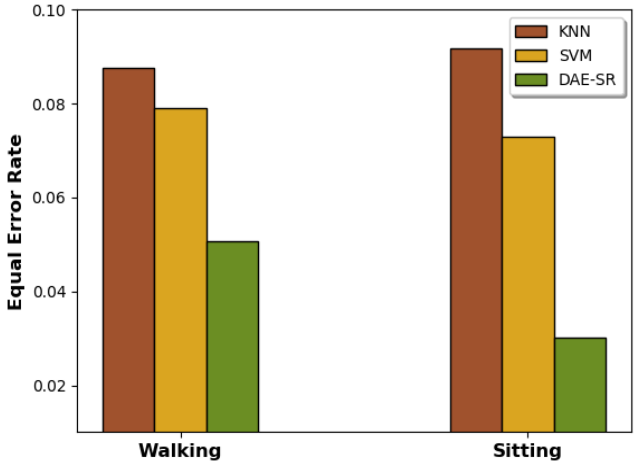

FIGURE 7. Comparison of equal error rate on continuous authentication technique with various classifiers.

6) EQUAL ERROR RATE

The equal error rate (EER) of authentication technique is determined based on the false acceptance rate (FAR) and false

rejection rate (FRR). It is given by,

$$\text{FAR} = \frac{f_p}{(f_p + t_n)} \tag{33}$$

$$\text{FRR} = \frac{f_n}{f_n + t_p} \tag{34}$$

$$\text{EER} = \frac{\text{FAR} + \text{FRR}}{2} \tag{35}$$

The equal error rate on different classifiers is described in above figure. Here, the proposed authentication method achieved a lowest equal error rate of 0.050% at walking and 0.030% standing state. Other compared classifiers got higher equal error rate than the DAE-SR. The obtained ERR values of KNN and SVM at both states are given in table 1 and 2.

The comparison of results from different classifiers shown that the proposed DAE-SR classifier is better than the other neural network based classifiers such as, KNN and SVM. The error rate of KNN is much higher than the DAE-SR and SVM. It reduces the accuracy of KNN based continuous authentication system. On DAE-SR, it reduces the error rate by predicting the right users and earned higher accuracy while classifying the users.

V. CONCLUSION

In this work, an intelligent continuous authentication technique is presented for authenticating the smart phone users. This continuous authentication technique will authenticate the user periodically with theirs behavioral features. It provide more security for smart phones than other one time based authentication techniques like pattern, password, PIN, face recognition, finger print and so on. The technique proposed in this work uses various features from mobile devices and it is extracted from collected data from the different sensors embed on mobiles and other events such as, touch, key press, pinch, scroll, and stroke. Based on these data the behavior of every user will be identified by the authentication system. Moreover, the best features from the extracted features were selected by using the BOA. The best features selected with the BOA will be utilized for classifying the user. The authorized user of smart phone is identified and classified with the DAE-SR technique. The results of DAE-SR are compared with other deep learning based classifiers such as KNN and SVM. The result shows that the present technique is better than the KNN and SVM. The DAE-SR got maximum accuracy of 0.950 % and 0.970 % on walking and sitting state.

REFERENCES

[1] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 136–148, Jan. 2013.

[2] M. Derawi and P. Bours, "Gait and activity recognition using commercial phones," *Comput. Secur.*, vol. 39, pp. 137–144, Nov. 2013.

[3] H. Crawford, K. Renaud, and T. Storer, "A framework for continuous, transparent mobile device authentication," *Comput. Secur.*, vol. 39, pp. 127–136, Nov. 2013.

[4] P. Casale, O. Pujol, and P. Radeva, "Personalization and user verification in wearable systems using biometric walking patterns," *Pers. Ubiquitous Comput.*, vol. 16, no. 5, pp. 563–580, 2012.

[5] S. R. M. Prasanna, S. K. Sahoo, and T. Choubisa, "Multimodal biometric person authentication: A review," *IETE Tech. Rev.*, vol. 29, no. 1, pp. 54–75, 2012.

[6] X. Zhao, T. Feng, W. Shi, and I. Kakadiaris, "Mobile user authentication using statistical touch dynamics images," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1780–1789, Nov. 2014.

[7] J. A. Unar, W. C. Seng, and A. Abbasi, "A review of biometric technology along with trends and prospects," *Pattern Recognit.*, vol. 47, no. 8, pp. 2673–2688, 2014.

[8] O. Alpar, "Keystroke recognition in user authentication using ANN based RGB histogram technique," *Eng. Appl. Artif. Intell.*, vol. 32, pp. 213–217, Jun. 2014.

[9] A. Mahfouz, T. M. Mahmoud, and A. S. Eldin, "A survey on behavioral biometric authentication on smartphones," *J. Inf. Secur. Appl.*, vol. 37, pp. 28–37, Dec. 2017.

[10] C. Shen, Y. Chen, and X. Guan, "Performance evaluation of implicit smartphones authentication via sensor-behavior analysis," *Inf. Sci.*, vols. 430–431, pp. 538–553, Mar. 2018.

[11] P. S. Teh, N. Zhang, A. B. J. Teoh, and K. Chen, "A survey on touch dynamics authentication in mobile devices," *Comput. Secur.*, vol. 59, pp. 210–235, Jun. 2016.

[12] P. Kang and S. Cho, "Keystroke dynamics-based user authentication using long and free text strings from various input devices," *Inf. Sci.*, vol. 308, pp. 72–93, Jul. 2015.

[13] O. Alpar, "Intelligent biometric pattern password authentication systems for touchscreens," *Expert Syst. Appl.*, vol. 42, nos. 17–18, pp. 6286–6294, 2015.

[14] G. Kambourakis, D. Damopoulos, D. Papamartzivanos, and E. Pavlidakis, "Introducing touchstroke: Keystroke-based authentication system for smartphones," *Secur. Commun. Netw.*, vol. 9, no. 6, pp. 542–554, 2016.

[15] A. Alzubaidi and J. Kalita, "Authentication of smartphone users using behavioral biometrics," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1998–2026, 3rd Quart., 2016.

[16] A. Jain and V. Kanhangad, "Exploring orientation and accelerometer sensor data for personal authentication in smartphones using touchscreen gestures," *Pattern Recognit. Lett.*, vol. 68, pp. 351–360, Dec. 2015.

[17] L. Zhou, Y. Kang, D. Zhang, and J. Lai, "Harmonized authentication based on ThumbStroke dynamics on touch screen mobile phones," *Decis. Support Syst.*, vol. 92, pp. 14–24, Dec. 2016.

[18] C.-L. Liu, C.-J. Tsai, T.-Y. Chang, W.-J. Tsai, and P.-K. Zhong, "Implementing multiple biometric features for a recall-based graphical keystroke dynamics authentication system on a smart phone," *J. Netw. Comput. Appl.*, vol. 53, pp. 128–139, Jul. 2015.

[19] C. Shen, Y. Zhang, X. Guan, and R. A. Maxion, "Performance analysis of touch-interaction behavior for active smartphone authentication," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 498–513, Mar. 2016.

[20] D. Dasgupta, A. Roy, and A. Nag, "Toward the design of adaptive selection strategies for multi-factor authentication," *Comput. Secur.*, vol. 63, pp. 85–116, Nov. 2016.

[21] M. Ehatisham-ul-Haq, M. A. Azam, U. Naeem, Y. Amin, and J. Loo, "Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing," *J. Netw. Comput. Appl.*, vol. 109, pp. 24–35, May 2018.

[22] W. Meng, Y. Wang, D. S. Wong, S. Wen, and Y. Xiang, "*TouchWB*: Touch behavioral user authentication based on Web browsing on smartphones," *J. Netw. Comput. Appl.*, vol. 117, pp. 1–9, Sep. 2018.

[23] 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," *Appl. Soft Comput.*, vol. 62, pp. 1077–1087, Jan. 2018.

[24] I. Lamiche, G. Bin, Y. Jing, Z. Yu, and A. Hadid, "A continuous smartphone authentication method based on gait patterns and keystroke dynamics," *J. Ambient Intell. Hum. Comput.*, pp. 1–14, Nov. 2018. [Online]. Available: https://link.springer.com/article/10.1007/s12652-018-1123-6

[25] Y. Li, H. Hu, G. Zhou, and S. Deng, "Sensor-based continuous authentication using cost-effective kernel ridge regression," *IEEE Access*, vol. 6, pp. 32554–32565, 2018.

[26] S. García, J. Luengo, and F. Herrera, "Data preparation basic models," in *Data Preprocessing in Data Mining* (Intelligent Systems Reference Library 72). Cham, Switzerland: Springer, 2015. doi: 10.1007/978-3-319-10247-4_3.

[27] S. Arora and S. Singh, "Butterfly optimization algorithm: A novel approach for global optimization," *Soft Comput.*, vol. 23, no. 3, pp. 715–734, 2019.
[28] E. Hosseini-Asl, J. M. Zurada, and O. Nasraoui, "Deep learning of part-based representation of data using sparse autoencoders with nonnegativity constraints," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 12, pp. 2486–2498, Dec. 2016.

VISHNU SHANKAR received the M.Tech. degree in computer science and technology from the School of Computer and Systems Sciences, Jawaharlal Nehru University, India, where he is currently pursuing the Ph.D. degree. He has published various papers in conferences and journals. His research interests include authentication and machine learning. He is also a Life Member of the Computer Society of India.

KARAN SINGH received the Engineering degree in computer science and engineering from the Kamala Nehru Institute of Technology, Sultanpur, Uttar Pradesh, India, and the M.Tech. degree in computer science and engineering from the Motilal Nehru National Institute of Technology (MNNIT) at Allahabad (deemed university), Uttar Pradesh. He is currently pursuing the Ph.D. degree in computer science and engineering with MNNIT. He has supervised 35 M.Tech. degree students and four Ph.D. Scholars. He was with Gautam Buddha University, from 2010 to 2014. He has organized various workshops, sessions, and conferences and training. He is currently with the School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi. He has published over 70 research papers in journals and good conferences. His primary research interests include computer networks, computer network security, multicast communications, and IoT.

He was a Professional Member of the Association for Computing Machinery (ACM), NY, USA, the Computer Science Teachers Association (CSTA), USA, the Computer Society of India (CSI), Secunderabad, India, the Cryptology Research Society of India (CRSI), Kolkata, India, the International Association of Computer Science and Information Technology (IACSIT), Singapore, the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (ICST), USA, the International Association of Engineers (IAENG), Hong Kong, the Association of Computer Electronics and Electrical Engineers (ACEEE), India, the Internet Society (ISOC), USA, and the Academy and Industry Research Collaboration Center (AIRCC), India. He has organised one week STC on Network and Cyber Security at JNU, New Delhi, where he is going to organize the international conference on Networks and Cryptology. He was the General Chair of the QShine (international conference) with Gautam Buddha University, in 2013. He was nominated for Who's Who in World, in 2008, and the IEEE MGM Award. He is a Reviewer of the IEEE and Elsevier conferences. He is also a Reviewer of international journals and the IEEE TRANSACTIONS. He is an Editorial Board Member of the *Journal of Communications and Networks* (CN), USA.