International Journal of Mobile Computing and Multimedia Communications
Volume 13 • Issue 1

Optimal Weighted Logarithmic Transformation Converted HMOG Features for Automatic Smart Phone Authentication

Vinod P. R., Noorul Islam Centre for Higher Education, India*
Anitha A., Noorul Islam Centre for Higher Education, India

ABSTRACT

This paper intends to develop an automatic behavior-based smart phone authentication model by three major phases: feature extraction, weighted logarithmic transformation, and classification. Initially, from the data related to the touches/gesture of the smartphone user, hand movement, orientation, and grasp (HMOG), features are extracted with the aid of grasp resistance and grasp stability. These extracted features are mapped within the particular range by normalizing HMOG. These normalized data are multiplied with the weights followed by logarithmic transformation in the weighted logarithmic transformation phase. As a novelty, the decision-making process related to the logarithmic and weight selection is based on the improved optimization algorithm, called modified threshold-based whale optimization algorithm (MT-WOA). The final feature vectors are fed to DBN for recognizing the authorized users. Finally, a performance-based evaluation is performed between the MT-WOA+DBN and the existing models in terms of various relevant performance measures.

KEYWORDS

HMOG, Modified Threshold Function, Smart Phone Authentication, Weighted Logarithmic Transformation, Whale Optimization Algorithm

1. INTRODUCTION

Recently, the smart phones play a ubiquitous role in the life of human beings as they have become a part and parcel of life. In the recent days, there is a wide spread of mobile devices such as smart phones, tablets, and portable computers. As a part of this, the smart phone devices are capable of storing a vast quantity of private information, and hence the authentications of smart phones from illegal users (who are not the owners of smart phone) are an increasing demand among the smart phone users (Gasti *et al.,* 2016*;* Galdi *et al.,* 2018). One among the commonly utilized manual authentication processes is password, which needs to be memorized by the users for future login. The main drawback behind these short passwords is, they can be lost or forgotten or else they could be shared illegally, by which the attackers can easily interrupt the device (Thavalengal & Corcoran, 2016). Most of the password based login option is employed at the beginning of the usage of smart phones, and once the device is logged in and left aside, there is a probability of illegal users to hack the private information of the user. Moreover, in the sense of making the smart phones as user-friendly devices, the frequent typing of passwords during each of the login sessions annoyed the smart phone users (Valsesia *et al.,*

DOI: 10.4018/IJMCMC.301968 *Corresponding Author

2017). Therefore, there is a necessity to have a continuous user authentication without frequent user involvement after login (Ehatisham-ul-Haq *et al.,* 2018*;* Alghamdi & Elrefaei, 2018).

The behavior-based authentication on the basis of the physiological characteristics of the user is a boon to this user authentication approach. In the behavior-based authentication, the behavior of the legitimate user profiles is initially generated, and the devices check for the remarkable difference between the current user activities as well as the profiles (Laghari *et al.,* 2016). In case of capturing a difference, the mobile device generated an alarm to portray that the user is an illegal user. This verification of the behavior-based authentication commences during the login section and keeps continuing even after login. In the mobile devices, the behavior-based authentication is a grooming area, and it does not require any dedicated devices. The keystroke-based authentication which accomplishes the authentication process via the accelerometer and the touch screen-based biometrics that makes the authentication with the aid of multiple sensors fall under the behavior-based authentication approaches (Nyang *et al.,* 2014*;* Lin, et al. (2010). Most of the recent researches on the behavior-based authentication have focused on the login task alone; these approaches fail to exhibit the difference in the user task after login and during the continuous usage of device. It is a more challenging task to record the continuous behavior-based user authentication after the user login.

The most promising approach among the available authentication approaches is the biometric-based authentication. One among them is the fingerprint-based biometric authentication systems, which is utilized in larger extent due to its low implementation cost. It fails to obtain high-quality images from the finger prints at times of cut, tear, dirt and so on. The iris-based biometric authentication is based on the biological composition of the iris (Alzubaidi & Kalita, 2016*;* Schaffer, 2015). This is much reliable than the fingerprint, and here the accuracy of the recognition gets diminished for individual wearing glasses, eye lenses and etc. Further, a high level of accuracy is obtained from the retina recognition, and there is chance for the authentication process to become worse due to high blood pressure and diabetics. The other biometric authentication technique is the ear recognition technique, and here the authenticated is made on the basis of the unique shape and appearance of human being ear. This is a much comfortable method while compared to iris and retina recognition. In contrast, the ear based authentication cannot provide a strong establishment of an individual's identity (Martinez-Diaz *et al.,* 2016*;* Yang *et al.,* 2019). Therefore, there is a necessity to develop a continuous biometric-based authentication model with the aim of getting rid of the drawbacks in each of the existing authentication models.

The Major Contribution Of This Paper Is Listed Below:

1. To develop behaviour based smart phone authentication model with the aid of (i) Feature extraction (ii) Weighted logarithmic transformation (iii) Classification.
2. The features related to touches/ gestures so called as HMOG are extracted from input data belonging to accelerometer, gyroscope, and magnetometer using grasp resistance and grasp stability.
    4. The normalization of data is done, which is further multiplied with weight and perform logarithmic transformation in the weighted logarithmic transformation phase.
    5. The decisions on weights and logarithmic functions are made with a new optimization model referred as MT-WOA, which is called as transformation plane optimization.
    6. The final feature vector is subjected to DBN for detecting the authorized user. At the end, the performance validation is done by comparing the proposed model MO- WOA+ DBN over conventional models.

The overall organization of the paper is discussed as follows: The literature work on smart phone authentication model with their advantages and challenges are discussed in Section II. The architecture of the proposed smart phone authentication model is portrayed in Section III. The optimal weighted

logarithmic features for smart phone authentication model are depicted in Section IV. Section V provides a vivid explanation of the obtained results, and Section VI provides a strong conclusion to this paper.

2. LITERATURE REVIEW

2.1. Related Works

Shen *et al.,* 2018 proposed an innovative approach for continuous authentication and monitoring of the smart phone users by means of utilizing the motion sensors such as accelerometer and gyroscope. From the motion-sensors, the data features like time, frequency and wavelet-domain were extracted, and the characterization of the fine-grains of user movements was accomplishing using conduct empirical feature analysis.

Sitová *et al.,* 2016 have used HMOG features with the intention of authenticating the smartphone users in an continuous manner. This approach was efficient in capturing the subtle micro-movement as well as the resulting orientation dynamics on the basis of the grasping behaviors, holding and trapping of the smart phone. The data for authentication of the smart phones were gathered under two main conditions such as: 1) sitting and 2) walking. The extracted features were evaluated on the basis of three different features like HMOG, keystroke, and tap. Further, the evaluation of the features was accomplished by authentication, BKG, and energy consumption on smart phones.

Buriro *et al.,* 2019proposed AnswerAuth as an innovative behavioral biometric-based smart phone authentication mechanism in terms of sliding and lifting movements. The authorization was made at the time of sliding the lock button on the screen to unlock the phone and in bringing the phone towards the ear. The behaviour based movement of smart phone both in unlocking and the way of moving the phone towards the ear were monitored by accelerometer, gyroscope, gravity, magnetometer, and touch screen sensors.

Lu & Liu, 2015 formulated a novel re-authentication system referred as safeguard for accurate verification of smart phone users on the basis of on-screen finger movements. There was a transparency for the users about the back-end computation and processing on the key features. The unique features from each user were extracted from fine-grained on-screen biometric metrics such as sliding dynamics and pressure intensity.

Zhu *et al.,* 2017 developed a new handy user authentication scheme referred as ShakeIn to authorize the user during the shaking movement of the smart phone especially at unlocking. The effective motion sensors embedded in the smart phone had captured the unique and reliable biometrical features of users shaking movement of the phone. Further, to enhance the authentication of the smart phones, ShakeIn had endowed the users with an utmost flexibility in operation; thereby permitting the users to customize the way of shaking the phone.

Cao & Chang formulated a novel new nonintrusive and continuous mobile user verification framework with the objective of diminishing the required frequency utilized by user to feed the security token. Further, the tailored HMM as well as SLRT were employed to construct a low-cost, readily available, anonymized, and multimodal smart phone data.

Yang *et al.,* formulated IA system on the basis of adaptive sampling in order to choose the dynamic sets of activities for user behavior in an automatic manner. The authentication features were obtained from various activities like the location of the user, usage of application and motion of user. PLDA was employed for more accurate extraction of the features. The soft biometric-based authentication model was superior to the hard biometric-based authentication as well as password-based authentication in terms of energy efficiency for battery-powered mobile devices and lack of explicit user action.

Agrawal & Patidar, 2014 formulated IA approach with the intention of enhancing the password pattern by employing an additional security layer. In this approach, three security checks were undergone in two steps. In the initial step, the matching of the mobile angle that the user holds the

mobile was carried out. In the second step, the time taken to draw the pattern, as well as pattern check, was performed.

Shankar& Karan,2019 deployed Deep Auto Encoder and Softmax Regression Model. It authenticates users based on their behavioural characteristics. Continuous authentication is easy on the user's brain because there is nothing to memorise. In this work, ten different sets of data from ten different users in 12 different scenarios were collected in order to identify the users. As a result, a large amount of data will be stored on the dataset that must be normalized. Using two different normalisation techniques, namely,Normalization using Min-Max and Z-score. The DAE-SR achieved 0.950 percent and 0.970 percent accuracy in predicting users in various states (walking and sitting).

Gaber *et al.,*2020 developed an efficient authentication method that provides implicit authentication for smartphone users while avoiding the additional cost of special hardware and addressing the smartphone's limited capabilities. These techniques are evaluated using the random forest classifier. It is also used in our authentication method to complete the classification task. The experimental results using a public dataset revealed that the filter-based technique is the best.The selection of features to create an implicit authentication method for the smartphone environment. Itshowed accuracy results of around 97.80 percent while using only 25 features out of 53 features. To authenticate users, mobile resources are used.

2.2 Review

The literature has come out with several techniques for behavior based authentication of smart phones as per Table 1. The mobile phone authentication poses various challenges that need rectification for the future. Some of the benefits and drawbacks in smart phone authentication are portrayed below. In K-NN and SVM (Shen *et al.,* 2018), the authentication as well as re- authentication accuracy is high. But, it suffers from the drawback like high EER. In HMOG (Sitová *et al.,* 2016), EER while walking as well as sitting is low and the sensor sampling rate is also low. The major shortcoming of this model is the lack of cross-device interoperability. A higher acceptance rate is achieved with ANSWERAUTH, but the training of ANSWERAUTH is difficult (Buriro *et al.,* 2019). Further, SVM has Low FRR and FAR as an advantage (Lu & Liu, 2015). Apart from this, the level of accuracy is low, and the authentication process is slower. ShakeIn (Zhu *et al.,* 2017), has the advantage of low average equal error rate and high reliability under varying transport conditions. The major drawback of this model is its lack of consideration to both physiological and behavioral characteristics of the user. With SLR (Cao & Chang), the detecting illegitimate user's rate is high, and it also achieves a higher trade-off between usability and security. The major shortcoming of this model lies in high time consumption in authentication. With PLDA (Yang *et al.,*), there take place more accurate and precious feature extraction, and here the major cons lie in the unsolved behavior deviation. The Markov-based decision procedure (Agrawal & Patidar, 2014) has higher authentication accuracy and low FP and FN rate. The main disadvantage of this model is more expensive and Slow identification process. Thus, the necessity of designing an optimal authentication model becomes essential.

3. PROPOSED SMART PHONE AUTHENTICATION MODEL

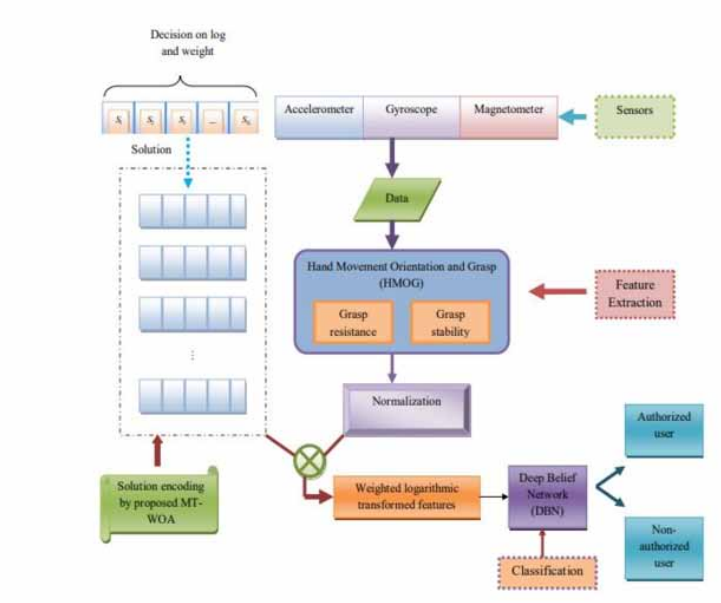
3.1 Architecture of Proposed Model

The presently available smart phone authentication mechanisms such as PINs, graphical passwords, and fingerprint scans are limited in terms of security. To override the challenges faced by the traditional smart phone authentication techniques, the proposed smart phone authentication model is developed as per Fig. 1. This model follows two major phases (i) Feature extraction (ii) Weighted logarithmic transformation (iii) Classification. Initially, the features relating the touches/ gestures of the smart phone users are extracted using HMOG by grasp resistance and grasp stability. The HMOG features are further subjected to normalization to map the features within the particular range of 0.01 to 0.99.

Table.1 Features and challenges of conventional behaviour-based smart phoen authentication

Author [citation]	Adopted methodology	Features	Challenges
Shen *et al.,* 2018	K-NN and SVM	High authentication and re-authentication accuracy. High discrimination accuracy	High EER Infeasible to PAP as well as to AWC
Sitová *et al.,* 2016	HMOG	Low EER while walking and sitting Low sensor sampling rate	Not applicable under stringent constraints. Lack of cross-device interoperability
Buriro *et al.,* 2019	Answerauth	High acceptance rate Highly robust against the possible mimicry attacks.	Not consideration on and seamless detection of the users' current activity The training of ANSWERAUTH is difficult.
Lu & Liu, 2015	SVM	Low FAR Low FRR	Low accuracy Tedious process
Zhu *et al.,* 2017	ShakeIn	Low average equal error rate Highly reliable even under varying transport conditions	High FPE especially under shoulder-surfing attacks. No consideration on both physiological and behavioral characteristics
Cao & Chang	HMM and SLR	Detecting illegitimate users rate is high High trade-off between usability and security	Low effectiveness and efficiency High time consumption and high battery power usage
Yang *et al.,*	PLDA	More accurate and precious feature extraction High compatibility	Behavior deviation is left unsolved Time consumption is high
Agrawal & Patidar, 2014	Markov-based decision procedure	High accuracy Low FP and FN rate	More expensive Slow identification process
Shankar& Karan, 2019	Deep Auto Encoder and Softmax Regression Model	High Accuracy	High consumption time
Gaber *et al.*,2020	Authentication Method	It requires less memory and processing time is also reduced.	It is not applicable to other datasets. Only suitable for the same number of datasets.

Figure 1. Diagrammatic representation of the proposed behaviour based intelligent, smart phone authentication mode



In the weighted logarithmic transformation phase, the normalized data has to be multiplied with the weight, followed by logarithmic transformation. As a main contribution, the decision-making process associated with the logarithmic, and weight selection depends on a new optimization model. Here, the improved WOA termed as MT-WOA is proposed for optimizing the transformation plane. Further, the final feature vector is subjected to DBN, which recognizes the user as authorized or not.

3.2 HMOG-Based Feature Extraction

This research makes use of two types of HMOG features: grasp resistance and grasp stability (Sitová *et al.,* 2016). The computation of these features is accomplished using the data gathered from three different sensors, namely accelerometer, gyroscope, and magnetometer. Typically, during the taping of the screen, the subtle micro-movements, as well as the orientation patterns of users, are captured by the HMOG features. In this research, HMOG features are extracted from the signals during the tap events.

Grasp Resistance Features: The resistance of a hand grasps corresponding to the forces exhibited by the user at the time of touch/ gesture events are measured in the grasp resistance. The resistance is quantified as a change in movement, orientation and magnetic field as per the readings gathered from the accelerometer, gyroscope and from magnetometer, respectively during the tap event. Let the sensor readings in x, y and z axes be represented as X, Y and Z, respectively, which is in time series format. Let $Z_1, Z_2, \cdots, Z_m$ be the individual sensor readings collected during the time $l_1, l_2 \cdots, l_m$ in z axis. Assume H as the time series of the magnitude of sensor readings, in which each element H_o is computed using Eq. (1).

$$H_o = \sqrt{y} \tag{1}$$

Moreover, l_{start} and l_{end} specify the start and the end time of the tap event, respectively. In between l_{start} and l_{end}, the time at which maximum reading recorded by the sensor is manifested as $l_{tap-max}$ .The time when the stability is reached after the end of the tap movement is represented as l_{min}. The centre of 100ms window before and after the tap event is represented as $l_{center-before}$ and $l_{center-after}$, respectively. The average sensor readings before and after recording the sensor readings in 100ms window is represented as $Before_{avg100ms}$ and $After_{avg100ms}$, respectively. During the tap events, the average of readings is depicted as Avg_{tap}.

Moreover, from the accelerometer, gyroscope, and magnetometer, the five grasp resistance features are extracted in the four dimensions viz. magnitude, x., y and z axes. Totally, 5×3×4=60 features are extracted. For easiness, the grasp resistance feature on z axis is only extracted here. The steps utilized for determining the grasp resistance features is given below (Sitová *et al.,* 2016).

(i) At every taps, measure the mean Z.
(ii) During each trap evaluate the standard deviation of Z.
(iii) In Z readings, evaluate the difference in Z which the difference is between $Before_{avg100ms}$ and $After_{avg100ms}$ tap events.
(iv) Evaluate the net change caused by a tap in Z readings as $Avg_{tap} - After_{avg100ms}$.
) Observe the maximum change caused by a tap in Z readings and this feature is calculated as $Avg_{tap} - Before_{avg100ms}$.

Grasp Stability Features: The stability features portrays the quantification of the perturbations that are generated by the finger-force tent to disappear, when the event is completed. The steps followed in grasp stability features computation is exhibited as follows.

(i) After the tap event, the time duration for achieving the movement as well as orientation stability is measured as $lend_{min}$.

(ii) For the mean sensors, the normalized time duration is calculated before and after tap event as per Eq. (2).

$$\Delta_{duration} = \frac{l_{center-after} - l_{center-before}}{After_{avg100ms} - Before_{avg100ms}} \tag{2}$$

(iii) Calculate the normalized time duration for mean sensor values in response to tap event is accomplished as shown in Eq. (3).

$$\Delta_{\max-avg} = \frac{l_{center-after} - l_{tap-max}}{After_{avg100ms} - Avg_{tap}} \tag{3}$$

From, three sensors and four sensor readings (H , X , Y and Z) three grasp features are extracted. From here, total of 3×3×4=36 features is obtained.

Hence the extracted two sets of features can be represented as $F_n = F_{1,} F_{2,\cdots} F_{N_t}$, where $n = 1,2,\cdots, N_t$. The total number of features is represented as N_t .

3.3 Deep Belief Network-Based Classification

The weighted logarithmic transformed features are applied to DBN classifier, for detecting the authorized users. DBN (Hua *et al.,* 2015) was introduced in 1986 by Smolensky, and it comprises of input layer, output layer, and the hidden layer. The input layer holds the visible neurons, and the output layer has the hidden neurons. There exists an interrelationship in between the hidden neurons as well as input neurons and lacks in relationship between hidden neurons and visible neurons. In between the visible and hidden neurons, there is an exclusive connection in a symmetric manner. For each input, the corresponding output can be obtained from DBN with the help of the stochastic neuron model. In addition, the Boltzman network is utilized in DBN with the aim of achieving the outcomes in a probabilistic manner. DBN outcome takes the binary form and it is represented as r . Eq. (4) and Eq. (5) manifests the probability $\left(K_p\left(\delta\right)\right)$, which is in the sinusoidal function. The probability noise level is curtailed by the pseudo temperature parameter L , when $L > 0$. Moreover, Eq. (6) exhibits the stochastic model of the probability in a deterministic form.

$$r = \begin{Bmatrix} 1 & with K_p\left(\delta\right) \\ 0 & with 1 - K_p\left(\delta\right) \end{Bmatrix} \tag{4}$$

$$K_{p}\left(\delta\right)=\frac{1}{1+e^{\frac{-\delta}{L}}} \tag{5}$$

$$\lim_{L\to 0^{+}} K_{p}\left(\delta\right)=\lim_{L\to 0^{+}}\frac{1}{1+e^{\frac{-\delta}{L}}}=\begin{cases}0 & for \quad \delta<0\\ \frac{1}{2} & for \quad \delta=0\\ 1 & for \quad \delta>0\end{cases} \tag{6}$$

For configuring the neuron states h of the Boltzmann machine, the energy factor plays a crucial role and the mathematical formula for energy of Boltzmann machine is represented in Eq.(7). In addition, the weight between the neuron and the biases of the neurons in DBN is manifested as $M_{i,j}$ and α. The joint configuration in between the visible q as well as hidden neurons d in terms of energy is indicated in Eq. (8), Eq. (9), Eq. (10) and Eq. (11). The binary states of the visible state and the hidden state i and j are represented as h_{i} and h_{j}, respectively.

$$Eg\left(h\right)=-\sum_{i<j}M_{i,j}h_{i}h_{j}-\sum_{i}\alpha_{i}.h_{i} \tag{7}$$

$$\Delta Eg\left(h_{i}\right)=\sum_{j}h_{j}M_{i,j}+\alpha_{i} \tag{8}$$

$$Eg\left(\vec{q},\vec{d}\right)=-\sum_{(i,j)}M_{i,j}q_{i}d_{j}-\sum_{i}q_{i}u_{i}-\sum_{j}d_{i}g_{j} \tag{9}$$

$$\Delta Eg\left(q_{i},\vec{d}\right)=\sum_{j}M_{ij}d_{j}+u_{i} \tag{10}$$

$$\Delta Eg\left(\vec{q},d_{j}\right)=\sum_{j}M_{ij}q_{j}+g_{j} \tag{11}$$

The learning pattern of RBM is considered as the weight parameters obtained from the encoded probability distribution of the input data. The weighting assignment of RBM is determined as per Eq. (12) and here the assigned probabilities can be maximized by RBM itself. The input visible vector is denoted as q. Moreover, as per the energy function shown in Eq. (13), RBM has the capability of assigning probability to each unique visible as well as hidden vector. The assigned weight is represented as G_{e} and the training set is indicated as O. Then, by adding energy of all the possible states of the neurons, the partition function $\left(V\right)$ is obtained as per Eq. (14).

$$G_e = \max_{\hat{G}} \prod_{q \in O} P\left(\vec{q}\right) \tag{12}$$

$$P\left(\vec{q},\vec{d}\right) = \frac{1}{V} e^{-Eg\left(\vec{q},\vec{d}\right)} \tag{13}$$

$$V = \sum\nolimits_{\vec{q}\vec{d}} e^{-Eg\left(\vec{q},\vec{d}\right)} \tag{14}$$

Moreover, during the evaluation of energy between the visible or hidden neuron, the standard Boltzmann Machine do not depend on the visible or hidden neurons, whereas the RBM does. RBM is efficient in data reconstruction, but lacks in data classification, hence unsupervised learning is accomplished to train RBM. The contrastive divergence (CD) is employed, since the time for RBM to get converged with the prescribed model is high. The training patters MLP layer makes use of the hidden neurons as the input and this is similar to RBM layer. The training process of MLP is accomplished using the training patterns $\left(W^b, U^b\right)$. W^b and U^b represents the output and desired output, respectively. Moreover, b represent the training pattern within the limit $1 \le b \le B$. Eq. (15) specifies the error between the output vector and the desired output.

$$Err = U^b - W^b \tag{15}$$

The steps involved in the CD algorithm are listed below.

The binary input is assumed by selecting the training samples q and clasping them on to the visible neurons.

The probability of the hidden neurons P_d is computed by multiplying visible vector q with the weight matrix G and this is represented as $\left(P_d = \psi\left(G.q\right)\right)$ on the basis of Eq. (16).

$$p\left(d_j \to 1 \mid \vec{q}\right) = \psi\left(g_j + \sum\nolimits_i q_i M_{i,j}\right) \tag{16}$$

From the probability P_d , the hidden states d are sampled.

The positive gradient ζ^+ is the outer product of q and P_d and it is computed as $\zeta^+ = q.p_d^T$.

From the hidden state $\hat{d}$, the reconstruction of the visible state q' takes place as per Eq. (17). Further, the reconstruction of the visible state q' takes place by resampling the hidden states $\hat{d}$.

$$p\left(q_i \to 1 \mid \vec{d}\right) = \psi\left(u_i + \sum\nolimits_j d_j M_{i,j}\right) \tag{17}$$

The negative gradient ζ^- is the exterior product of vectors q' and $\hat{d}$ .The negative gradient is calculated as $\zeta^- = q'.\hat{d}^T$.

From the positive gradient ζ^+ , the negative gradient ζ^- is subtracted in order to achieve the weight updates. This updating of weights is accomplished as per Eq. (18)

$$\Delta G = \chi\left(\zeta^{+} - \zeta^{-}\right) \tag{18}$$

With the newly obtained values, the updating of weights take place is shown in Eq.(19)

$$\Delta M_{i,j}^{*} = \Delta M_{i,j} + M_{i,j} \tag{19}$$

4. OPTIMAL WEIGHTED LOGARITHMIC FEATURES FOR SMART PHONE AUTHENTICATION MODEL

4.1 Weighted Logarithmic Transformation

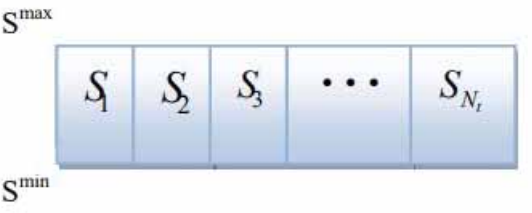
The extracted HMOG features are subjected for weighted logarithmic scale transformation. Initially, the extracted features are normalized within the range 0.01 to 0.99. Here, 0.01 is selected to avoid infinity, and 0.99 is selected to avoid zero. After normalization, the transformation plane optimization is adopted. The main intention of this optimization is to decide the logarithmic function and the weight to be multiplied with features. Since the solution set increases the solution length, both the decision is taken within one variable. The solution generated here ranges in between 0.0 to 1.9 as per Fig.2.

Each solution variable includes both the decision regarding log or non log and the value of the weight that is to be multiplied with the features. As mentioned in Fig. 2, the solution is represented as S_j, where $j = 1, 2, 3, \cdots, N_t$. The length of the solution is the total number of features, which is denoted as N_t. The bounding limit of solution is S^{min} and S^{max}. The real number of solution variable 0 or 1 represents non log or log transformation and the decimal portion indicates weight. For example: In 0.0, 0 in the integer place denotes the non-log transformation and the .0 in the decimal place depicts the weights. In the same way, in 1.9, the 1 in the integer position indicates the log transformation and 0.9 in the decimal position is taken as weight. The maximum and the minimum weights are represented as w^{max} and w^{min}, respectively. Thus, the solution bound is specified as per Eq. (20) and Eq. (21).

$$S^{min^{min}} \tag{20}$$

$$S^{min^{max}} \tag{21}$$

Figure 2. Representation of generated solution for encoding



4.2 Objective Model

In the solution encoding, the fitness evaluation is carried out after transforming the solution into normal form (i.e, separation of log and weight decision). While evaluation, the solution is split to two forms based on Eq. (22), from which the transformed data is obtained concerning both logarithmic and weight decisions. In Eq. (22), d_{ij} indicates the input data, S_j indicates the input solution, $\hat{S}_j$ indicates the separated solution on logarithmic decision, and $\overline{S}_{ij}$ indicates the separated solution on weight decision.

$$DT_{ij} = \hat{S}_j \log\left(d_{ij} \times \overline{S}_{ij}\right) + \left|\left(1 - \hat{S}_j\right)\left(d_{ij} \times \overline{S}_{ij}\right)\right| \tag{22}$$

$$\hat{S}_j = \begin{cases} 1; if S_j \geq 1 \\ 0; else \end{cases} \tag{23}$$

$$\overline{S}_{ij} = S_j - \hat{S}_j \tag{24}$$

The main objective function of the proposed smart phone authentication model is to minimize the training error between the actual and predicted outcome of DBN as shown in Eq. (25), where the computation of Err is based on Eq. (15).

$$Obj = \min(Err) \tag{25}$$

4.3 Conventional Whale Optimization Algorithm

The Australian researches Mirjalili and Lewis had introduced WOA based on the inspiration gained from the hunting mechanism of the hump-back whales (Mirjalili & Lewis, 2016). The bubble-net- feeding mechanism is an interesting obsession as it has the special hunting method of the whales. The upcoming section discusses about the 3 major stages of hunting in the hump-back whales.

(i) Encircling Prey: The hump-back whales localize their prey and then encircle the prey; this encircling is an exclusive capability of the whales. Eq. (26) and Eq. (27) represents the exclusive encircling of prey mechanism. Here, a refers to the current iteration and the coefficient vector are depicted as J and Q . The term S^* portrays the best solution obtained so far. In addition, S depicts the position vector. The absolute value and element-by-element multiplication are represented as $|.|$ and ".", respectively. The mathematical formula for vectors J and Q are represented in Eq. (28) and Eq. (29), respectively. In both the exploration and exploitation phase, the value of f keeps linearly decreasing from 2 to 0 over the iterations and s is a random vector in [0,1].

$$R = \left|QS^*\left(a\right) - S\ \left(a\right)\right| \tag{26}$$

$$S\left(a+1\right) = S^*\left(a\right) - J \cdot R \tag{27}$$

$$J = 2f.s - f \tag{28}$$

$$Q = 2.s \tag{29}$$

(ii) Bubble-Net Attacking Method (Exploitation Phase): This is the most important phase as it encloses the Shrinking encircling mechanism and Spiral updating position.
   (a) Shrinking encircling mechanism: By decreasing the value of f, the shrinking mechanism is achieved. Moreover, in the interval $\left[-f, f\right]$ the value of J is random, in which m is decreasing from 0 to 2 over the course of iterations. Then, the new position of the search agent can be obtained in between the original position and the current best agent by setting the value of J in the interval $\left[-1, 1\right]$.
   (b) Spiral updating position: The mathematical formula corresponding to the spiral updating of the position of the whales is depicted in Eq.(30) and Eq. (31), in which the distance between the whale and the prey is manifested as R and the dimensions of the logarithmic spiral is a constant value and it is represented as c. In addition, k is a random number in the limit [−1, 1]. Eq. (32) exhibits the final update formula of WOA, where φ is a random number in the interval [0, 1].

$$S\left(a+1\right) = R'e^{ck}.Cos\left(2\pi k\right) + S*\left(a\right) \tag{30}$$

$$R = \left|S^{*}\left(a\right) - S\left(a\right)\right| \tag{31}$$

$$S\left(a+1\right) = \begin{cases} S*\left(a\right) - J.R for & \varphi < 0.5 \\ R'.e^{ck}.Cos\left(2\pi k\right) + S*\left(a\right) for & \varphi \geq 0.5 \end{cases} \tag{32}$$

(iii)Search for Prey (Exploration Phase): On the basis of Eq.(33) and Eq.(34), all other whales update their position by considering the randomly chosen individual whale. The random position vector selected from the current population is denoted as $S_{(rand)}$.

$$R = \left|QS_{(rand)} - S\right| \tag{33}$$

$$S\left(a+1\right) = S_{(rand)} - J.R \tag{34}$$

Proposed MT-WOA

The transformation plane is optimized with the help of proposed optimization, MT-WOA. In fact, the existing WOA algorithm suffers from the drawbacks of local optima stagnation and slow

Algorithm 1: Conventional WOA (Mirjalili & Lewis, 2016)

The whale population $S_b, whereb = 1,2,..,v$ **is initialized**
For each individual search agent, evaluate the fitness
S^* is the best search agent
While $\left(a < \max imimcountofiterations\right)$
For each search agent
m, J, Q, k, ϕ are updated
If 1 $\left(\phi < 0.5\right)$
If 2 $\left(\left\|J\right\| < 1\right)$
The current search agent's position is updated by using Eq.(27)
Else if 2 $\left(\left\|J\right\| \geq 1\right)$
The random agent $S_{(rand)}$ is selected
The current search agent's position is updated by using Eq. (34)
End if 2
Else if 1 $\left(\phi \geq 0.5\right)$
The current search agent's position is updated by using Eq.(30)
End if 1
End for
Evaluate whether any search agent has gone beyond the search space and amend it
Fitness of individual search agent is evaluated.
In case of obtaining a better solution, update S^*
$a = a + 1$
End while
Return S^*

convergence speed. In order to overcome these drawbacks, the current model intends to develop an improved WOA algorithm referred as MT-WOA. In the conventional WOA, the value of a random number φ is compared over the threshold value to decide the update formula, which is fixed as 0.5. To improvise the performance, the proposed MT-WOA computes the threshold value Th based on Eq. (37). Moreover, at iteration $a = 0$, the value of φ is fixed at 0.5 like in conventional WOA. From the next iteration, Eq. (33) tries to compute the Th value, where the number of solutions whose

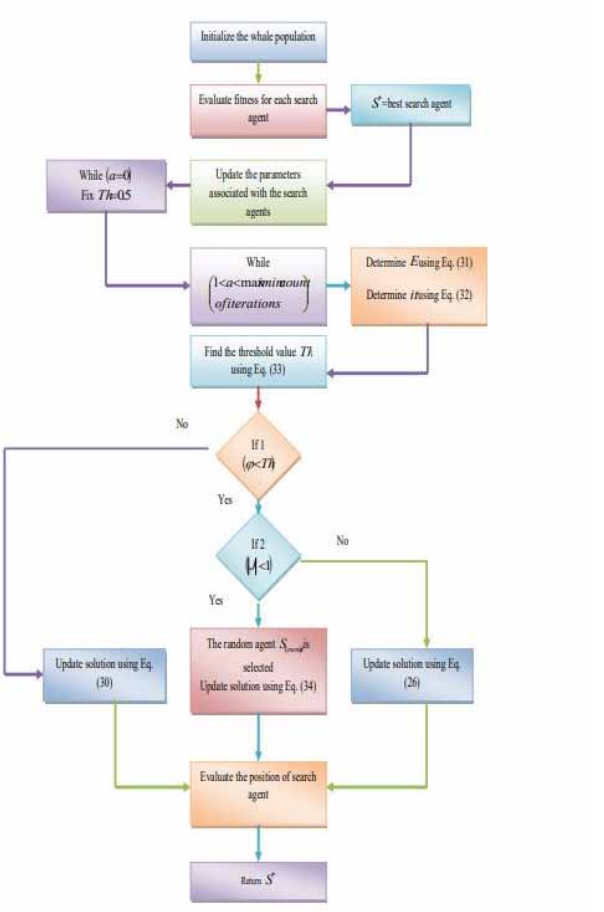
current fitness f is better than the old fitness f^{old} (minimized error) is determined by E using Eq. (35). Further, the term It is determined using Eq. (36), where v indicates the total number of solutions.

$$E = length\left(find\left(f < f^{old}\right)\right) \tag{35}$$

$$It = 0.9 \times \left(\frac{E}{v}\right) \tag{36}$$

$$Th = 0.05 \times \left(f \,/\, mean\left(f\right)\right) + it \tag{37}$$

Figure 3. Flow chart of the proposed smart phone authentication model



Algorithm 2: Proposed MT-WOA

The whale population $S_b, whereb = 1,2,..,v$ is initialized

For each individual search agent, evaluate the fitness

S^* is the best search agent

For each search agent

m, J, Q, k, ϕ are updated

While $\left(a = 0\right)$

Fix $Th = 0.5$

While $\left(1 < a < \max imimcountofiterations\right)$

Determine E using Eq. (35)

Determine it using Eq.(36)

Find the threshold value Th using Eq.(37)

If 1 $\left(\phi < Th\right)$

If 2 $\left(\left|J\right| < 1\right)$

The current search agent's position is updated by using Eq.(26)

Else if 2 $\left(\left|J\right| \geq 1\right)$

The random agent $S_{(rand)}$ is selected

The current search agent's position is updated by using Eq.(34)

End if 2

Else if 1 $\left(\phi \geq Th\right)$

The current search agent's position is updated by using Eq.(30)

End if 1

End for

Evaluate whether any search agent has gone beyond the search space and amend it

Fitness of individual search agent is evaluated.

In case of obtaining a better solution, update S^*

$$a = a + 1$$

End while

Return S^*

5. RESULTS AND DISCUSSIONS

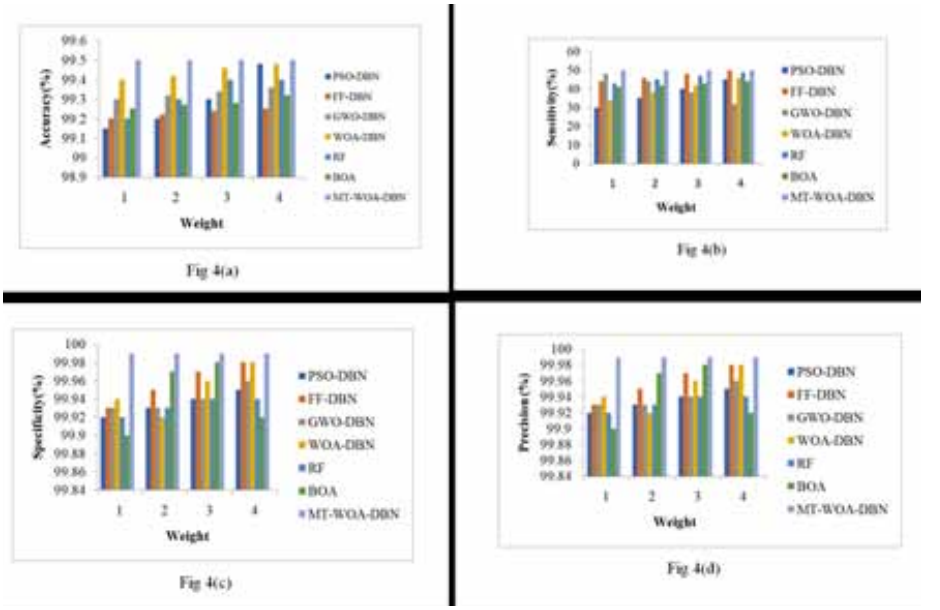
5.1 Experimental Setup

The proposed intelligent smart phone authentication model using MT-WOA+DBN was implemented in MATLAB, and the outcome of each of the analysis is observed. In the current research work, the dataset was collected from (https://www.cs.wm.edu/~qyang/hmog.html: Access data 2019-03-16; Sitová *et al.,* 2016). The data collection tool for the smart phones authentication process to record real-time touch, key press data as well as sensors of user's interaction with the phone were developed. The data gathered from the smart phone usage scenarios are (1) document reading (2) text production (3) navigation on a map to locate a destination. For the analysis, the population size was set at 10, and the count of iterations was 25. After the modeling, the performance of MT-WOA+DBN model was compared over the conventional models like PSO+DBN (Tanweer *et al.,* 2015), FF+DBN (Fister *et al.,* 2013), GWO+DBN (Wu *et al.,* 2012) and WOA+DBN (Mirjalili & Lewis, 2016) in terms of accuracy, specificity, Precision, FPR, FNR, NPV, FDR, F1-score and MCC. The entire performance analysis outperforms MT-WOA model over other existing models.

5.2 Performance Analysis by Varying the Weighting Factor

Based on the proposed model, the weight in weighted logarithmic phase is fixed as minimum bounding limit=0, and maximum bounding limit=0.9. For further analysis, the maximum bounding limit of weighting factor is varied to four sets, namely, weighting factor 1=0.1, weighting factor 2=1, weighting factor 3=10, and weighting factor=100. Fig. 4 exhibits the performance analysis of MT-WOA-based smart phone authentication model over the existing model by varying the weighting factor from 1, 2, 3 and 4. In Fig. 4(a), the accuracy of MT-WOA model at the weighting factor 2 is 0.89% better than PSO+DBN, 0.54% better than FF+DBN, 0.44% better than GWO+DBN, 0.51% better than WOA+DBN, 0.48% better than RF and 0.59% better than BOA. The sensitivity of MT-WOA+DBN model in Fig. 4(b) at the weighting factor 2 is 60%, 2%, 10%, 4%, 8% and 4% superior to the conventional models like PSO+DBN, FF+DBN, GWO+DBN, WOA+DBN, RF and BOA,

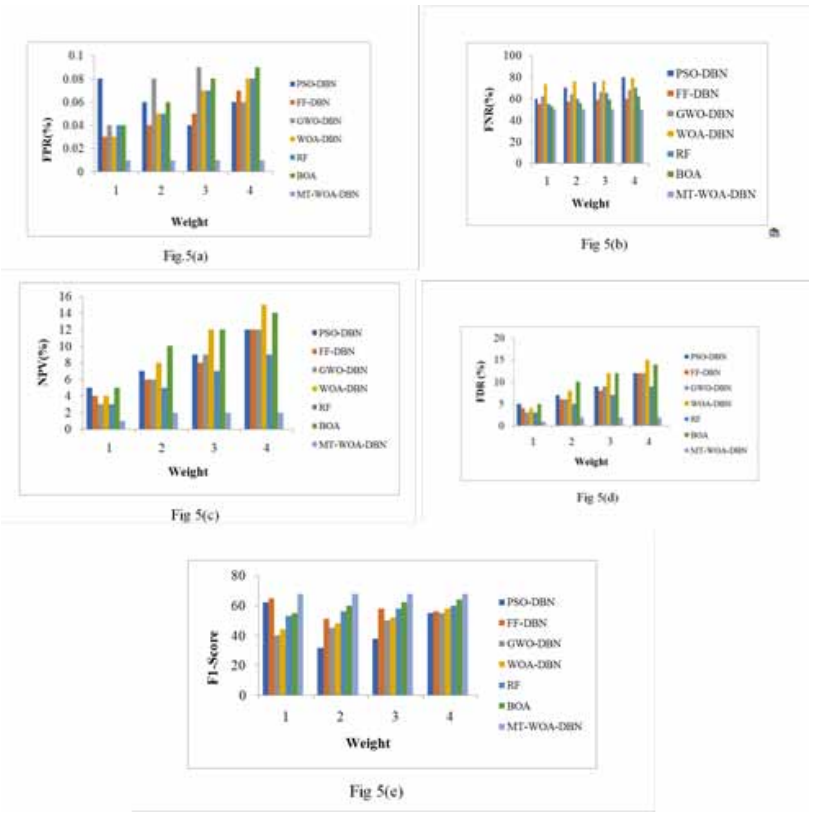
Figure 4. Performace analysis of MT-WOA+DBN model over the existing models by varying the weighting factors focusing on (a) Accuracy (b) Sensitivity (c) specificity (d) Precison



respectively. The specificity of MT-WOA+DBN model is 0.08%, 0.018%, 0.02%, 0.04%, 0.06% and 0.08% better than the state-of-art model like PSO+DBN, FF+DBN, GWO+DBN, WOA+DBN, RF and BOA, respectively at the weighting factor of 1 in Fig. 4(c). Then, an enhancement of 15%, 4%, 3%, 8.6%, 4% and 3% is recorded by MT-WOA+DBN model over the extant model like PSO+DBN, FF+DBN, GWO+DBN, WOA+DBN, RF and BOA,respectively in terms of precision at the weighting factor 1 in Fig. 4(d).

From Fig. 5(a), FPR of MT-WOA+DBN model at the weighting factor 1 is 73.75%, 4.5%, 8.6%, 47.5%, 6% and 8% better than the conventional model like PSO+DBN, FF+DBN, GWO+DBN and WOA+DBN, RF and BOA, respectively. The weighting factor is fixed at 2 in Fig. 5(b) and FNR of MT-WOA+DBN model is 60%, 4%, 8.2%, 9%, 7% and 12% better than the conventional models like PSO+DBN, FF+DBN, GWO+DBN, WOA+DBN, RF and BOA,respectively. Moreover, NPV of MT-WOA+DBN model at the weighting factor 1 in Fig. 5(c) is 0.08%, 0.01%, 0.02%, 0.04%, 0.06% and 0.08% better than the state-of-art model like PSO+DBN, FF+DBN, GWO+DBN, WOA+DBN, RF and BOA,respectively. In Fig. 5(d), FDR of MT-WOA+DBN model is 86.6%, 33.3%, 50%, 75%, 45% and 52% superior to PSO+DBN, FF+DBN, GWO+DBN, WOA+DBN, RF and BOA, at the weighting factor 1. An enhancement of 16.6%, 3.8%, 3%, 12.8%, 3.5% and 6% is recorded at the weighting factor of 1 in Fig. 5(e) by MT-WOA+DBN model over the conventional models like PSO+DBN, FF+DBN, GWO+DBN, WOA+DBN, RF and BOA,respectively in terms of F1-score. MCC of MT-WOA+DBN model is 35.7%, 5.71%, 2.8%, 7.14%, 4% and 8% better than the conventional

Figure 5. Performace analysis of MT-WOA+DBN model over the existing models by varying the weighting factors focusing on (a) FPR (b) FNR (c) NPV (d) FDR (e) F1-score (j)MCC

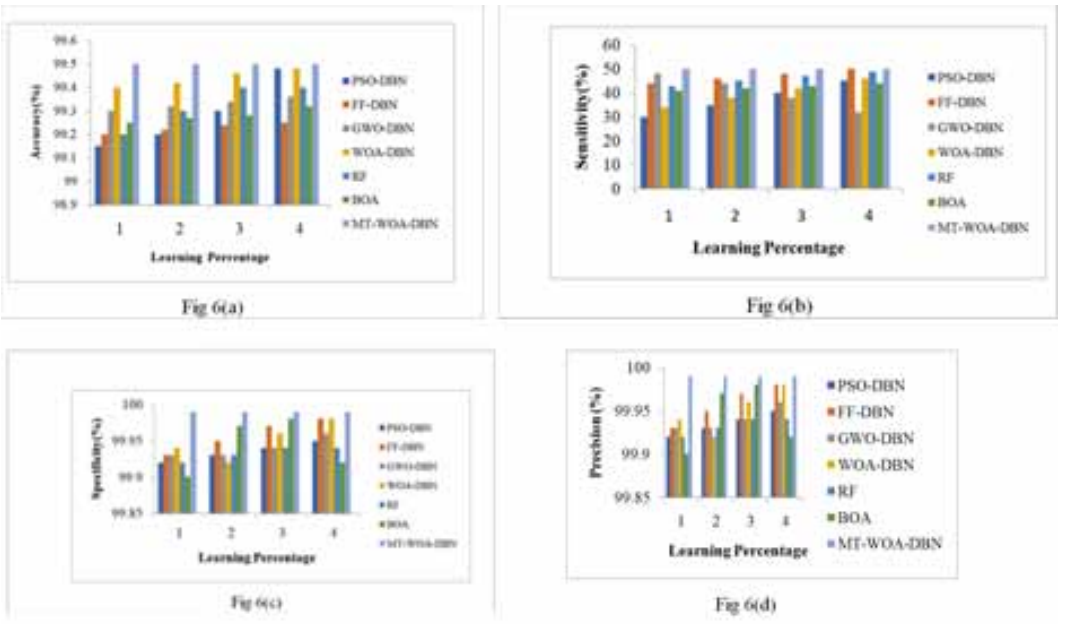


model like PSO+DBN, FF+DBN, GWO+DBN, WOA+DBN, RF and BOA, at the weighting factor 2 in Fig. 5(f).Thus from the analysis, it is clear that the proposed model outperforms the existing model in terms of all the performance metrics, while varying the weighting factor.

5.3 Performance Analysis by Varying the Learning Percentage

The performance analysis of MT-WOA+DBN-based smart phone authentication models over the existing models with respect to different learning percentage is shown in Fig. 5. Here, the learning percentage is varied from 40, 60 and 80. The accuracy of MT-WOA+DBN model at the learning percentage of 80 is 0.6%, 0.55%, 0.5%, 0.1%, 0.66% and 0.58%, better than the existing models like PSO+DBN, FF+DBN, GWO+DBN,WOA+DBN, RF and BOA, respectively as per Fig. 6(a). The sensitivity of MT-WOA+DBN model in Fig. 6(b) at the learning percentage of 80 is 11.1%, 4%, 6%, 60%, 12% and 12% better than conventional models like PSO+DBN, FF+DBN, GWO+DBN, WOA+DBN, RF and BOA,respectively. In Fig. 6(c), the specificity of MT-WOA+DBN model at the learning percentage of 80 is 0.035%, 0.01%, 0.015%, 0.01%, 0.05% and 0.04% superior to traditional model like PSO+DBN, FF+DBN, GWO+DBN, WOA+DBN, RF and BOA,respectively. Moreover, at the learning percentage of 65, the precision of MT-WOA+DBN model is 4%, 3%, 4.3%, 5%, 4.6% and 5% better than state-of-art model like PSO+DBN, FF+DBN, GWO+DBN WOA+DBN, RF and BOA, respectively as per Fig. 6(d).

Figure 6. Performace analysis of MT-WOA+DBN model over the existing models by varying the learning focusing on (a) Accuracy (b) Sensitivity (c) specificity (d) Precison



In Fig. 7(a), an improvement of 50%, 48%, 56%, 45% and 54% is recorded by MT-WOA+DBN model over the existing model like PSO+DBN, FF+DBN, GWO+DBN, RF and BOA, in terms of FPR at the learning percentage of 55. The learning percentage is fixed at 90 in Fig. 7(b) relating to FNR and MT-WOA+DBN model shows an enhancement of 9.09%, 7.4%, 6.8%, 37.5%, 42% and 36% over PSO+DBN, FF+DBN, GWO+DBN, WOA+DBN, RF and BOA,respectively. At the

learning percentage of 85, NPV of MT-WOA+DBN model in Fig. 7(c) is 0.025%, 0.005%, 0.03%, 0.02% and 0.05% better than the traditional models like PSO+DBN, FF+DBN GWO+DBN, RF and BOA, respectively. Moreover, in Fig. 7(d), FDR of MT-WOA+DBN model at the weighting factor 85 is 71%, 33.33%, 31%, 35% and 40% superior to state-of-art models like PSO+DBN, FF+DBN, GWO+DBN, RF and BOA, respectively. In Fig. 7(e), at the learning percentage of 80 in MT-WOA+DBN model is 11.7%, 10%, 9%, 57.14%, 8% and 13% superior to the conventional models like PSO+DBN, FF+DBN, GWO+DBN, WOA+DBN, RF and BOA,respectively in terms of F1- score. MCC of MT-WOA+DBN model exhibits an improvement of 28.5% over PSO+DBN, 28.5% over FF+DBN, 7.1% over GWO+DBN, 2.8% over WOA+DBN, 9% over RF and 12% over BOA at the learning percentage of 40 in Fig. 7(f). From the performance analysis of MT-WOA+DBN model, it is clear that the proposed model is superior to the existing models in terms of performance measures by varying the learning percentage.

Figure 7. Performace analysis of MT-WOA+DBN model over the existing models by varying the weighting factors focusing on (a) FPR (b) FNR (c) NPV (d) FDR (e) F1-score (f)MCC

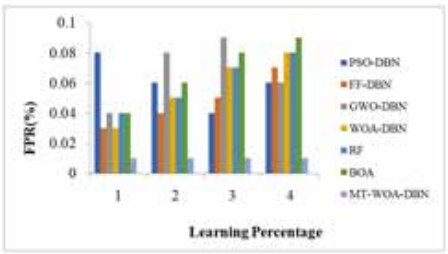


Fig 7(a)

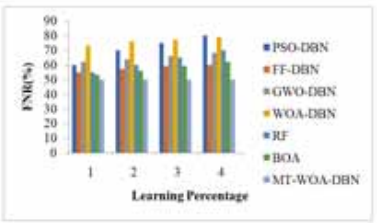


Fig 7(b)

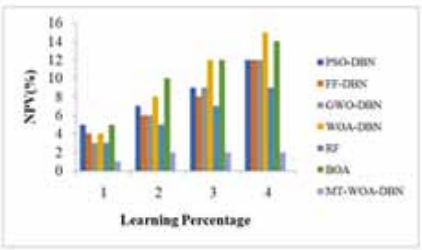


Fig 7(c)

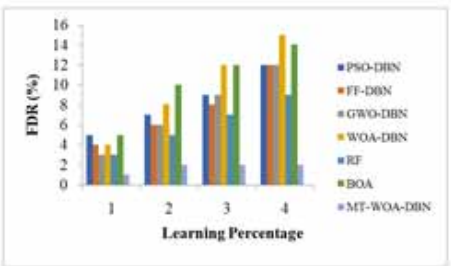


Fig 7(d)

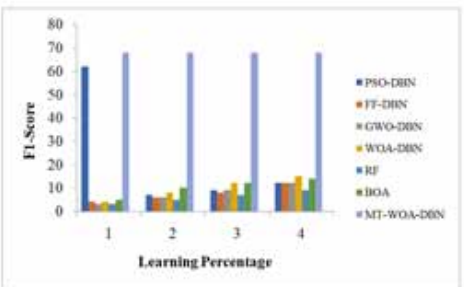


Fig 7(e)

5.4Overall Performance Analysis

Table II portrays the performance evaluation of MT-WOA+DBN model over the existing models in terms of accuracy, sensitivity, specificity, precision, FPR, FNR, NPV, FDR, F1-Score and MCC. Here, the accuracy of MT-WOA+DBN model is 0.07%, 0.003%, 0.007% and 0.02% superior to the existing models like PSO+DBN, FF+DBN, GWO+DBN, and WOA+DBN, respectively. The sensitivity of MT-WOA+DBN model is 0.28% superior to the traditional GWO+DBN. An enhancement of 0.07%, 0.003%, 0.006%, and 0.03% is recorded by MT-WOA+DBN model over the extant models like PSO+DBN, FF+DBN, GWO+DBN and WOA+DBN, respectively in terms of specificity. The precision of the projected model is 12.8% better than PSO+DBN, 0.55% better than FF+DBN, 1.10% better than GWO+DBN and 5.49% better than WOA+DBN. Further, FPR of MT-WOA+DBN model is 89.8%, 24.9%, 39.9% and 77.7% superior to the traditional models like PSO+DBN, FF+DBN, GWO+DBN, and WOA+DBN, respectively. MT-WOA+DBN model shows an improvement of 0.27% over the GWO+DBN model in terms of FNR. An improvement of 0.07%, 0.003%, 0.006%, and 0.03% is recorded by MT-WOA+DBN model over the traditional model like PSO+DBN, FF+DBN, GWO+DBN and WOA+DBN, respectively in terms of NPV. Then, MT-WOA+DBN model shows an enhancement of 88.3% by PSO+DBN, 24.5% by FF+DBN, 39.5% by GWO+DBN and 76.4% by WOA+DBN in terms of FDR. F1-score of MT-WOA+DBN model is 4.9% better than PSO+DBN, 18.4% better than FF+DBN, 0.56% better than GWO+DBN and 1.9% better than WOA+DBN. MCC of MT-WOA+DBN model is 7.2% superior to PSO+DBN and 0.28% superior to FF+DBN. Thus, from the overall performance analysis, it is clear that the proposed model overcomes the existing models like PSO+DBN, FF+DBN, GWO+DBN, and WOA+DBN on considering all the performance metrics.

Table 2. Overall performance analysis on proposed over conventional smart phone authentication model

Metrics	PSO+DBN (Tanweer *et al.,* 2015)	FF+DBN (Fister *et al.,* 2013)	GWO+DBN (Wu *et al.,* 2012)	WOA+DBN (Mirjalili & Lewis, 2016)	MT-WOA+DBN	RF	BOA
Accuracy	0.99411	0.99482	0.99478	0.99456	0.99485	0.9920	0.9922
Sensitivity	0.49306	0.49306	0.49167	0.49306	0.49306	0.4938	0.4928
Specificity	0.99917	0.99989	0.99986	0.99962	0.99992	0.99986	0.99962
Precision	0.85749	0.97796	0.97253	0.92932	0.98338	0.97253	0.92932
FPR	0.000828	0.000112	0.00014	0.000379	8.42E-05	0.00014	0.000379
FNR	0.50694	0.50694	0.50833	0.50694	0.50694	0.50833	0.50694
NPV	0.99917	0.99989	0.99986	0.99962	0.99992	0.99986	0.99962
FDR	0.14251	0.022039	0.027473	0.070681	0.01662	0.027473	0.070681
F1-score	0.6261	0.65559	0.65314	0.64428	0.6568	0.65314	0.64428
MCC	0.64774	0.69251	0.68957	0.67479	0.69445	0.68957	0.67479

6. CONCLUSION

This paper has focused on developing a behavior based automatic smart phone authentication model by following three major phases: (i) Feature extraction (ii) Weighted logarithmic transformation (iii) Classification. In the feature extraction phase, HMOG features related to the touch/ gesture of smart phone users were extracted using the grasp resistance and grasp stability. These extracted features

were normalized to map them within the limited range. In the weighted logarithmic transformation phase, these normalized data were multiplied with the weights followed by logarithmic transformation. The decision-making process related to the logarithmic and weight selection was based on proposed MT-WOA optimization model. In the classification phase, the final feature vectors were fed to DBN for recognizing the authorized users. In order to know about the enhancement in the performance of MT-WOA+DBN model, a performance based evaluation was made between MT-WOA+DBN and the existing models like PSO+DBN, FF+DBN, GWO+DBN and WOA+DBN in terms of accuracy, sensitivity, specificity, Precision, FPR, FNR, NPV, FDR, F1-score and MCC. From the analysis, the overall accuracy of MT-WOA+DBN model is 0.07%, 0.003%, 0.007% and 0.02% superior to the existing models like PSO+DBN, FF+DBN, GWO+DBN, and WOA+DBN, respectively. Hence, the proposed smart phone authentication model using weighted logarithmic transformation was done effectively, which has been substantiated well. In future, the experimental results would be undertaken via real mobile devices.

FUNDING AGENCY

Publisher has waived the Open Access publishing fee.

REFERENCES

Agrawal, A., & Patidar, A. (2014). Smart Authentication for Smart Phones. *International Journal of Computer Science and Information Technologies*, *5*(4), 4839–4843.

Alzubaidi, A., & Kalita, J. (2016). Authentication of Smartphone Users Using Behavioral Biometrics. *IEEE Communications Surveys and Tutorials*, *18*(3), 1998–2026.

Arabian Alghamdi, S. J., & Elrefaei, L. A. (2018). Dynamic Authentication of Smartphone Users Based on Touchscreen Gestures. *Arabian Journal for Science and Engineering*, *43*(1), 789–810.

Buriro, A., Crispo, B., & Conti, M. (2019). AnswerAuth: A bimodal behavioral biometric-based user authentication scheme for smartphones. *Journal of Information Security and Applications*, *44*, 89–103.

Cao, H., & Chang, K. (2018). Nonintrusive Smartphone User Verification Using Anonymized Multimodal Data. *IEEE Transactions on Knowledge and Data Engineering*.

Ehatisham-ul-Haq, M., Azam, M. A., Naeem, U., Amin, Y., & Loo, J. (2018). Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing. *Journal of Network and Computer Applications*, *109*, 24–35.

Fister, I., Fister, I. Jr, Yang, X.-S., & Brest, J. (2013). A comprehensive review of firefly algorithms. *Swarm and Evolutionary Computation*, *13*, 34–46.

Galdi, C., Nappi, M., Dugelay, J., & Yu, Y. (2018). Exploring New Authentication Protocols for Sensitive Data Protection on Smartphones. *IEEE Communications Magazine*, *56*(1), 136–142.

Gasti, P., Šedenka, J., Yang, Q., Zhou, G., & Balagani, K. S. (2016). Secure, Fast, and Energy-Efficient Outsourced Authentication for Smartphones. *IEEE Transactions on Information Forensics and Security*, *11*(11), 2556–2571.

Hua, Y., Guo, J., & Zhao, H. (2015). Deep Belief Networks and deep learning. *Proceedings of 2015 International Conference on Intelligent Computing and Internet of Things*, 1-4.

Laghari, W-u-R., & Memon, Z. A. (2016). Biometric authentication technique using smartphone sensor. *Applied Sciences and Technology (IBCAST),* 381-384.

Lin, Y. (2010). SPATE: Small-Group PKI-Less Authenticated Trust Establishment. *IEEE Transactions on Mobile Computing*, *9*(12), 1666–1681.

Lu, L., & Liu, Y. (2015). Safeguard: User Reauthentication on Smartphones via Behavioral Biometrics. *IEEE Transactions on Computational Social System*, *2*(3), 53–64.

Martinez-Diaz, M., Fierrez, J., & Galbally, J. (2016). Graphical Password-Based User Authentication With Free-Form Doodles. *IEEE Transactions on Human-Machine Systems*, *46*(4), 607–614.

Mirjalili, S., & Lewis, A. (2016). The Whale Optimization Algorithm. *Advances in Engineering Software*, (95), 51–67.

Mohamed, W. (2021). Abo.(2020). Implicit authentication method for smartphone users based on rank aggregation and random forest. *Alexandria Engineering Journal*, *60*(1), 273–283.

Nyang, D., Mohaisen, A., & Kang, J. (2014). Keylogging-Resistant Visual Authentication Protocols. *IEEE Transactions on Mobile Computing*, *13*(11), 2566–2579.

Schaffer, K. B. (2015). *Expanding Continuous Authentication with Mobile Devices. Computer*, *48*(11), 92–95.

Šedenka, J., Govindarajan, S., Gasti, P., & Balagani, K. S. (2015). Secure Outsourced Biometric Authentication With Performance Evaluation on Smartphones. *IEEE Transactions on Information Forensics and Security*, *10*(2), 384–396.

Shen, C., Chen, Y., & Guan, X. (2018). Performance evaluation of implicit smartphones authentication via sensor-behavior analysis. *Information Sciences*, *430-431*, 538–553.

Shen, C., Zhang, Y., Guan, X., & Maxion, R. A. (2016). Performance Analysis of Touch-Interaction Behavior for Active Smartphone Authentication. *IEEE Transactions on Information Forensics and Security*, *11*(3), 498–513.

Sitová, Z. (2016). HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users. *IEEE Transactions on Information Forensics and Security*, *11*(5), 877–892.

Tanweer, M. R., Suresh, S., & Sundararajan, N. (2015). Self regulating particle swarm optimization algorithm. *Information Sciences*, *294*, 182–202.

Thavalengal, S., & Corcoran, P. (2016). User Authentication on Smartphones: Focusing on iris biometrics. *IEEE Consumer Electronics Magazine*, *5*(2), 87–93.

Valsesia, D., Coluccia, G., Bianchi, T., & Magli, E. (2017). User Authentication via PRNU-Based Physical Unclonable Functions. *IEEE Transactions on Information Forensics and Security*, *12*(8), 1941–1956.

(2019). Vishnu, and Karan Singh.(2019). An intelligent scheme for continuous authentication of smartphone using deep auto encoder and softmax regression model easy for user brain. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 48645–48654.

Wu, B., Qian, C., Ni, W., & Fan, S. (2012). The improvement of glowworm swarm optimization for continuous optimization problems. *Expert Systems with Applications*, *39*(7), 6335–6342.

Yang, Y., Guo, B., Wang, Z., Li, M., & Zhou, X. (2019). BehaveSense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics. *Ad Hoc Networks*, *84*, 9–18.

Yang, Y., Sun, J., & Guo, L. (2016). PersonaIA: A Lightweight Implicit Authentication System based on Customized User Behavior Selection. *IEEE Transactions on Dependable and Secure Computing*.

Zhu, H., Hu, J., Chang, S., & Lu, L. (2017). ShakeIn: Secure user authentication of smartphones with single-handed shakes. *IEEE Transactions on Mobile Computing*, *16*(10), 2901–2912.

Vinod P. R. is currently working inNoorul Islam Centre for Higher Education.

Anitha A. is currently working on Noorul Islam Centre for Higher Education.