GAIT based Behavioral Authentication using Hybrid Swarm based Feed Forward Neural Network

Gogineni Krishna Chaitanya[1]*, Krovi Raja Sekhar[2]
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram, 522502, Andhra Pradesh
India

Abstract—**Authentication of appropriate users for accessing the liable gadgets exists as one among the prime theme in security models. Illegal access of gadgets such as smart phones, laptops comes with an uninvited consequences, such as data theft, privacy breakage and a lot more. Straight forward approaches like pattern based security, password and pin based security are quite expensive in terms of memory where the user has to keep remembering the passwords and in case of any security issue risen then the password has to be changed and once again keep remembering the recent one. To avoid these issues, in this paper an effective GAIT based model is proposed with the hybridization of Artificial Neural Network model namely Feedforward Neural Network Model with Swarm based algorithm namely Krill Herd optimization algorithm (KH). The task of KH is to optimize the weight factor of FNN which leads to the convergence of optimal solution at the end of the run. The proposed model is examined with 6 different performance measures and compared with four different existing classification model. The performance analysis shows the significance of proposed model when compared with the existing algorithms.**

***Keywords**—GIAT behavioral pattern recognition; feedforward neural network; krill herd algorithm*

I. Introduction

For the verification of identity one of the most trustworthy and effective approach is Biometric method [1]. Its advancements in the recent years are more significant than any other models due to its uniqueness in recognition [2]. One among the significance of biometric is, it has the tendency to connect with the authenticated user in a straightforward manner rather than linking the originality through a third-party mediator such as keywords or tokens [3]. From the other perspective of biometric, there exits GAIT recognition [4] in which the person can be identified by their gesture such as walk, running, etc. [5]. The uniqueness of a person gesture is often carried out in a more effective manner than when it compared with recognition through keywords or patterns. The verification of GAIT is carried out by any of the three forms through video mode, wearable and floor sensor [6]. The authentication of user is the first step for reducing the access of illegal persons [7]. The process is done through the verification of the given identity by the user. The other way of recognizing the authenticated user apart from biometric is through knowledge-based verification [8]. The knowledge-based verification is the process of information which is given by the authenticated user to verify the genuine of the person. Example methods of knowledge-based verification are pattern, pin, passwords, etc. [9]. The disadvantage of this knowledge-based system is forgotten schema and stolen. To overcome this disadvantage an additional feature is added in mobile phones which is the recognition of users through fingerprint biometric [10]. This helps the equipment to verify the users which further gives another step of verification [11].

The recognition of human movements and their biometrics has reached a greater level of importance in the sectors such as military, airport, banks [12]. In some of the regions, authentication of users through a password are pin numbers are often leading to tedious process or it is sometimes recognized as less defense particularly is some of the assaults listed in [13]. Sometimes the catchy words of passwords are often easily predicted. On the other side if non-dictionary words are kept as passwords there is a high possibility of easy forgotten scenario [14]. One more way of authentication of authenticated users is proposed namely Speech recognition. However, the background noise is often making the system to be confused in recognizing the authenticate user. Also, it has the probability to be hacked [15]. Even in biometric recognition patter also if there exists face-based recognition and if the face is unclear it also may lead to difficulty [16].

Sometimes after the usage of authenticated person there is a possibility of leaving the gadget without any lock and hence the probability of accessing it by an unauthenticated user is also high till the gadget gets locked [17]. Hence GAIT type of recognition is proposed to address their problems in smart phones. In this model, the embedded sensor with the device [18] observes the movement of user. If it matches with the authenticated user’s movement then the phone will be unlocked. Through this model the user need not any other secondary verification activity to access the gadget. In this model, the unauthenticated user cannot access it since the sensor completely observes the user’s motion and if it does not match it will be locked [19]. An optimal FNN network is used to classify the authenticated user and unauthenticated user [20]. The proposed model holds Krill Herd algorithm for optimizing the weights of FNN.

Thus, the rest of the paper is organized as follows: Section 2 deals with the literature study. Section 3 discusses the problem statement. Section 4 discusses the FNN and Krill herd algorithm. Section 5 holds the experimental evaluation of the proposed model and the last section concludes the paper.

*Corresponding Author

II. Related Works

The entry check point of a gadget often not secured enough, and it is open for data theft by any way means. In the year 2019, author Praveen kumar Rayani proposed a model [21] using Naïve Bayes classifier for effective verification of authenticated users using GAIT behavioral pattern recognition. The input for the proposed model is Boolean based banner model. Using this model, the authorization of intended data thief is being identified which improves the security of data in mobile devices. Sometimes the smart locks in the mobile device's issues certain kinds of problems such as holding on something for quite some time for being able to approve the authenticity. To address this issue Author Kazhuki, et al. [22] proposed a model that recognizes the walking gesture with the help of sensors in the mobile devices. Another model using key based arrangement model [23] which was proposed by Arne Brusch, et al. to reduce the imperfection in recognition of GAIT based behavior. To prove the significance of the proposed model an effective power based attacking mechanism is used to test the integrity of the model. The output shows the consistency and the integrity of the proposed model by recognizing the GAIT based behavior in mobile device.

Answering based author authentication was proposed by the author Buriroa [24] which is used to record thousands of GAIT movement to propose an effective plan using behavioral pattern in GAIT. The other models include [25] waiving of hand gesture etc. in this paper the contributions are listed as follows:

- An effective FNN hybridized with Swarm based Krill Herd Algorithm is developed for effective classification of authenticated and unauthenticated users [29].
- For the background subtraction from videos Kernel Compactness approximation is used to improvise the quality of the frames.
- The proposed model is implemented and evaluated under suitable testbed.
- The performance of the proposed model is examined and proved its significance by comparing with the existing models.

III. Problem Statement

One among the popular electric device is smartphone. Since it received a significant number of users worldwide, the problems such as hacking, phishing are also become common in nature for smart devices. One such mode of authentication is password or pattern lock or pin number. As it is discussed in the introduction section, these become void due to the restrictions it holds. To address this issue a mechanism called GAIT behavioral authentication system is proposed. Fig. 1 shows the model of normal authentication models such as key, face and pin-based authentication process.

In this plan, if the secret word space of the subsequent stage is distinguishable or arranged to parody, at that point it experiences in interior assault. This plan sets aside some additional effort for verification. To defeat interior assaults and data robbery, a potential arrangement is recognized through social biometrics of cell phone since the personal conduct standards of the individual client are indistinguishable.

A. Information Gathering

The information for the recognition of authentication of users is collected using the sensor namely Gyroscope along with the accelerometer of the mobile devices and it collects the information such as the users style and gestures of running, sitting, walking and standing. The collected information are then sent to the model in the mobile device. The model is developed with the identification module of authenticated and unauthenticated users. In case if any illegal access is done on the gadget then the model identifies the irregulating and denote it to the user's knowledge.

B. Pre-Processing

The preprocessing phase will remove the unwanted low-quality pixels for conducting the experiment in most effective way. The performance of the model can be well evaluated when the input is with less error values. It is removed using the pixilation model for reducing the unwanted pixels in the frames of the video.

C. Feature Reduction using Kernel Compactness Approximation

The behavior recognition with the help of sensors lead to recognizing the actions of the users in 3D form. The input should be read in a 3-dimensional proforma so that it is effective to read the entire walking sitting or running model of the user [30]. The mode we used to generate all the key pairs that are useful for generating the Gram metric where the complexity to solve is in quadratic form.

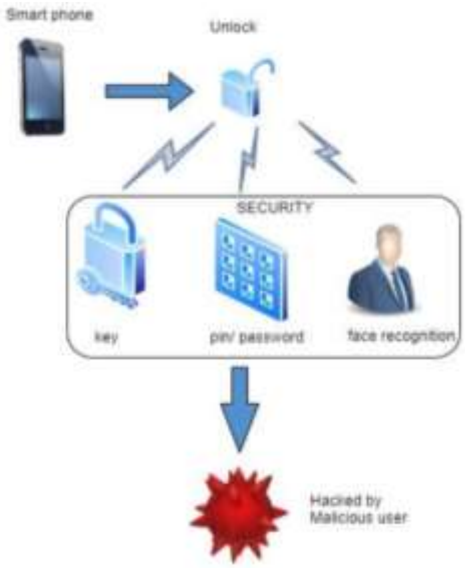


Fig. 1. Problem Statement Features.

The kernel module of a frame can be shown in the form of k and it is represented in the following as:

$$k(m,n) = \int \beta_p \theta_p(m) \theta_p^*(n)$$

where β_p is the value of eigen and θ_p is the eigen vector in normalized form.

$$T_r f = \int k(m) f(m) d\mu(m)$$

where $f(m)$ denotes the features that are selected for user authentication purpose, the above equation is used for verification process.

IV. Working Principle Multi-Layer Perceptron in FNN

The Feedforward Neural Network model is shown the Fig. 2. The number of input layer in any FNN will be 1. There may be more than one number of input variables in the input player. In Fig. 1, the input value ranges from 1 to n. The next layer is the hidden layer. Unlike input layer the hidden layer may range between any number of positive integer values and the number of neurons in the hidden layer is also not restricted. In general, the total number of hidden layers are between the range 3 and 6. The total number of output neurons should be at least one.

Each layer in FNN have certain input and output. In the input layer the input values depend on the problem. This will generate the input for the hidden layer and the output of the hidden layer will be calculated using Eq. (1).

$$s_j = \sum_{i=1}^{n} \left(W_{i,j} \times X_i \right) - \theta_j \tag{1}$$

And the output of the hidden layer will be gone through Equation (2) which is given below:

$$S_j = \frac{1}{(1+\exp(-s_j))} \tag{2}$$

The variable j denotes the number of neurons in the hidden layer. The output computation is done using Eq. (3).

$$o_k = \sum_{j=1}^{h} \left(W_{j,k} \times S_j \right) - \theta_k \tag{3}$$

And finally, the output value is given to the activation function Eq. (4) and it is given as.

$$O_k = \frac{1}{(1+\exp(-o_k))} \tag{4}$$

In the above model the weights (W) and the bias values $(\theta)$are random in general which ranges between 0 and 1. This often leads to non-optimal model construction. This can be eradicated by proposing the algorithm for handling the values such as weights and bias.

A. Krill Herd Algorithm

Krill herd algorithm has the potential to search for an optimal solution in the given stamp of time. It is inspired from the Krills concept. There are three processes which holds the search process in krills.

1) Movements imposed by other krills
2) Foraging
3) Random diffusion

And the combined solution can be represented as

$$\frac{dX_i}{dt} = N_i + F_i + D_i \tag{5}$$

The calculation of $N, F \ and \ D$ are computed as follows:

The induction of movement by other solutions (Krills) can be computed as.

$$N_i^{new} = N^{max} \alpha_i + \omega_n N_i^{old} \tag{6}$$

And the value of α is computed as

$$\alpha_i = \alpha_i^{local} + \alpha_i^{target} \tag{7}$$

Every Krill has its own foraging behavior which can be computed as follows:

$$F_i = V_f \beta_i + \omega_f F_i^{old} \tag{8}$$

The computation of β_i is given as follows:

$$\beta_i = \beta_i^{food} + \beta_i^{best} \tag{9}$$

The generation of new solutions can be done using Diffusion factor as follows:

$$D_i = D^{max} \left(1 - \frac{I}{I_{max}} \right) \delta \tag{10}$$

The Pseudo code of the Krill Herd algorithm is given in Algorithm 1 and the flowchart is shown in Fig. 3.

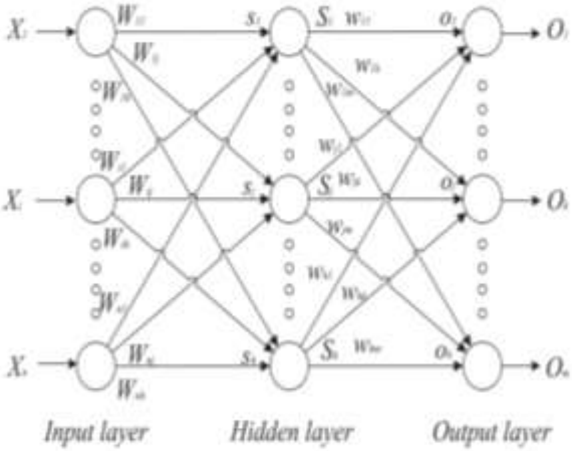


Fig. 2. Feedforward Neural Network.

Krill Herd Algorithm for Tuning weight parameters

```
Begin
Step 1: Initialize $Iter \leftarrow 1, i \leftarrow 0, k \leftarrow 0$
Step 2: for each $KHIndiv \in KHSize$ do
        $Pop_{KHIndiv} \leftarrow LB + (UB - LB) * rand()$
    end for
Step 3: for each $KHIndiv \in KHSize$ do
        $Fit(Pop_{KHIndiv}) \leftarrow f(Pop_{KHIndiv})$
    end for
Step 4: Repeat through Step 8 Until $Max_{IT} \leq Iter$, then go to
        Step 9
Step 5: Movement Induced by other Krill's
    Step 5.1: Repeat through Step 5.3Until $i < KHSize \mid$
              $i \in KHIndiv$ else goto Step 6
Step 5.2: $\alpha_i = \alpha_i^{local} + \alpha_i^{target}$
Step 5.3: $N_i^{new} = N^{max}\alpha_i + \omega_n N_i^{old}$

Step 6: Foraging motion of individual Krill's without Swarm
        colonial behavior
    Step 6.1: Repeat through Step 5.3Until $i < KHSize \mid$
              $i \in KHIndiv$ else goto Step 7
Step 6.2: $\beta_i = \beta_i^{food} + \beta_i^{best}$
Step 6.3: $F_i = V_f \beta_i + \omega_f F_i^{old}$

Step 7: Individual movement of Krill Herd in a random
        manner
    Step 7.1: Repeat through Step 7.2Until $i < KHSize \mid$
              $i \in KHIndiv$ else goto Step 8
Step 7.2: $D_i = D^{max}\left(1 - \frac{I}{I_{max}}\right)\delta$

 Step 8: Repeat through Step 8.2Until $i < KHSize \mid i \in$
 $KHIndiv$ else goto Step 9
 Step 8.1: $\frac{dX_i}{dt} = N_i + F_i + D_i$
 Step 8.2: $\Delta t = C_t \sum_{j=1}^{NV}(UB_j - LB_j)$
Step 8.3: $X_i(t + \Delta t) = X_i(t) + \Delta t \frac{dX_i}{dt}$
Step 9: Return $\min(Fit(Pop_{KHIndiv}))$
End
Output: $\min(Fit(Pop_{KHIndiv}))$
```

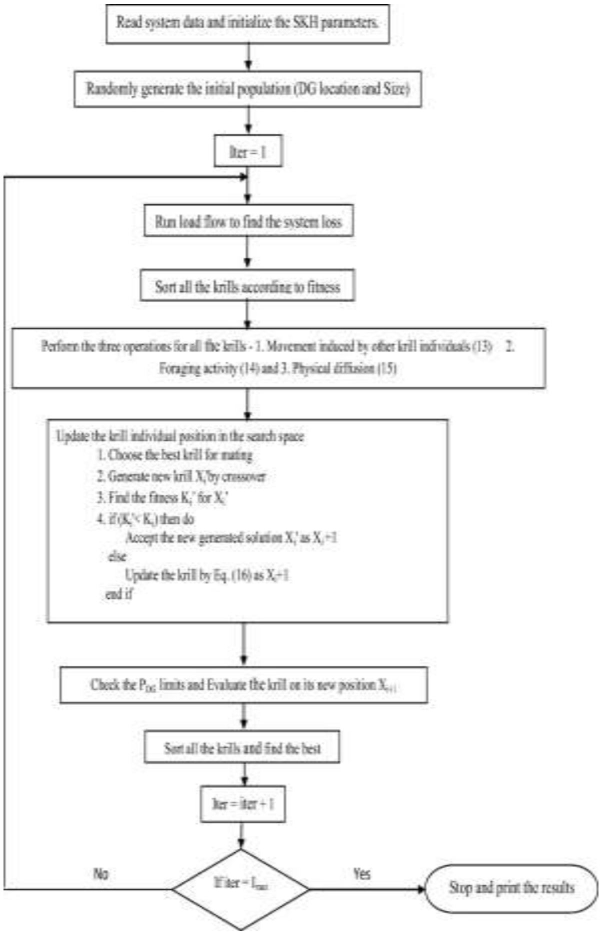

Read system data and initialize the SKH parameters.
Randomly generate the initial population (DG location and Size)
Iter = 1
Run load flow to find the system loss
Sort all the krills according to fitness
Perform the three operations for all the krills - 1. Movement induced by other krill individuals (13) 2. Foraging activity (14) and 3. Physical diffusion (15)
Update the krill individual position in the search space
1. Choose the best krill for mating
2. Generate new krill X_i'by crossover
3. Find the fitness K_i' for X_i'
4. if (K_i'< K_i) then do
Accept the new generated solution X_i' as X_i+1
else
Update the krill by Eq. (16) as X_i+1
end if
Check the P_{DG} limits and Evaluate the krill on its new position X_{i+1}
Sort all the krills and find the best
Iter = iter + 1
No
If iter = I_{max}
Yes
Stop and print the results

Fig. 3. Flowchart of Krill Herd Algorithm.

V. Experimental Evaluation

The proposed model is implemented in Python 3.7 with the system configuration Windows 10 Pro, with Intel core i7 processor speed 3.2GHz, with 16 GB primary storage and 1TB secondary storage. The proposed model identifies the user authentication with the help of GAIT based behavioral pattern recognition. To prove the significance of the proposed model, effective classification algorithms are used for evaluation on the same information which is gathered through sensors.

A. Case Study

The verification model of users is given in Fig. 4. The flow of identification between authenticated and unauthenticated is clearly given for better understanding of the proposed model.

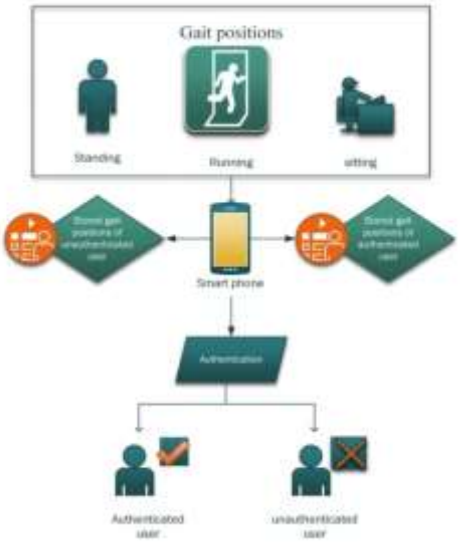


Fig. 4. GAIT Verification Process.

Initially the authenticated behavior will be recorded based on the sensors to provide the training using legible users for the smart device. Later the unauthenticated behaviors are also recorded and given as input for training to find the illegal access. Once the training phase is over, the model will be ready for deployment of identifying the legal and illegal access and the users.

B. Performance Measures

The prove the performance of the proposed model 4 different classification algorithms are chosen namely Naïve Bayes classifier [21], Decision Forest-Decision jungle [26], Random forest [27] and SVM [28]. The different performance measures include Accuracy, Precision, Recall, F-Measure, False Accept Rate and False Reject Rate.

The confusion matrix useful for the interpretation of results is shown in Fig. 5.

1) Accuracy: The accuracy denotes the ratio between sum of true positive and true negative to the sum of all true positive, true negative, false positive and false negative value. Table I shows the overall percentage acquired by all algorithms along with the proposed algorithm.

$$Accuracy = \frac{True\ Positive + True\ Negative}{True\ Positive + True\ Negative + False\ Positive + False\ Negative}$$

From the Fig. 6, on comparing the results of accuracy with existing algorithms, our proposed model proves its significance in terms of percentage over NB with1%, DF-DJ with 7%, RF with 2% and SVM with 1%.

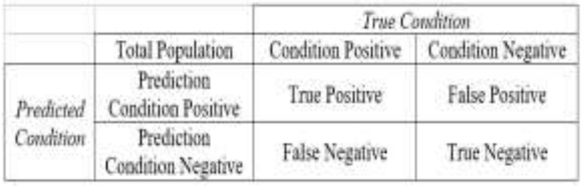
2) Precision: Precision denotes the ratio between total number of identified correct answers with the total number of actual correct classification. The formula for calculation of precision from the confusion matrix is given in Table II and depicted as graph in Fig. 7.

$$\boldsymbol{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

On comparing the results of accuracy with existing algorithms, our proposed model proves its significance in terms of percentage over NB with 4%, DF-DJ with 15%, RF with 9% and SVM with 10%.

3) Recall: The performance measure recall denotes the ratio between actual positive values to the overall identification of positive values from the dataset. The formula for calculation of recall from the confusion matrix is given in Table III and depicted as graph in Fig. 8.

$$Recall = \frac{True\ Positive}{True\ Positive + False\ Negative}$$



		True Condition	
	Total Population	Condition Positive	Condition Negative
Predicted Condition	Prediction Condition Positive	True Positive	False Positive
	Prediction Condition Negative	False Negative	True Negative

Fig. 5. Confusion Matrix.

TABLE I. COMPARISON OF ACCURACY OF FNN-KL WITH EXISTING ALGORITHMS

Algorithms	Accuracy (%)
Naïve Bayes classifier	98.08
Decision Forest-Decision jungle	91.92
Random forest	97.16
SVM	97.11
FNN-KL	99.12

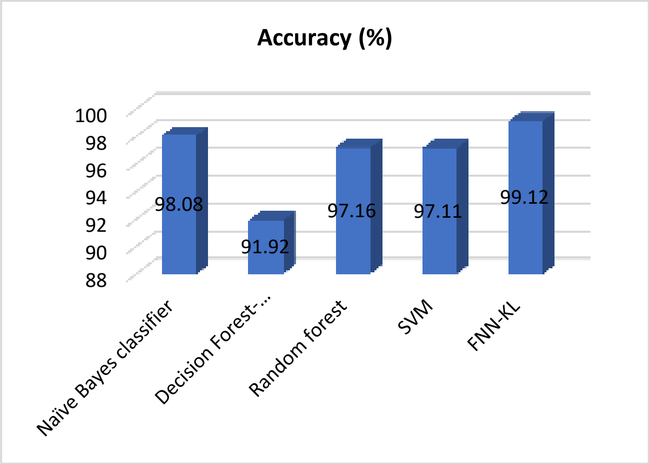


Fig. 6. Comparison Chart on Accuracy (%).

TABLE II. COMPARISON OF PRECISION OF FNN-KL WITH EXISTING ALGORITHMS

Algorithms	Precision (%)
Naïve Bayes classifier	95.53
Decision Forest-Decision jungle	84.44
Random forest	89.65
SVM	88.65
FNN-KL	99.58

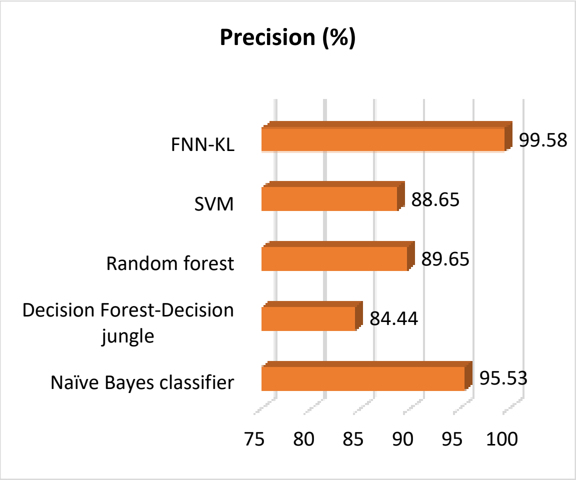


Fig. 7. Comparison Chart on Precision (%).

TABLE III. COMPARISON OF RECALL OF FNN-KL WITH EXISTING ALGORITHMS

Algorithms	**Recall (%)**
Naïve Bayes classifier	86.11
Decision Forest-Decision jungle	90.34
Random forest	80.21
SVM	80.26
FNN-KL	95.47

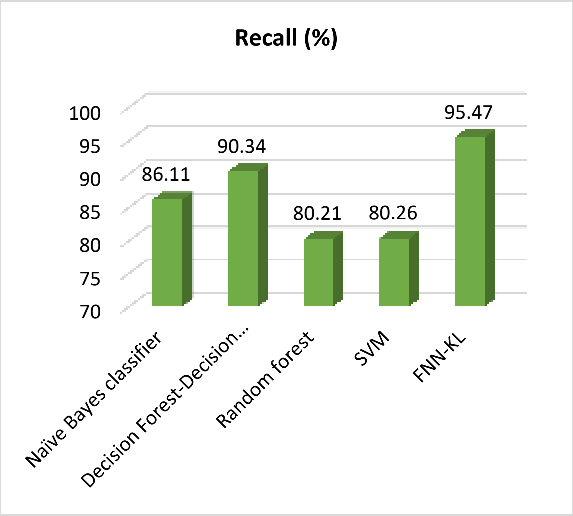


Fig. 8. Comparison Chart on Recall (%).

On comparing the results of accuracy with existing algorithms, our proposed model proves its significance in terms of percentage over NB with 9%, DF-DJ with 5%, RF with 15% and SVM with 16%.

4) F-Measure: The F-score is a meta measurement taken from precision and recall. The mathematical model of calculating F-Score is given in Table IV and depicted as graph in Fig. 9.

$$F - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

TABLE IV. COMPARISON OF F-MEASURE OF FNN-KL WITH EXISTING ALGORITHMS

Algorithms	**F-measure (%)**
Naïve Bayes classifier	93.27
Decision Forest-Decision jungle	81.73
Random forest	92.50
SVM	94.48
FNN-KL	95.12

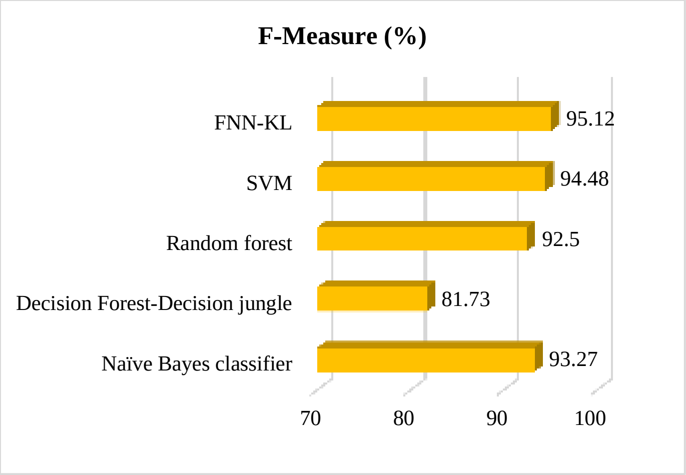


Fig. 9. Comparison Chart on F-Measure (%).

On comparing the results of accuracy with existing algorithms shown in Fig. 9, our proposed model proves its significance in terms of percentage over NB with 1%, DF-DJ with 1%, RF with 1% and SVM with 2%.

5) False Accept Rate: False accept rate for the given model is computed based on the number of unauthenticated users used the gadget. The values for the model are given in Table V. It shows that the proposed model significantly shows less error rate when compared with existing systems.

On comparing the results of accuracy with existing algorithms shown in Fig. 10, our proposed model proves its significance in terms of percentage over NB with 81%, DF-DJ with 76%, RF with 87% and SVM with 86%.

6) False Reject Rate: False reject rate is the identification of unauthenticated users to access the gadget and it lies as the ratio between the two models is given in Table VI.

TABLE V. COMPARISON OF FALSE ACCEPT RATE OF FNN-KL WITH EXISTING ALGORITHMS

Algorithms	**FAR (%)**
Naïve Bayes classifier	3.93
Decision Forest-Decision jungle	1.33
Random forest	2.31
SVM	1.38
FNN-KL	1.35

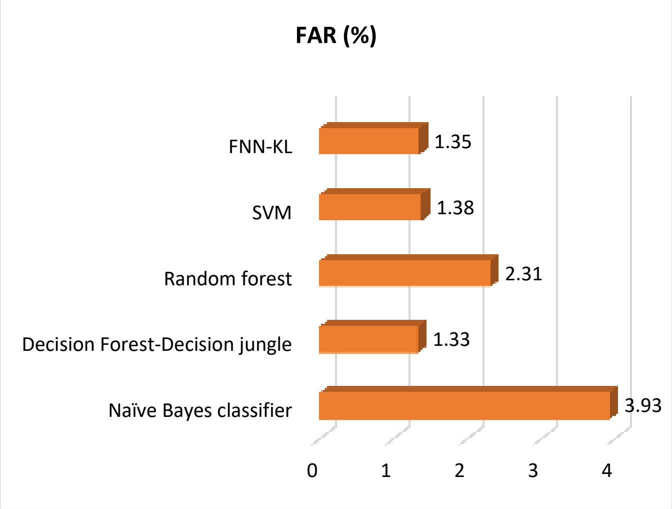


Fig. 10. Comparison Chart on FAR (%).

TABLE VI. COMPARISON OF FALSE REJECT RATE OF FNN-KL WITH EXISTING ALGORITHMS

Algorithms	**FRR (%)**
Naïve Bayes classifier	3.26
Decision Forest-Decision jungle	2.22
Random forest	2.20
SVM	2.41
FNN-KL	6.85

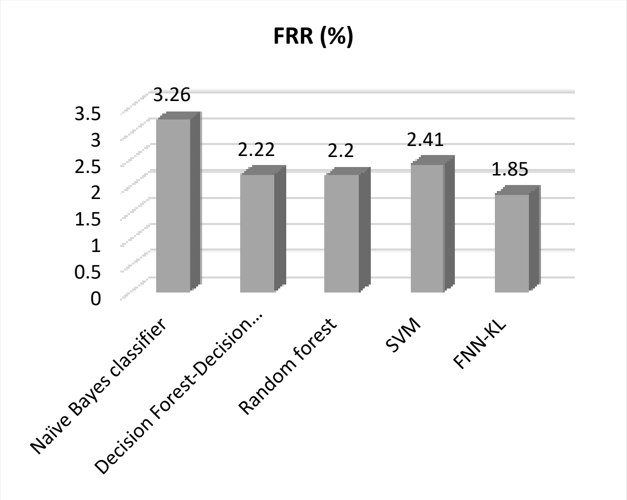


Fig. 11. Comparison Chart on FRR (%).

On comparing the results of accuracy with existing algorithms shown in Fig. 11, our proposed model proves its significance in terms of percentage over NB with 86%, DF-DJ with 79%, RF with 79% and SVM with 81%.

VI. Conclusion

In this paper, an GIA based behavioral pattern recognition namely Feedforward Neural Network-Krill Herd (FNN-HL) is proposed for solving recognition of user for accessing the gadget. The proposed model comprises of FNN for classification of authenticated and unauthenticated users and KH algorithm for tuning the weight and bias values in FNN. The performance of the proposed model is compared with four existing classification algorithms. The performance measures of the proposed model indicate the significance of FNN-KL when compared with other existing algorithms. The future work of this model can be extended with reducing the time complexity of processing the input frames.

References

[1] Belkhouja, Taha, et al. "Biometric-based authentication scheme for Implantable Medical Devices duringemergency situations." Future Generation Computer Systems 98 (2019): 109-119.

[2] Mohsin, A. H., et al. "Based Blockchain-PSO-AES techniques in finger vein biometrics: A novelverification secure framework for patient authentication." Computer Standards & Interfaces 66 (2019):103343.

[3] Nazarkevych, Mariya, et al. "Biometric Identification System with Ateb-Gabor Filtering." 2019 XIthInternational Scientific and Practical Conference on Electronics and Information Technologies (ELIT).IEEE, 2019.

[4] Khan, Muhammad Hassan, Muhammad Shahid Farid, and Marcin Grzegorzek. "A non-linear viewtransformations model for cross-view gait recognition." Neurocomputing (2020).

[5] Huitzil, Ignacio, et al. "Gait recognition using fuzzy ontologies and Kinect sensor data." InternationalJournal of Approximate Reasoning 113 (2019): 354-371.

[6] Bai, Guifeng, and Yunqiang Sun. "Application and research of MEMS sensor in gait recognitionalgorithm." Cluster Computing 22.4 (2019): 9059-9067.

[7] Spagnoletti, Paolo, et al. "Securing national e-ID infrastructures: Tor networks as a source ofthreats." Organizing for the Digital World. Springer, Cham, 2019. 105-119.

[8] Zhou, Yuchen, et al. "Cyber-Physical-Social Systems: A State-of-the-Art Survey, Challenges andOpportunities." IEEE Communications Surveys & Tutorials (2019).

[9] Joudaki, Zeinab, Julie Thorpe, and Miguel Vargas Martin. "Enhanced Tacit Secrets: System-assignedpasswords you can’t write down, but don’t need to." International Journal of Information Security 18.2(2019): 239-255.

[10] Choudhary, Swati K., and Ameya K. Naik. "Multimodal Biometric Authentication with SecuredTemplates—A Review." 2019 3rd International Conference on Trends in Electronics and Informatics(ICOEI). IEEE, 2019.

[11] Sharma, Rohit, Rajendra Prasad Mahapatra, and Naresh Sharma. "The Internet of Things andItsApplications in Cyber Security." A Handbook of Internet of Things in Biomedical and Cyber PhysicalSystem. Springer, Cham, 2020. 87-108.

[12] Kakkad, Vishruti, Meshwa Patel, and Manan Shah. "Biometric authentication and image encryption forimage security in cloud framework." Multiscale and Multidisciplinary Modeling, Experiments andDesign 2.4 (2019): 233-248.

[13] Liu, Yu, et al. "Account Lockouts: Characterizing and Preventing Account Denial-of-ServiceAttacks." International Conference on Security and Privacy in Communication Systems. Springer, Cham,2019.

[14] Karim, Nader Abdel, Zarina Shukur, and AbedElkarim M. AL-banna. "UIPA: User authentication methodbased on user interface preferences for account recovery process." Journal of Information Security andApplications 52 (2020): 102466.

[15] Melnik, S. V., and N. I. Smirnov. "Voice Authentication System for Cloud Network." 2019 Systems ofSignals Generating and Processing in the Field of on Board Communications. IEEE, 2019.

[16] Mehraj, Tehseen, et al. "Critical Challenges in Access Management Schemes for Smartphones: AnAppraisal." Smart Network Inspired Paradigm and Approaches in IoT Applications. Springer, Singapore,2019. 87-113.

[17] Ku, Yeeun, et al. "Draw It As Shown: Behavioral Pattern Lock for Mobile User Authentication." IEEEAccess 7 (2019): 69363-69378.

[18] Ahmadi, S. Sareh, Sherif Rashad, and Heba Elgazzar. "Machine Learning Models for Activity Recognitionand Authentication of Smartphone Users." 2019 IEEE 10th Annual Ubiquitous Computing, Electronics &Mobile Communication Conference (UEMCON). IEEE, 2019.

[19] Do, Quang, Ben Martini, and Kim-Kwang Raymond Choo. "The role of the adversary model in appliedsecurity research." Computers & Security 81 (2019): 156-181.

[20] Fairley, Michael, David Scheinker, and Margaret L. Brandeau. "Improving the efficiency of the operatingroom environment with an optimization and machine learning model." Health care managementscience 22.4 (2019): 756-767.

[21] Rayani, Praveen Kumar, and Suvamoy Changder. "Continuous Gait Authentication against UnauthorizedSmartphone Access through Naïve Bayes Classifier." International Conference on Intelligent Computingand Communication. Springer, Singapore, 2019.

[22] Watanabe, Kazuki, et al. "Gait-Based Authentication Using Anomaly Detection with Acceleration of TwoDevices in Smart Lock." International Conference on Broadband and Wireless Computing, Communicationand Applications. Springer, Cham, 2019.

[23] Bruesch, Arne, et al. "Security Properties of Gait for Mobile Device Pairing." IEEE Transactions on MobileComputing(2019).

[24] Buriro, Attaullah, Bruno Crispo, and Mauro Conti. "AnswerAuth: A bimodal behavioral biometric-baseduser authentication scheme for smartphones." Journal of information security and applications 44 (2019):89-103.

[25] Shen, Chao, et al. "Waving Gesture Analysis for User Authentication in the Mobile Environment." IEEENetwork 34.2 (2020): 57-63.

[26] Kumar, Vivek, Chirag Gupta, and Vatsal Agarwal. "Gait-Based Authentication System." EmergingTechnologies in Data Mining and Information Security. Springer, Singapore, 2019. 685-691.

[27] Kececi, Aybuke, et al. "Implementation of machine learning algorithms for gait recognition." EngineeringScience and Technology, an International Journal (2020).

[28] Lamiche, Imane, et al. "A continuous smartphone authentication method based on gait patterns andkeystroke dynamics." Journal of Ambient Intelligence and Humanized Computing 10.11 (2019): 4417-4430.

[29] Odili, Julius Beneoluchi, Mohd Nizam Mohmad Kahar, and Shahid Anwar. "African buffalo optimization:A swarm-intelligence technique." Procedia Computer Science 76 (2015): 443-448.

[30] Mukuta, Yusuke, and Tatsuya Harada. "Kernel approximation via empirical orthogonal decomposition forunsupervised feature learning." Proceedings of the IEEE Conference on Computer Vision and PatternRecognition. 2016.

AUTHORS

Gogineni Krishna Chaitanya research scholar received his Bachelors Degree in Computer Science from Acharya Nagarjuna University and Masters Degree from JNTUK. He is currently pursuing Ph.D degree with Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Vaddeswaram, 522502 Andhra Pradesh, India. His research interests include digital forensics, Biometrics, Authentication and Machine Learning.

Dr. K Raja Sekhar received his Ph.D Degree in Computer Science and Engineering from Acharya Nagarjuna University. He is currently a Professor with the of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Vaddeswaram, 522502 Andhra Pradesh, India. He has published more than 50 articles in journals and Conference proceedings. His research interests include Digital forensics, Biometrics, Network Security and Usable security. He received several Excellence awards and several best paper awards. He has been on the editorial boards of several journals.