A Deep Learning Framework for Intrusion Detection and Multimodal Biometric Image Authentication

M. Gayathri* and C. Malathy

Department of Computer Science and Engineering, S.R.M. Institute of Science and Technology, Kattankulathur campus, Chennai, India
E-mail: gayathrm2@srmist.edu.in
**Corresponding Author*

Received 05 July 2021; Accepted 24 August 2021;
Publication 29 October 2021

Abstract

Nowadays, a demand is increased all over the world in the field of information security and security regulations. Intrusion detection (ID) plays a significant role in providing security to the information, and it is an important technology to identify various threats in network during transmission of information. The proposed system is to develop a two-layer security model: (1) Intrusion Detection, (2) Biometric Multimodal Authentication. In this research, an Improved Recurrent Neural Network with Bi directional Long Short-Term Memory (I-RNN-BiLSTM) is proposed, where the performance of the network is improved by introducing hybrid sigmoid-tanh activation function. The intrusion detection is performed using I-RNN-BiLSTM to classify the NSL-KDD dataset. To develop the biometric multimodal authentication system, three biometric images of face, iris, and fingerprint are considered and combined using Shuffling algorithm. The features are extracted by Gabor, Canny Edge, and Minutiae for face, iris, and fingerprint, respectively. The biometric multimodal authentication is performed by the proposed I-RNN-BiLSTM. The performance of the proposed I-RNN-BiLSTM has been analysed through different metrics like accuracy, f-score, and confusion matrix. The simulation results showed that the proposed system gives better

Journal of Mobile Multimedia, Vol. 18_2, 393–420.
doi: 10.13052/jmm1550-4646.18212

results for intrusion detection. Proposed model attains an accuracy of 98% for the authentication process and accuracy of 98.94% for the intrusion detection process.

Keywords: Authentication, deep learning; recurrent neural network, multimodal, biometric, intrusion detection.

1 Introduction

In recent years, authentication mechanism is employed for preventing non-authorized person to access of data. Authentication is a process of identifying a particular person based on the person prototype stored in the database and used to differentiate the actual and fake users. Nowadays, Biometric authentication is an emerging topic of research by researchers for revolutionary developments in the modern era. A biometric system is utilized to identify a person either genuine or cheat by using their physiological traits (hand geometry, face, fingerprint etc.) and behavioural characters (voice, gait, signature etc.). This earlier biometric system which was developed, used a single trait for recognition and do not provide better authentication for highly secured application. While, there are several works progressing in the field of biometric authentication, the identification of persons purely depends upon their physiological or behavioural characteristics, but there is a lot of challenges involved resulting in different unsolved problem. Because it is more complex during computations and data capturing. Many Intrusion Detection Systems (IDS) have been proposed in the literature. However, several models face the challenge of utilizing large power for computations. The performance might also tend to be low. It is very much vital to identify the intruder, since the data being exchanged is at the risk of getting stolen. In that concern, the proposed work suggests a two-layer data protection model, which comprises of an IDS model to identify the presence of an attack and an authentication model for a second level of imposter detection.

Multimodal Biometric Systems (MBS) are developed to overcome those problems which arise due to the noise and intra class variability. MBS can be used to combine different physical and behavioural traits such as face, iris, fingerprint, gait and signature etc. A new approach of MBS was developed with improved security and to overcome the limitations [1] Abozaid et al., designed an efficient multimodal biometric identification to recognize the person by combining features of the face and voice of an individual This method served as human authentication tool [2]. Three classifiers were used

to perform voice and face identification. Eventhough biometric recognition involves rapid development in technology, it must provide security to transmit the data and images through the internet, because it may utilize the weak link to steal the information. Shanker et al., proposed the conventional method of using passwords and Identity cards, but it had some security issues. The Safety of these systems can be easily broken by misusing them for false endeavours [3].

SreeVidya, B et al., proposed a security framework based on Multimodal Biometric Hash Key Cryptography (MBHC) which focused on authentication and security of data stored in the cloud [4]. The input images used for this study were Face, iris, and fingerprint images of the individual. Feature extraction was carried out by linear filter, whereas, Artificial Fish Swarm Optimization was employed for feature selection, followed by SVM for classification. The cryptographic algorithm employed for encryption and decryption was AES. Jahnavi, S et al., proposed a visual crypto mask steganography which supports the good capacity of the payload using the multimodal technique [5]. Fingerprint and face were considered for biometric embedding and these images were processed through a magic sheet that combines cover and mask images, which is in turn combined with a random visual crypto method. Brown, R. et al., developed a multimodal system of authentication system with the help of ML and blockchain technology [6]. The images considered for the study were face and fingerprint with age and gender as features. The results were classified using the Decision Tree algorithm. The visual shadow creation technique was employed by Evangelin, L. N et al, used several shadows of the secret image. It has been utilized for encryption and decryption using Elliptic Curve Cryptography (ECC) [7].

Deep learning has been applied in various domains to enhance the accuracy level. It includes the natural language processing (NLP), and speech recognition, etc. [8, 9]. Ali Z. et al., designed biometric multimodal system that employed computational resources on an optimal basis using portable personal devices like edges [10]. The ultimate goal of this proposed work is to provide reliable encryption and decryption, but it does not involve any secret sharing templates. Henceforth, the system has still prone to security threats. Multimodal biometric system which uses 3 inputs such as fingerprint, finger vein, and iris was developed by Walia, G. S. et al., used the optimal score based fusion mechanism, and moreover it is not support the adaptability nature of the score level scheme. Even though these methods discriminate against individuals accurately, they do not guarantee data privacy [11].

Sandeep Singh et al., developed a neural community (DNN) which projected the drawbacks of unimodal structure with respect to FAR and FRR, hence, the importance of multimodal biometric system is enhanced [12]. A multi-modal discriminative method of dimensionality reduction that performs data fusion of various modalities was proposed by Zhu, Q. et al., Even though these methods achieved discriminate against individuals accurately, it does not give guaranteed data privacy [13]. The ultimate promising deep learning architectures used by the computer vision community, consist of different neural networks namely convolutional neural networks (CNN) [14], recurrent neural networks (RNN), combinations of CNNs and RNNs (CRNNs), [15, 16], auto encoders (AEs) [17] generative adversarial networks (GANs) [18] and (6) fully connected neural networks (FCs) [19].

An improved anti-spoof ability was successfully demonstrated by Syed AqeelHaider et al., is based on hand-related intrinsic modalities. Three modalities were combined and fuzzy rule based system was designed to get a better accuracy of 92% [.20]. New design of multimodal biometric authentication system named DeepKey framed by Xiang zang et al., used two traits namely EEG and Gait. This system performed well against spoof attacks. Deepkey was designed in a way it provided two important key components where one to block hackers and the other one to identify the subject using Recurrent Neural Network (RNN). Both components worked in parallel [21].

In recent days many researchers focused on Recurrent Neural Network – Bidirectional Long Short-Term Memory (RNN-BiLSTM) for authenticating purpose. ECG data is handled by RNNs and it adds the bidirectional-LSTM (BiLSTM) variants to it, to overcome the problem of vanishing gradient. Saadatnejad et al., imposed a scheme with two small LSTM networks to incorporate the ECG features in wearable devices for continuous monitoring [22].

R. Vinayakumar et al., designed an Intrusion detection (ID) system which can detect actions by collecting details. This system helps in analysing the network behaviour, collecting log information of the users, on the network. Basically, ID system developed verifies the presence of irregular behaviours [23]. IT system security policy and indication of being attacked in the system is very much required for each network. Compared with traditional system, yiruri, et al., ID system is sensible, dynamic, and effective complement to firewall, which actually performs as a passive protection mean to attacks [24].

The previous research experiments prove that the need for the attack detection needs an improvement and has not been appropriately analysed. ShidehSaraeian et al., developed a hybrid network-based Intrusion Detection System (IDS) with the help of deep learning technique to detect intrusion on network using the NSL-KDD, ISCXIDS 2012 datasets. Both the datasets were analysed. Traffic analysis was done on the network Wireshark tool. The results proved that deep learning method achieved higher accuracy in comparison with other machine learning techniques [25, 26].

In this research work, Improved Recurrent Neural Network – Bidirectional Long Short-Term Memory (IRNN-BiLSTM) classifier is proposed. In this model a hybrid activation function called sigmoid-tanh activation function is used for improving the performance of the conventional RNN-BiLSTM. The proposed work takes the input of digital images of face, iris, fingerprint and user's system parameters. The proposed IRNN-BiLSTM attack classifier unit is initially employed for identifying the intrusions caused by the imposters. In the proposed research work, NSL-KDD dataset is given for testing the attack classification model. If the user is not a client but an imposter, then the access is denied. But if the user is an authorized client, then he/she undergoes an authentication check. The proposed IRNN-BiLSTM authentication unit matches the multimodal biometric data with the database and classifies whether the user is an authorized user or not.

The remaining part of this research paper is structured in the following manner. Section 2 related works; Section 3 proposed methodology; Section 4 results and discussion and Section 5 provide a conclusion and scope to extend the work in the future.

2 Related Works

Intrusion detection system (IDS) plays a major part in terms of certifying information security. Intrusion detection system (RNN-IDS) based on RNN is an essential tool for developing a model to classify and identify the various attacks in the network. Network IDSs are differentiated into two categories such as signature-based network IDSs and anomaly-based network IDSs. Tang et al., developed a self-taught learning (STL) approach which was based on the deep learning techniques and tested with NSL-KDD dataset for a network intrusion detection system. Performance observed shown more better results [27]. LSTM was used on KDDCup99 dataset and it proved that it can classify the attack. Krishnan and Raajan et al., constructed a model as a sawy self-erudition-based IDs RNN structure for attack classification. Compared

with the baseline methods, this method had improved in measurements in terms of classification of accuracy and time consuming [28]. Yin et al., developed a deep learning method based on RNN-IDS, which was tested with NSLKDD dataset. RNN-IDS performance is improved when compared with the to the traditional classification algorithms [29].

Mohamed et al., performed the binary and multiclass classification with convolutional neural network and Long Short-Term Memory (LSTM) for specific IDS system using UNSW-NB15 dataset [30]. The CNN layers were used to bring out the significant features from network. Pramita et al., framed a method for intrusion detection with NSL-KDD dataset which was trained by genetic algorithm (GA) combined with RNN-LSTM. It has been identified that LSTM-RNN based classifiers provide optimal feature set progresses for intrusion detection [31].

2.1 Deep Learning Methods for Biometric Images

Biometric recognition process is more accurate when deep learning methods are adopted. Deep learning helps in feature learning, generalizing the datasets.

Deep Boltzmann Machines: DBM is an extension of restricted Boltzmann machine which is a energy based model with three hidden layers. Face biometric uses DBM method.

Deep Belief Network: It is graphical model with one visible layer and n hidden layers. Pretraining is done with multilayer perceptron. Face, voice, keystroke biometrics uses this DBN.

Stacked Auto encoders: Auto encoders are used for back propagation and unsupervised learning. It is feed forward non recurrent neural network. More Number of hidden layers are added for deep autoencoders. Face uses auto encoders.

Convolution Neural Networks: CNN uses kernel weights and pooling layers. Pooling layer comprises the feature map. Face, fingerprints, palm prints, iris, signature and gait uses CNN approach.

Recurrent Neural Networks: A recurrent neural network uses memory and it has feedback mechanism between the layers. Each layer depends on the previous layer. For processing the features of voice, text, speech, videos RNN method is preferred.

From the survey it is concluded that many works related to intrusion detection system has been employed with various algorithms, various neural network models. In this paper IRNN-BiLSTM based attack classifier unit is employed to identify the intrusions caused by the imposters in multimodal authentication model.

2.2 Problem Statement

There is huge demand for data security, especially during transmission, due to the increase in cybercrime activities. The existing scenarios lacks security in privacy preservation of data. Various attacks are done on the biometric images which is a threat to leakage of sensitive data. Visual cryptography helps to secure the data during transmission by converting the data to meaningless shares which provides no information.

2.3 Challenges

Nowadays authentication process is done with the help of biometrics, hence the major challenge which lies behind is the efficient processing of biometric data. Intrusion is a major concern with all data transmission process. It is very much important to address all kinds of attacks in any authentication procedure to ensure the authenticity of the individual. Hence two-layer security model is needed to address the Intrusions faced by the network.

3 Proposed Methodology

In this proposed method, three types of physiological biometric inputs such as face, fingerprint and iris of an individual is considered for the identification purpose. The new shuffling algorithm is designed based on a pixel element is employed to generate shares which are considered to be the encryption process. The decoding process is the reconstruction of original biometric images results from the shares generated. These shares will not reveal any meaningful information. The concept of shares are designed by the visual cryptographic scheme. The reconstructed images are passed through the bilateral filter to eliminate noise and preserve edges. Each Biometric Data develops different image segmentation technique like Binary segmentation for finger-print image, face segmentation for face image, and Daugman's integro differential operational for iris image. Images are segmented using the feature extraction with respected techniques followed for fingerprint, iris,

and face images are minutiae, canny, and Gabor feature extraction algorithms respectively. The features extracted from the reconstructed images are used to train with I-RNN-BiLSTM model. The fusion technique is important for any kind of multimodal data. For the data transmission process the pixel level fusion or the sensor level fusion is adopted when three modalities namely face, iris and fingerprint are considered as input. Feature level fusion is adopted for the authentication and intrusion detection purpose. There are many traits available which includes the physiological traits and behavioral traits. Behavioral traits encounter issues with high non matching rate; hence we have chosen physiological traits like face, fingerprint and Iris. Iris biometrics provides a better accuracy, while the face and fingerprint are a user-friendly trait which are available with ease. This combination of traits would be effective to handle multimodal inputs with ease.

Binary classification results in two categories namely normal and anomaly. Multi-class classification has five categories of detection such as normal, denial of service (DoS), probe, user-to root (U2R), and remote-to-local (R2L). Simple machine learning algorithm of NSL-KDD is used for classification-clustering problems. A hybrid activation function called sigmoid-tanh activation function is employed in the I-RNN-BiLSTM Network. The LSTM network designed achieves a higher detection rate when combined with the basic RNN network. The attack is identified using the I-RNN-BiLSTM classification model, and the authentication model is used to evaluate attack presented. If it is matched the process continues otherwise access is denied and again the training process is repeated. Figure 1 represents block architecture of two layered security model for biometric authentication system which is based on IDS.

3.1 Secure Biometric Multimodal Processing

The face, iris and fingerprint images are taken as input images. A novel shuffling algorithm is applied on the three input images by using the visual cryptographic technique. As a part of shuffling algorithm odd- even row share and odd-even column share is constructed for the input images. Shuffling process contain three input images namely face, iris and finger print image. These three input images are further separated into seven input images as contain seven segments, they are separated as in the similar manner as mentioned in the above process, first input image of the face is separated into three namely R plane, G plane, and B plane, second the iris image is separated into two namely binary and inverse binaries and similarly the third

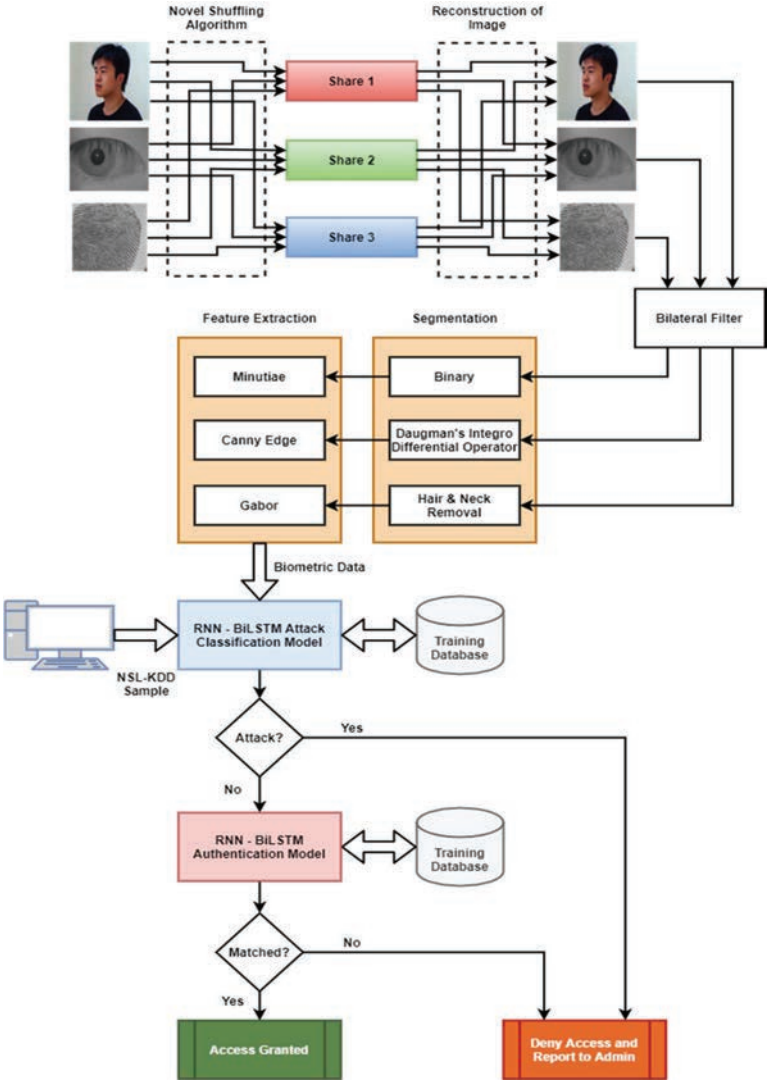

Figure 1 The proposed framework of two-layer security model.

finger print image is separated into two namely binary and inverse binaries. All these input images are resized into 255*255 matrix form, as initially with three segments and each segment contain 85 rows and columns. Then, from the seven input images, each odd number on the rows are formed the first share as S1 (odd) for 85 rows and similarly the even number on the rows

Algorithm 1 Odd-Even row share

Objective: To construct novel complexity share by using rows
Input: $X\{i\}, i = 1, 2, \ldots 7$
Output: $S_R\{i\}, i = 1, 2, 3, 6$. Each S_R is a share image.

```
procedure SR = Share–Row(X)
n = Number of rows in X{1}
a = bn/3c;
Y {1,1} = Odd–Numbers from 1 to a
Y {1,2} = even–Numbers from 1 to a
Y {2,1} = Odd–Numbers from a + 1 to 2 × a
Y {2,2} = even–Numbers from a + 1 to 2 × a
Y {3,1} = Odd–Numbers from (2 × a) + 1 to n
Y {3,2} = even–Numbers from (2 × a) + 1 to n
ct = 1
for i = 1 to 3 do
    for l = 1 to 2 do
        Z = ∅
        for k = 1 to |Y {i,l}| do
            for j = 1 to 7 do
                Z = [Z;X{j}(Y {i,l}(k),:)]
            end for
        end for
    end for
end for
SR{ct} = Z; ct = ct + 1
```

formed S1 (even) for 85 rows. Then similarly, for second share, seven input images of each odd number on the rows are formed into another share as S2 (odd) for 85 rows from (86–170), in the similar manner each even number on the rows formed S2 (even) for 85 rows from (86–170) and finally the last share from the seven input images of each odd number on the rows are formed as S3 (odd) for 85 rows from (171–255), in the similar manner each even number on the rows formed S3 (even) for 85 rows from (171–255). The algorithm for odd-even row and column share are given below in Algorithm 1. The even and odd shares of row shares and even and odd shares of column shares are shown in Figure 2.

3.2 Pre-processing, Segmentation and Feature Extraction

The authentication processes are carried out with four steps such as bilateral filter, segmentation, feature extraction and I-RNN-BiLSTM. I-RNN-BiLSTM is further separated into 2 parts, namely training and testing parts.

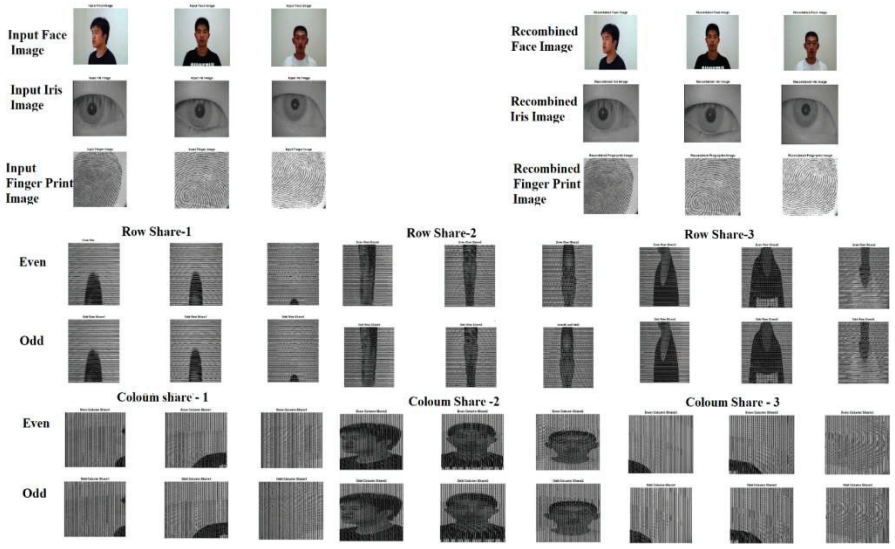

Figure 2 Reconstruction of input images using shuffling algorithm.

The bilateral filtering method is then used to remove the noise and to preserve the edges. Binary segmentation is used for fingerprint image, Daugman's integrodifferential operator is utilized for the eye image, and the neck and hair removal are used to identify the given face image clear. The feature extraction of the images is done on the specific inputs. The features that are extracted from the input images are given to the IRNN BiLSTM to classify and approve authentication based on IDS deployed.

3.3 Modal classification and intrusion detection

One of the best recognized and broadly used deep learning algorithms in image classification application is the RNN. RNNs mostly adopted for the supervised approach but it has a problem of discharging gradients. To overcome the gradient issues during training process an LSTM can be combined to the RNN network. LSTM networks exchange all units in the hidden layer with memory blocks. BiLSTM, on the other hand, supports data flow through two directions. Thus, the RNN-BiLSTM network can provide good performance in intrusion detection. Moreover, IDS is the most significant tool against complex attacks in the networking environment.

The extracted image features from the decryption process (reconstructed image from the shares) are trained and tested using the I-RNN-BiLSTM. The

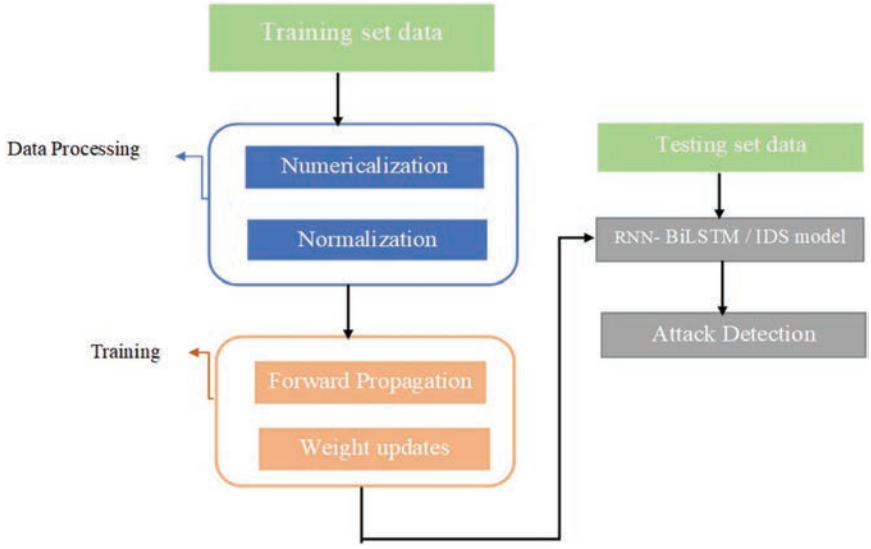

Figure 3 Training and testing procedure for image classification.

RNN algorithm receives an input image, to identify its features and identify it, and then produces the result of classification. The testing and training procedures for image classification in shown in Figure 3.

Four gates are used in the operation of BiLSTM. The memory cells in the BiLSTM network helps in regulating the gates. The gates are responsible for controlling the incoming and outgoing information flow. These gate outputs can be defined as follows,

$$i_t = \sigma(W_i \cdot (h_{t-1}, x_t) + b_i) \tag{1}$$

$$f_t = \sigma(W_f \cdot (h_{t-1}, x_t) + b_f) \tag{2}$$

$$o_t = \sigma(W_o \cdot (h_{t-1}, x_t) + b_o) \tag{3}$$

Where

$$h_t = o_t \times \text{sigmoid}(\tanh(c_t)) \tag{4}$$

$$c_t = (f_t \cdot c_{t-1}) + (i_t \cdot c'_t) \tag{5}$$

Where c_t is the cell state, c_{t-1} is the previous cell state. Where c_t is the cell state, i_t is the input state, o_t is the output state, f_t is the forget state, W is the weight vector and b is the bias vector.

The first phase is the training of the network with the original feature values. While training the grid, weight and bias are updated according to the loss function for every iteration. The inputs are multiplied with the weight and added with bias. The weight is computed with the error value calculated for every iteration of the training phase before adding to the bias. Training these parameters helps to achieve maximum network accuracy. After maximum accuracy has been reached, the weight and bias are set and fixed. With the final weight and bias only the testing process is carried out.

3.3.1 Intrusion detection

Attacks against Biometric Images:

Hill climbing attack: This attack aims at obtaining a synthetic sample from a matcher module to target the feature extractor module to malfunction.

Morphing attack: It is a kind of presentation attack which involves generating a synthetic template by obtaining multiple samples of subjects.

Presentation attack: Impersonating the biometric trait involves unauthorised access to the system.

Replay attack: This kind of attack normally comes in the middle of the communication channel, it discards the original data and sends fake data.

Inversion attack: Reversing the template or data is called the inversion attack.

Side channel attack: Attacker does not attack the system but gain information about the system.

Spoof Attack: The Spoof attack's major aim is to make the whole of the biometric system degrade. It achieves this by "the submission of a stolen, copied or synthetically replicated biometric trait to the sensor to defeat the biometric system security in order to gain unauthorized access".

Trojan Horse Attack: This attack is common across all computing systems today where the execution file looks like it is executing what the user wants but does notorious stuff behind the user's back.

Zero Effort Attack: This attack is common attempt where the attacker attacks directly by trying to imitate the behavioural traits of the user without actually knowing in detail about the user's traits. An attack can be called a zero-effort attack when the attack directly gives the actual biometric of the user. An example of the latter can be keeping the user's finger on his phone to gain access.

Statistical Attack

This attack is similar to that of Zero Effort but with the difference being the attacker has a general statistical information on the biometric. This type of attack is mostly commonly seen in behavioural biometrics such as keystrokes etc.

Denial-of-Service Attacks (DoS): The attacker tries to reduce a source or system feature unusable by genuine users by creating it too busy with false requests. Due to hardware failures, software bugs, environmental conditions, or even the combination of these factors Dos attacks happens in the network.

The above explained categories of attacks fall under few attacks of NSLKDD dataset like DoS, Probing, etc. Denial of service attack is considered important as it denies access to the genuine users of the biometric system. This type of attacks can be detected by the intrusion detection process and it can be avoided by strong authentication mechanism. Different types of DoS attacks: blackhole, Gray hole, flooding, and scheduling attacks. Some attacks try to exploit viruses in network software and protocol stack by sending abnormal packets. The distant access is enough to perform DoS attacks and the examples like back, ping of death, smurf, Neptune, teardrop etc.

For the detection of DoS attacks, NSL-KDD dataset is considered in this work. NSL-KDD is an improved version of the KDDCup'99 datasets. Duplicated data are removed in NSL-KDD so that it achieves better performance in intrusion detection. The NSL-KDD dataset [32] has two data sets like KDD Train+, and KDD Test +. In KDD train+ having training dataset and KDDTest+, having testing dataset and both are designed with responding attack labels. Three main processes such as, data transferring, data normalization and feature detection are carried out with the dataset processing. In data transferring, the trained images are first converted into a number because; dataset has numbers as features. These symbolic features include some protocols and service types. In data normalization transferring symbolic features are converted into numerical values as a well-proportioned range, hence, the bias where the features of higher points is removed from the dataset. All features within the record are normalized by the respective maximum value and falls into [0–1] range which is same for all. The transferring and normalization process is applied to test dataset.

Tables 1: [33] and Table 2: [34] characterize the NSL-KDD dataset.

Table 1 Attack categories of NSLKDD

Major Categories	Sub Categories
Denial of service(DoS)	Neptune, smurf
User to Root(U2R)	Buffer overflow, perl
Remote to local(R2L)	Guess password, imap
Probing	Ipsweeping, nmap

Table 2 Few instances by attack type of NSLKDD

Attack	No of Instances in NSLKDD Dataset	Attack Category
Normal	67343	normal
Neptune	41214	DoS
Smurf	2646	DoS
Buffer overflow	30	U2R
Perl	3	U2R
Guess passwd	53	R2L
Imap	11	R2L
Ipsweeping	3599	Probe
Nmap	1493	Probe

4 Results and Discussion

4.1 Dataset Description

The dataset used for biometric authentication model is SDUMLA-HTM Database at Shandong University, Jinan, China. It contains real multimodal biometric images of 106 individuals. For our experiment we took 10 individuals and their three biometric trait images of face, iris and fingerprint (each sample 10 so totally 300 images). The dataset used for attack detection model is NSLKDD. The authorization has been checked for these individuals against 23 attacks of NSLKDD dataset. It is a multimodal dataset. Face data with different poses, with different expressions and different illumination levels included in the dataset. Five Iris images are obtained from left eye and five images from the right eye is recorded for an individual (total of 10 for a single person). Fingerprint data is available with five different sensors for multiple fingers.

4.2 Experimental Results

The proposed system's is an implementation using MATLAB Tool and the performance of the system in both the phases namely; attack detection and user authentication is analyzed and evaluated with the following metrics:

Accuracy, Error rate, Sensitivity, Specificity, Precision, Recall and F1-Score.

4.2.1 Performance analysis of attack detection model

The training process of the IRNN-BILSTM is shown in the below Figure 4. The training is performed with the learning rate of 0. 001. Activation function used here is a hybrid version of sigmoid and tanh. Each layer of the attack detection model uses the prelu function. The number of max epochs used in training process is 100 with minimum batch size of 20. Fully connected output layer is embedded with the softmax function. The overall architecture which undergoes the IRNN-BILSTM process for authentication is indicated by Figure 5.

Physiological biometric inputs from face, iris and fingerprints are processed using the novel shuffling algorithm and the features obtained are further used for intruder detection in the IRNN-BiLSTM network. The network is trained using the NSL-KDD dataset that comprises of data belonging to the different categories of attacks namely; Normal, Probe, DoS, U2R and R2L. The first phase of the proposed algorithm is executed to classify the given input as an 'attack' or 'not an attack' and the performance of

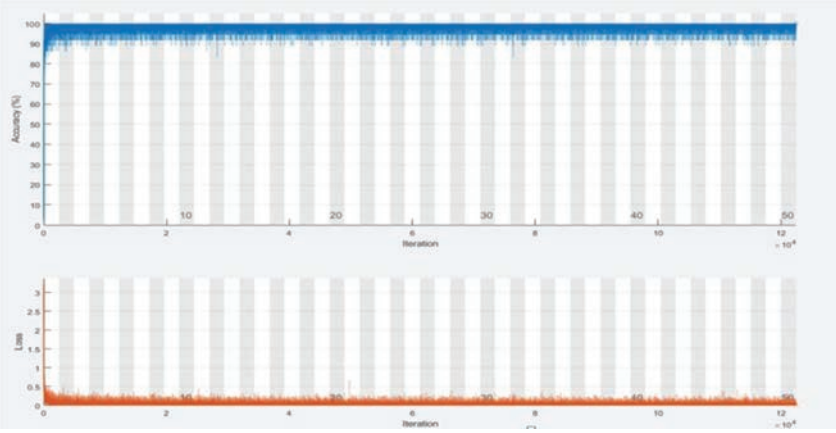

Figure 4 Training process of the IRNN-BILSTM.

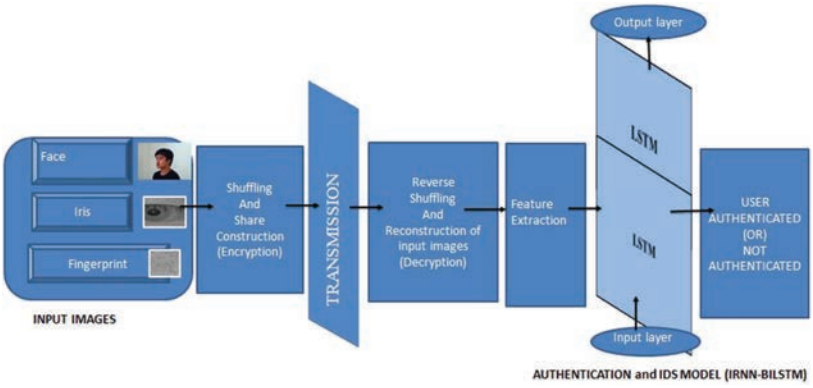

Figure 5 Authentication process of Bi LSTM.

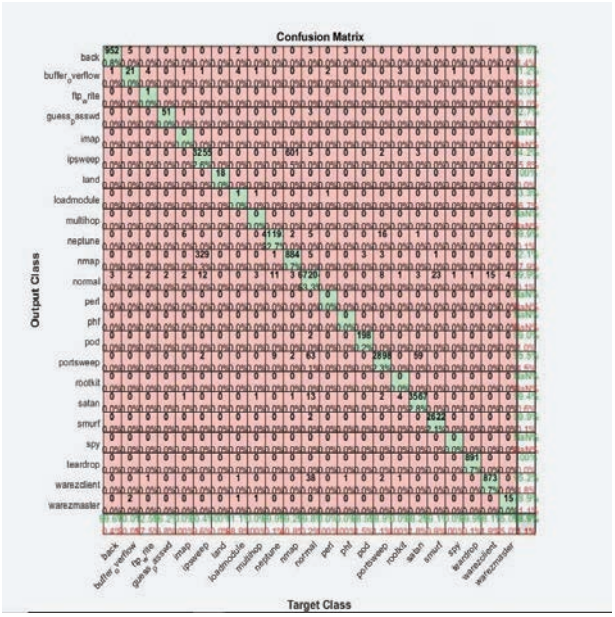

Figure 6 Confusion matrix representing the attack classifier.

the RNN-BiLSTM classification model is represented through a confusion matrix depicted below in Figure 6.

The confusion matrix essentially portrays the effective ratios between classes of the output class and the target classes. After detecting an intrusion using the classifier, the following step involves making a decision whether to

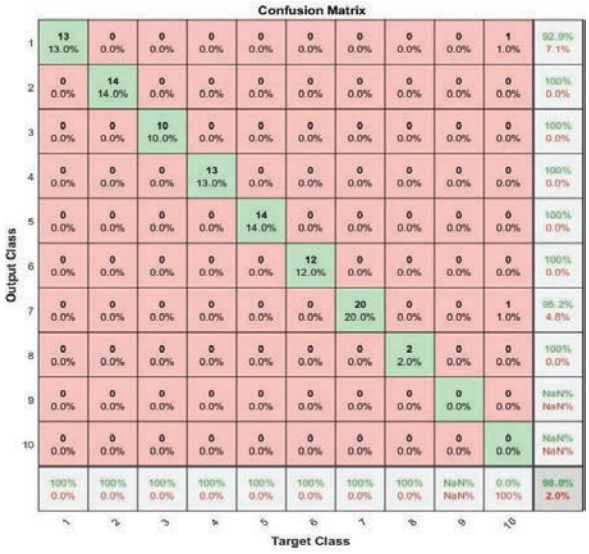

Figure 7 Confusion matrix representing authorization.

'grant the access or deny granting the accesses to the user, depending on the RNN-BiLSTM authentication model's result. A matched entry in the RNN-BiLSTM authentication model will give the user, his/her requested access and if the model gives a negative response to the input entry, the user is denied an access and is treated as an intrusion. Similar to the confusion matrix of intrusion detection, a confusion matrix given in (refer Figure 7) can also be formulated to depict the relationship between the output class and target class during authorization.

The performance of both the phases i.e. attack detection and authorization is evaluated through significant metrics such as accuracy, precision, recall, error rate, F1-score, sensitivity and specificity. Tables 3 and 4 lists the metrics and their corresponding resultant values obtained by the proposed algorithm in both the phases.

Accuracy: Accuracy is the ratio of the sum of TN and TP to the sum of TN, TP, FN, and FP.

$$Accuracy\% = \frac{TP + TN}{TP + TN + FP + FN} \times 100 \tag{6}$$

Error Rate: Error rate can be calculated from accuracy as:

$$Error\ Rate\% = 100 - Accuracy \tag{7}$$

Table 3 Performance of the proposed IRNN-BiLSTM network-based attack detection model

Metric	Intrusion Detecting Classifier (in %)
Specificity	99.98
Precision	1
Recall	1
F1-Score	1
Error Rate	1.055
Accuracy	98.945

Table 4 Performance of the proposed IRNN-BiLSTM network-based authentication model

Metric	Authentication Classifier (in %)
Specificity	98.85
Precision	1
Recall	1
F1-Score	1
Error Rate	2
Accuracy	98

Specificity: Specificity is the ratio of TN to the sum of TN and FP.

$$Precision = \frac{TN}{FP + TN} \tag{8}$$

Precision: Precision is the ratio of TP to the sum of TP and FP.

$$Precision = \frac{TP}{FP + TP} \tag{9}$$

Recall: Recall is the ratio of TP to the sum of TP and FN.

$$Recall = \frac{TP}{FN + TP} \tag{10}$$

F1-Score: F1-score is two times the ratio of the product of precision and recall to the sum of precision and recall.

$$F1\text{-}score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{11}$$

4.2.2 Performance validation

Additionally, a comparative analysis of the existing methods and the proposed system was carried out to prove the superiority of the proposed framework. Table 5 shows the comparison of the proposed intrusion detection model with the existing works which used the NSL-KDD dataset. Figures 8 and 9 represents the comparative analysis of attack detection model and authentication model.

From the table, it is clear that the accuracy and error rate of the proposed attack-detection model is 6.67% and 1.96% better compared to the existing works [37 and 38], respectively.

Table 6 shows the comparison of the proposed MBS authentication model with the existing classifiers such as Decision Tree (DT), K-Nearest Neighbor (KNN), and RNN.

From the results achieved by the proposed system, it was found that the proposed framework has produced a superior accuracy rate and minimal error rate, in the case of both attack detection and MBS authentication. The

Table 5 Comparison of attack detection models

Methods	Accuracy (in %)	Error Rate (in %)
XGBoost–DNN [38]	97	3
ILECA [39]	92.35	7.65
I-RNN-BiLSTM [Proposed]	98.945	1.055

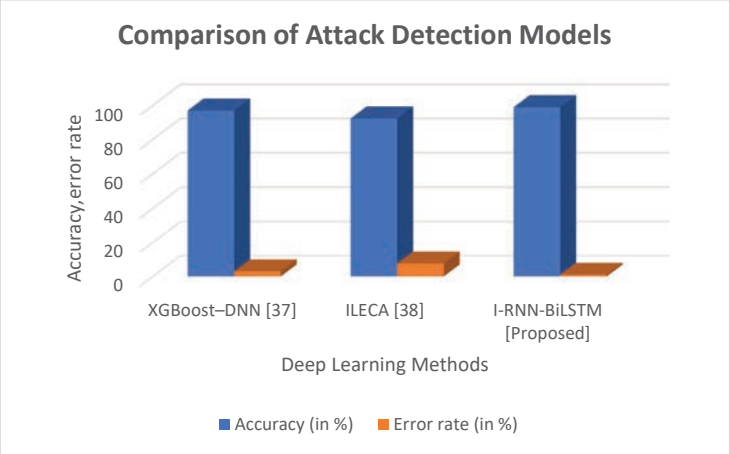

Figure 8 Comparison of attack detection model.

Table 6 Comparison of proposed authentication model with other classifiers

Methods	Accuracy (in %)	Error Rate (in %)
Decision Tree (DT)	91	9
K Nearest Neighbor (KNN)	92.6	7.4
RNN	95.5	4.5
I-RNN-BiLSTM [Proposed]	98	2

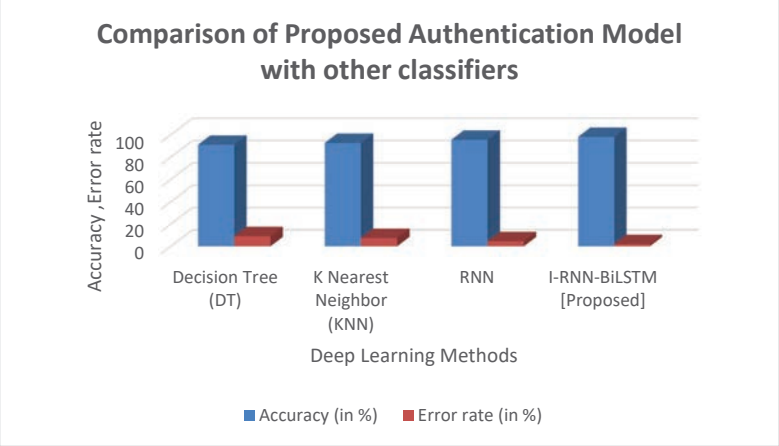

Figure 9 Comparison of authentication model.

accuracy of the proposed model is found to be 7%, 5.4%, and 2.5% better compared to DT, KNN, and RNN, respectively. This is because, DTs are unstable and so, even a small change in the input might lead to large changes in the structure of the tree. On the other hand, KNN requires large memory for computations and the prediction process slows down for large dataset. The traditional RNN classifier employs normal recurrent layer which has limited memory unlike BiLSTM. It is trained by Backpropagation algorithm and so the data transmission is one sided unlike BiLSTM. In addition, the traditional RNN employs sigmoid activation function which tend to vanish gradients unlike the proposed sigmoid-tanh activation function.

5 Conclusions

The growing need for information security has enabled the strict security regulations in a corporate environment to handle the intrusion attacks.

Advancements in this domain have produced solutions involving a variety of technologies with the currently popular one being the biometric technology. State-of-art methodologies have also worked on a combination of machine learning algorithm using distinctive inputs. Though all these aforementioned methodologies have exhibited great classification detection, their accuracies are not sufficient enough to produce a high performing classifier. Hence, a novel deep learning- based framework 'Improved Recurrent Neural Network – Bi-directional Long Short-Term Memory' is proposed for detecting the presence of an intrusion in the biometric inputs. The features extracted from the biometric inputs are used for the authentication purpose and attack detection by the proposed model. The I-RNN-BiLSTM provides the improved performance by combining RNN and LSTM together and is executed in two phases. The first phase involves detecting the presence of attacks and the second stage involves providing authorization (permission to access/deny) to the user after determining his/her true identity. These two stages are sequentially executed in the IRNN-BiLSTM classification and IRNN-BiLSTM authentication models respectively. The model was trained using the NSL-KDD dataset and its performance was evaluated on the basis of its accuracy, sensitivity, specificity, precision, error rate and recall. The proposed work can be applied to any kind of application in cloud, IOT, Smart healthcare which requires the privacy preserving aspect for data. This helps to detect network anomalies for securing the data during transmission and authentication process. Hybrid activation function improves the model accuracy for the attack detection process from 95% to 98.945%. From the results achieved by the proposed system, it was found that the proposed network achieved an overall accuracy of 98.945% and a very minimal error rate of 1.055% making it a suitable choice for an intrusion detection application The work helps to identify the intrusions in authentication model but it can further be improved by integrating it with block chain technology to provide higher level of security.

References

[1] Sree, S.R. Soruba and Dr. Radha, 'A Survey on Fusion Techniques for Multimodal Biometric Identification'. International Journal of Innovative Research in Computer and Communication Engineering. Vol. 02. pp. 7493–7497, 2015.

[2] Abozaid, A., Haggag, A., Kasban, H. and Eltokhy, M., 'Multimodal biometric scheme for human authentication technique based on voice

and face recognition fusion'. Multimedia Tools and Applications, 78, **78**, 16345–16361 (2019). https://doi.org/10.1007/s11042-018-7012-3.

[3] Shankar, K., Elhoseny, M., Chelvi, E.D. and Lakshmanaprabu, S.K. et al., 'An Efficient Optimal Key Based Chaos Function for Medical Image Security'. *IEEE Access*, 6, pp. 77145–77154, 2018. https://doi.org/10.1109/ACCESS.2018.2874026

[4] SreeVidya, B. and Chandra, E., 'Multimodal biometric hash key cryptography-based authentication and encryption for advanced security in the cloud'. Biomedical Research, Medical Diagnosis and Study of Biomedical Imaging Systems and Applications, *29*, 506–516, 2018. https://doi.org/10.4066/biomedicalresearch.29-17-1766.

[5] Jahnavi, S. and Nandini, C, 'Novel Multifold Secured System by Combining Multimodal Mask Steganography and Naive Based Random Visual Cryptography System for Digital Communication'. Journal of Computational and Theoretical Nanoscience, vol. 17, no. 12, pp. 5279–5295, 2020. https://doi.org/10.1166/jctn.2020.9420.

[6] Brown, R., Bendiab, G., Shiaeles, S and Ghita, B, 'A Novel Multimodal Biometric Authentication System Using Machine Learning and Blockchain'. International Networking Conference. Springer, pp. 31–46, 2020. https://doi.org/10.1007/978-3-030-64758-2_3.

[7] Evangelin, L.N. and Fred, A.L. 'Securing recognized multimodal biometric images using the cryptographic model'. Multimedia Tools and Applications, 18735–18752, 2021. https://doi.org/10.1007/s11042-021-10541-8.

[8] Hafemann, L.G., Oliveira, L.S., Cavalin, P.R. and Sabourin, R., 'Transfer learning between texture classifications tasks using convolutional neural networks'. International joint conference neural networks. pp. 1–7, 2015. https://doi.org/10.1109/IJCNN.2015.7280558.

[9] El Khiyari, H. and Wechsler H, 'Face recognition across time lapse using convolutional neural networks'. Journal of Information Security, vol. 7, no. 3, pp. 141–151, 2016. https://doi.org/10.4236/jis.2016.73010.

[10] Ali, Z., Hossain, M.S., Muhammad, G. and Ullah, et al., 'A. Edge-centric multimodal authentication system using encrypted biometric templates'. Future Generation Computer Systems, Vol. 85, pp. 76–87, 2018. https://doi.org/10.1016/j.future.2018.02.0404.

[11] Walia, G.S., Singh, T., Singh, K. and Verma, N, 'Robust multimodal biometric system based on optimal score level fusion model'. Expert Systems with Applications, vol. 116, pp. 364–376, 2019. https://doi.org/10.1016/j.eswa.2018.08.036

[12] Sandeep Singh Sengar, U. Hariharan and K. Rajkumar, 'Multimodal Biometric Authentication System using Deep Learning Method', International Conference on Emerging Smart Computing and Informatics (ESCI), AISSMS Institute of Information Technology, Pune, India. March 12–14, 2020. https://doi.org/10.1109/ESCI48226.2020.9167512.

[13] Zhu, Q., Xu, X., Yuan, N., and Zhang, Z. et al., 'Latent correlation embedded discriminative multi-modal data fusion'. Signal Processing, vol. 171, 107466, 2020. https://doi.org/10.1016/j.sigpro.2020.107466.

[14] Acharya, U.R., Oh, S.L., Hagiwara, Y. and Tan, J.H. et al., Gertych, A., San Tan, R., 'A deep convolutional neural network model to classify heartbeats'. Computers in Biology and Medicine, vol. 89, pp. 389–396. 2017. https://doi.org/10.1016/j.compbiomed.2017.08.022.

[15] Al Rahhal, M.M., Bazi, Y., Almubarak, H. and Alajlan, N. et al., 'Dense convolutional networks with focal loss and image generation for electrocardiogram classification'. IEEE Access, vol. 7, pp. 182225–182237, 2019. https://doi.org/10.1109/ACCESS.2019.2960116.

[16] Alcaraz, R., Abásolo, D., Hornero, R. and Rieta, J.J., 'Optimal parameters study for sample entropy-based atrial fibrillation organization analysis' Computer methods and programs in biomedicine, vol. 99, pp. 124–132, 2010. https://doi.org/0.1016/j.cmpb.2010.02.009.

[17] Andersen, R.S., Peimankar, A. and Puthusserypady, S., 'A deep learning approach for real-time detection of atrial fibrillation'. Expert Systems with Applications, vol. 115, pp. 465–473, 2019. https://doi.org/10.1016/j.eswa.2018.08.011.

[18] Andreotti, F., Carr, O., Pimentel, M.A., and Mahdi, A. et al., 'Comparing feature-based classifiers and convolutional neural networks to detect arrhythmia from short segments of ecg'. Computing in Cardiology (CinC), IEEE. pp. 1–4. 2017. https://doi:org/10.22489/CinC.2017.360-239.

[19] Attia, Z.I., Friedman, P.A., Noseworthy, P.A and Lopez-Jimenez et al., 'Age and sex estimation using artificial intelligence from standard 12-lead ecgs'. Circulation: Arrhythmia and Electrophysiology, vol. 12, e007284, 2019. https://doi.org/10.1161/CIRCEP.119.007284.

[20] Syed Aqeel Haider, Yawar Rehman and S.M. Usman Ali, 'Enhanced Multimodal Biometric Recognition Based upon Intrinsic Hand Biometrics', Electronics, vol. 9, pp. 1916, 2020. https://doi.org/10.3390/electronics9111916.

[21] Xiang zang, Linoyao, Chaoran Hung and Tao Gu et al., 'DeepKey: A Multimodal Biometric Authentication System via Deep Decoding

Gaits and Brainwaves', ACM Transactions on Intelligent Systems and Technology, Article No.: 49 https://doi.org/10.1145/3393619, May 2020. https://doi.org/10.1145/3393619.

[22] Saadatnejad, Saeed, Oveisi, Mohammadhosein and Hashemi et al., 'LSTM-Based ECG Classification for Continuous Monitoring on Personal Wearable Devices'. IEEE Journal of Biomedical and Health Informatics. pp. 1–1. 10.1109/JBHI.2019.2911367,2019. https://doi.org/10.1109/JBHI.2019.2911367.

[23] R. Vinayakumar, K. Soman, and P. Poornachandran, 'Evaluating effectiveness of shallow and deep networks to intrusion detection system', International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE, Udupi, India, pp. 1282–1289, September 2017. https://doi.org/10.1109/ICACCI.2017.8126018.

[24] Yirui Wu, Dabao Wei, and Jun Feng, 'Network Attacks Detection Methods Based on Deep Learning Techniques: A Survey', Hindawi Security and Communication Networks, Volume Article ID 8872923, 17 pages https://doi.org/10.1155/2020/8872923, 2020. https://doi.org/10.1155/2020/8872923.

[25] R. Vinayakumar, M. Alazab, K.P. Soman and P. Poornachandran, et al., 'Deep learning approach for intelligent intrusion detection system', IEEE Access, vol. 7, pp. 41525–41550, 2019. https://doi.org/10.1109/ACCESS.2019.2895334.

[26] Shideh Saraeian, and Mahya Mohammadi Golchi, 'Application of Deep Learning Technique in an Intrusion Detection System', International Journal of Computational Intelligence and Applications, vol. 19, No. 02, 2050016, 2020. https://doi.org/10.1142/S1469026820500169.

[27] T.A. Tang, L. Mhamdi, D. McLernon and S.A.R. Zaidi et al., 'Deep learning approach for network intrusion detection in software defined networking', International Conference on Wireless Network Mobile Communication. (WINCOM), pp. 258–263. Oct. 2016. https://doi.org/10.1109/WINCOM.2016.7777224

[28] R.B. Krishnan and N. Raajan, 'An intellectual intrusion detection system model for attacks classification using RNN', International Journal of Pharmaceutical Technology and Biotechnology, vol. 8, no. 4, pp. 23157–23164, 2016.

[29] Chuanlong Yin, Yuefei Zhu, Jinlong Fei, and Xinzheng He, 'A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks', IEEE Access, vol. 5, 2017. https://doi.org/10.1109/ACCESS.2017.2762418.

[30] M. Hassan, A. Gumaei, A. Alsanad, and M. Alrubaian et al., 'A Hybrid Deep Learning Model for Efficient Intrusion Detection in Big Data Environment', Information Sciences, vol. 513, 2019. https://doi.org/10.1016/j.ins.2019.10.069.

[31] Pramita Sree Muhuri, Prosenjit Chatterjee, Xiaohong Yuan and Kaushik Roy et al., 'Using a Long Short-Term Memory Recurrent Neural Network (LSTM-RNN) to Classify Network Attacks'. Information, vol. 11, pp. 243; doi:10.3390/info11050243. 2020. https://doi.org/10.3390/info11050243.

[32] Tavallaee, M., Bagheri, E., Lu, Wand Ghorbani, 'A Detailed Analysis of the KDD CUP 99 Data Set'. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, pp. 1–6, 8–10 July 2009. https://doi.org/10.1109/CISDA.2009.5356528.

[33] Dhanabal, L. and Shantharajah, S.P, 'A Study on NSL_KDD Dataset for Intrusion Detection System Based on Classification Algorithms.' Computer Science. vol. 4, pp. 446–452, 2015. https://doi.org/10.17148/IJARCCE.2015.4696.

[34] Hamid, Y. Balasaraswathi, V.R., Journaux, L. and Sugumaran, M. 'Benchmark Datasets for Network Intrusion Detection: A Review.' International Journal of Network. Security. vol. 20, pp. 645–654. 2018. https://doi.org/10.6633/IJNS.2018XX.20%28X%29.XX.

[35] M. Hammad, Y. Liu and K. Wang, 'Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint', IEEE Access, vol. 7, pp. 26527–26542, doi: 10.1109/ACCESS.2018.2886573.2019. https://doi.org/10.1109/ACCESS.2018.2886573.

[36] Muthukumar, A., and Kavipriya, A, 'A biometric system based on Gabor feature extraction with SVM classifier for Finger-Knuckle-Print'. Pattern Recognition Letters, vol. 125, pp. 150–156, 2019. https://doi.org/10.1016/j.patrec.2019.04.007.

[37] Chanukya, P.S. and Thivakaran, T.K., 'Multimodal biometric cryptosystem for human authentication using fingerprint and ear', Multimedia. Tools and Applications, vol. 79, pp. 659–673, 2020. https://doi.org/10.1007/s11042-019-08123-w.

[38] Devan, P., Khare, N. 'An efficient XGBoost–DNN-based classification model for network intrusion detection system'. *Neural Computing & Applications,* **32**, 12499–12514, 2020. https://doi.org/10.1007/s00521-020-04708-x

[39] Zheng, D., Hong, Z., Wang, N., and Chen, P. An Improved LDA-Based ELM Classification for Intrusion Detection Algorithm in IoT Application. *Sensors (Basel, Switzerland)*, *20*(6), 1706, 2020. https://doi.org/10.3390/s20061706

Biographies

M. Gayathri is an Assistant Professor in Department of Computer Science and Engineering S.R.M. Institute of Science and Technology, Kattankulathur campus, Chennai, India. Currently she is pursing Ph.D. (CSE) in S.R.M. Institute of Science and Technology, Chennai. She has over ten years of experience in Teaching. Her research interest is Security and Privacy in Biometrics, Network Security, Internet of Things and Cryptography.

C. Malathy is a Professor in Department of Computer Science and Engineering, S.R.M. Institute of Science and Technology, Kattankulathur campus, Chennai, India. She earned Ph.D. in Computer Science & Engineering from S.R.M. Institute of Science and Technology, Chennai. She has over Twenty-eight years of experience in Teaching and Research. Her areas of interest are Image processing, Data Mining and Computer architecture. She has published research papers in many international conferences and refereed journals.