Uluslararası İleri Doğa
Bilimleri ve Mühendislik
Araştırmaları Dergisi
Sayı 8, S. 136-151, 2, 2024
© Telif hakkı IJANSER'e aittir
Araştırma Makalesi

IJANSER

https://as-proceeding.com/index.php/ijanser
ISSN: 2980-0811

International Journal of Advanced
Natural Sciences and Engineering
Researches
Volume 8, pp. 136-151, 2, 2024
Copyright © 2024 IJANSER
Research Article

Classification of Keystroke Dynamics with Deep Learning Models

Mujahed Mohdfathi Mohammad ALISSA[1], Hasan TEMURTAŞ[2], Çiğdem BAKIR[3,*]

[1]*Kütahya Dumlupınar Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Bölümü, Kütahya, Türkiye*

[2]*Kütahya Dumlupınar Üniversitesi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Kütahya, Türkiye*

[3]*Kütahya Dumlupınar Üniversitesi, Mühendislik Fakültesi, Yazılım Mühendisliği Bölümü, Kütahya, Türkiye*

(Received: 22 February 2024, Accepted: 08 March 2024)

(4th International Conference on Innovative Academic Studies ICIAS 2024, March 12-13, 2024)

ATIF/REFERENCE: Alissa, M. M. M., Temurtaş, H. & Bakır, Ç. (2024). Classification of Keystroke Dynamics with Deep Learning Models. *International Journal of Advanced Natural Sciences and Engineering Researches, 8(2), 136-151.*

Abstract: Keystroke dynamics is a biometric application that determines the typing styles and behaviors of a person or people. It is generally used in authentication processes because it is easy to collect data and has low implementation costs. Authentication methods play an important role in ensuring information security and confidentiality. However, the inadequacy of biometric applications and the difficulties in determining data .based on people's behavior have necessitated the need for secure authentication and recognition systems Therefore, keystroke dynamics were classified using deep learning models such as Deep Neural Networks .(DNN) and Convolutional Neural Networks (CNN) and a reliable authentication system was developed Additionally, the results of the proposed deep learning models are presented comparatively. Authorization and ,authentication systems, which are the most important elements of information security and cyber security have been implemented by classifying and analyzing keystroke dynamics. In order to increase the success of .the system, it is aimed to determine the most optimum and accurate results with different hyperparameters This study will have an important place in the development of authentication and recognition systems, which play an important role in solving security problems such as authorization and data access by determining the ..different behavior and writing styles of user

Keywords: Keystroke, Security, DNN, CNN, Deep Learning

I. INTRODUCTION

Keystroke dynamics are biometric-based methods that perform identity recognition and verification by determining the biological and behavioral characteristics of users according to their typing styles in digital environments [1]. Users add timing information via digital devices such as keypads and keyboards and input their dynamics into the system, and in the light of this information, user authentication is carried out according to their behavior [2]. However, it is very difficult to authenticate by determining the behaviors and writing styles of the same user at different time periods [3]. Some studies have been carried out in the literature in recent years on user identity recognition for this problem.

Lin and his colleagues used Convolutional Neural Networks (CNN) to identify unauthorized users in the system with biometric authentication method for strong encryption feature [4]. They have identified malicious users who will determine the hit order of passwords through authentication. In this study, the CNN model prevented unauthorized users from entering the system even if the password was leaked. The study achieved success of approximately 90% or more. Additionally, the performance of the system is accelerated with GPU parallel computing.

Mao and his colleagues proposed a keystroke dynamic authentication approach based on Convolutional Neural Network (CNN) and Bidirectional Long Short Term Memory (BI-LSTM) methods in order to provide solutions to the security problems that arise with network attacks [5]. The feature vector they obtained in their study constituted the keystroke content and duration. While processing the feature vectors with CNN, it creates the training network with the BI-LSTM method. With the study conducted using the Buffola data set, it was determined that FRR (False Rejection Rate), FAR (False Acceptance Rate) and EER (Equal Error Rate) were 3.09%, 3.03% and 4.23%, respectively. They did. However, in order to increase the performance of the system, optimize it and improve the continuity of the system, the accuracy of the system must be analyzed in practical environments.

Aversano and his colleagues proposed a biometric authentication approach using the Deep Neural Network (DNN) method [6]. Three different data sets were used in this study. In addition, in the study, they determined the best classifier with different voting techniques such as majority and Bayesian and the K-means method. An accuracy of up to 0.997 has been achieved on very large data sets. In this study, 16 different features were considered and optimized to train a multi-classifier using deep neural networks.

User authentication methods have a very important place in ensuring cyber security of institutions and organizations and defending the system against possible dangers by applying security policies. In this context, Kiyani and his colleagues developed the Robust Recurrent Confidence Model (R-RCM) to ensure continuous session monitoring to ensure that authorized users log into the system [7]. They recommended that a login be made for each user transaction and that the login should be monitored throughout the transactions. With their proposed R-RCM model, the data were classified according to the probability score of the ensemble classifier. Based on this probability score, fake users were quickly detected.

Çevik and his colleagues developed an authentication system with a web application based on the keystroke data of 54 people working in a company [8]. In this study, two-factor authentication and keystroke dynamics based on user behavior are proposed. In the study, they compared the method they proposed with machine learning techniques such as Bagging, Decision Trees, Random Forest, Extra Trees and Gaussian Naive Bayes. Approximately 94% accuracy was achieved in their studies. For the performance of the study, faster and more efficient models can be developed with deep learning models such as Long-Short Term Memory Networks (LSTM) and Recurrent Neural Networks (RNN).

Maharjan and his colleagues developed a keystroke dynamics authentication system with Artificial Neural Networks for password-based authentication [9]. They achieved approximately 99% success rate. It is aimed to prevent password leakage with the hybrid sensors used in this study. The study can be improved with information from a large number of users in large data sets.

Piugie and his colleagues implemented key dynamics-based user authentication with the DNN method [10]. Keystroke dynamics are very important for password verification. Biometric data containing users' behavior was converted into image data and classified with the DNN method. In this study, the success of the authentication system was evaluated with Equal Error Rate (EER). In addition, this study observed the success of deep learning methods in biometric authentication processes. Features such as users' emotions can form training and test data of the proposed DNN method, and the success of the system can be increased by improving the data sets with preprocessing methods.

It is very difficult to attack by imitating personal keystroke information. A user's keystroke information may vary depending on the data at hand. For this reason, Lu and his colleagues classified keystroke datasets using CNN and Recurrent Neural Network (RNN) in free text writing in order to perform authentication processes by detecting user keystroke habits [11]. With these deep learning methods, they transformed keystroke data into feature vectors. In this study, they also used the CNN+RNN model for continuous authentication and tested this hybrid model on the buffola dataset. The data was processed with CNN to improve network performance. Then, the resulting feature vector entered the RNN. They tested their proposed model on two separate data sets and found the best false rejection rate (FRR) (2.07%, 6.61%), the best false acceptance rate (FAR) (3.26%, 5.31%), the best They found the good equal error rate (EER) to be (2.67%, 5.97%).

Andrean et al. proposed user authentication with a deep learning model using Multi-Layer Perceptron (MLP) in keystroke dynamics [12]. This model achieved an optimal EER of 4.45% compared to classification methods such as 9.6% (scaled Manhattan), 9.96% (Mahalanobis Nearest Neighbor), 10.22% (Open Value Count). The success of the proposed deep learning models was measured with many evaluation criteria such as RMSE, MAE, F-measure, MCC, ROC, PRC and confusion matrix. Further analysis can be performed on different datasets with autoencoders, RNN and different deep learning models.

Çeker and Upadhyaya implemented the biometric authentication system on three different data sets using CNN and Gaussian data augmentation techniques [13]. With this method, 10% higher accuracy and 7.3% Equal Error Rate (EER) was achieved. Acien and his colleagues implemented biometric authentication with Long Short-Term Memory (LSTM) [14]. New free-text keystroke biometrics systems based on RNN architecture are proposed, evaluated on four public databases trained with different learning strategies. In this proposed model, they compared different training samples and key lengths as features and compared traditional statistical methods with their proposed model called TypeNet.

II. MATERİAL AND METHOD

Deep learning is a subdiscipline of machine learning. Deep learning models can be expressed as artificial neural networks consisting of many layers. These layers enable complex and difficult problems to be solved. Deep learning models were developed inspired by the neuronal networks of the human brain [14]. A neuronal network consists of many neurons connected to each other. Each neuron receives inputs and produces an output after processing these inputs. In deep learning models, neurons are arranged in layers. Neurons in each layer receive inputs from the previous layer, process these inputs and send them to the next layer.

There are many different algorithms used in deep learning. These algorithms determine how neuronal networks will be trained and used. Some of the deep learning algorithms are [15]:

- Sequential backpropagation: This algorithm is the most common algorithm used to train neuronal networks. In the sequential backpropagation algorithm, the network makes predictions based on input data. These predictions are compared with actual values and the network is constantly updated to reduce errors. This process is repeated until the deep learning network makes accurate predictions.
- • Support vector machines for deep learning: This algorithm adapts support vector machines for deep learning applications. Support vector machines are a powerful machine learning algorithm used to learn nonlinear relationships in data.
- • Natural language processing for deep learning: These algorithms use deep learning for natural language processing tasks. Text classification, text summarization and question answering are included in natural language processing problems and deep learning methods can be used.

The three most commonly used deep learning algorithms are ANN, DNN and CNN.

• Artificial Neural Network (ANN): ANN is a deep learning algorithm that uses densely connected layers [16]. ANNs can be used for a variety of tasks, but they are especially effective for classification and regression.

• Deep Neural Network (DNN): DNN is a deep learning algorithm based on multilayer perceptrons [17]. DNNs can be used for a variety of tasks, but they are especially effective for classification and regression.

• Convolutional Neural Network (CNN): CNN is a deep learning algorithm that uses convolutional layers [18]. CNNs are particularly effective for image processing and natural language processing.

Our study consists of two stages. In the first stage, preprocessing of keystroke data was carried out. In the second stage, the data obtained was divided into 70% training and 30% testing. All the data obtained was classified with deep learning models (DNN and CNN) and the most successful results were tried to be determined. The success of deep learning models was calculated separately with both DNN and CNN, and accuracy results are presented comparatively for both training and test data. In addition to accuracy results, complexity matrices and ROC analyzes were also performed.

2.1.1. Derin Sinir Ağları (DNN)

Deep neural networks (DNN) are a subset of artificial neural networks (ANN). ANNs are artificial learning models that function similarly to neural networks in the human brain. DNNs are multilayer ANNs. It means that they contain a set of neurons that calculate the inputs of the next layer using the outputs of the neurons in each layer [19].

DNNs work by training on the training dataset. The training dataset contains a set of examples with the class or label of each example. Using the training dataset, DNN learns a model to assign input data to the relevant class or label. DNNs work using a series of mathematical operations. These operations are used to calculate the outputs of neurons in each layer. DNNs use optimization algorithms to improve their accuracy.

The strengths of DNNs are:

- Ability to handle complex data sets
- High accuracy
- Automatic feature extraction

The weaknesses of DNNs are:

- Education time
- Need for data pre-processing
- Tendency to overlearning

The mathematical foundations used in DNNs form the basis for understanding how DNNs work. Understanding these basics will help you use DNNs effectively and improve their performance. The mathematical foundations used in DNNs are:

- Linear algebra: The basis of DNNs is linear algebra. Linear algebra is a branch of mathematics dealing with vectors and matrices. DNNs use linear algebra concepts to calculate the outputs of neurons in each layer.
- Probability: DNNs use probability concepts to learn from training data. By learning about the probability distributions of examples in training data, DNNs improve the ability to accurately classify or predict new examples.
- Optimization: DNNs use optimization algorithms to improve their accuracy. Optimization algorithms adjust the weights and layer sizes of DNNs to best fit the training data.

Some of the linear algebra concepts that form the basis of DNNs are:

o Vectors

o Matrices

o Scalars

Multiplication

o Collection

o Transpose

• The way DNNs learn from training data using probability concepts can be explained as follows:

o DNN represents each sample in the training data as a vector representing a probability distribution.

o By learning about these probability distributions, DNN can improve its ability to accurately classify or predict new samples.

• Some of the optimization algorithms used to increase the accuracy of DNNs are:

o Gradient descent

o Stochastic gradient descent that man

2.1.2. Konvolüsyonel Sinir Ağları (CNN)

Convolutional neural networks (CNN) are one of the most successful models in the field of deep learning. CNNs can achieve high accuracy, especially in visual data-related tasks such as image processing and natural language processing. CNNs operate on two-dimensional data such as images. CNNs work by focusing on each part of the image. This enables CNNs to better learn important features of the image [20]. The CNN layer structure is shown in Figure 1 and consists of the following layers:

Convolution layer: Convolution is the process of moving a filter over an image. The filter is designed to highlight certain features of the image. The convolution process can be explained as follows:

• A filter is a matrix with a set of weights.

• The filter is moved over the image.

• Each filter weight is multiplied by the image pixels under the filter.

• These products form the output matrix of the filter.

The filter is designed to highlight certain features of the image. For example, an edge filter is designed to emphasize the density of edges in the image.

Pooling Layer: This layer, added to the convolution layers, prevents inconsistencies in the network by reducing the parameters in the calculation and network structure. The most commonly used pooling layer is the maximum pooling layer.

Maximum pooling: Maximum pooling is the process of selecting the largest value from parts of an image of a certain size. Maximum pooling is used to reduce the size of the image and preserve its important features. Maximum pooling reduces the size of the image, allowing the CNN to run faster and more efficiently. Additionally, maximum pooling helps preserve important features of the image.

The maximum pooling process can be described as follows:

- The maximum pooling window represents a portion of an image at a specific size.

- The maximum pooling window is moved over the image.

- For each maximum pooling window, the largest value within the window is selected.

Flattening Layer: Prepares all data for the last layer (Fully Connected Layer) by turning it into vectors.

Fully Connected Layer: The information received as a one-dimensional vector from the flattening layer is input to the network structure and the training process begins.

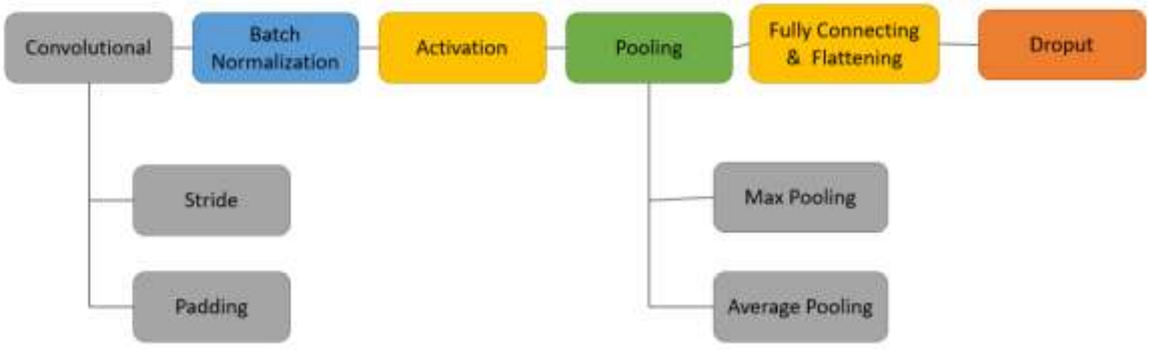

Figure 1 – CNN layer structure

The strengths of CNNs are:

- They can achieve high accuracy in tasks related to visual data.

- They can work even on low-dimensional datasets.

- They have the ability to learn autonomously.

The weaknesses of CNNs are:

- Training processes can be complex and time consuming.

- They are prone to overlearning.

CNNs are one of the fastest growing areas in artificial intelligence. CNNs have managed to achieve human-level or near-human-level performance on a variety of tasks. CNNs will continue to evolve in the future, performing more complex tasks and automating more human activities [21].

In general, the mathematical foundations used in convolutional neural networks form the basis for understanding how CNNs work. Understanding these basics will help you use CNNs effectively and improve their performance.

III. EXPERIMENTAL STUDY

In this study, Carnegie-Mellon University (CMU) keyboard stroke timing data, which has 20400 records with 34 features belonging to 51 individuals, where each individual entered their password at different times, was used. This data set contains information about the keyboard dynamics of 51 individuals, and each individual entered his password 50 times in total in 8 sessions. For each individual, there is a timing between entering their password in different sessions.

Table 1 shows the success rates of all data, training and test data according to DNN and CNN results. The results were taken according to 100 epochs, 50 batches and validation accuracy for hyperparameters, stopping if they did not increase 10 times. In the results obtained for 100 epochs, it was observed that the CNN model gave more successful results than the DNN model.

Table 1-Results of deep learning models

Data / Hyperparameter optimization	**DNN**	**CNN**
Train Data	96.98	98.90
Test Data	91.99	93.51

3.1. DNN RESULTS

In our study, the results of the DNN model were taken separately for training and testing, and more detailed analysis was performed with ROC analyses. The complexity matrix of some randomly selected classes for the training data of the DNN model, calculated according to the hyper parameters that give the most optimum result, is shown in Figure 2.

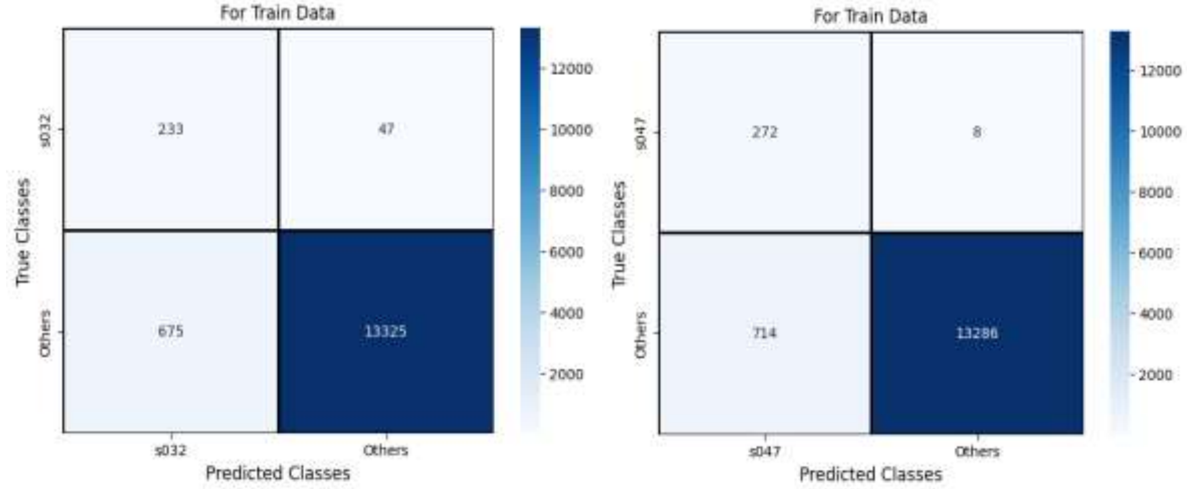

Figure 2 - Confusion matrix for training data

Figure 3 shows the complexity matrices of some randomly selected classes for the test data in the DNN model, according to the most optimal hyperparameter selection.

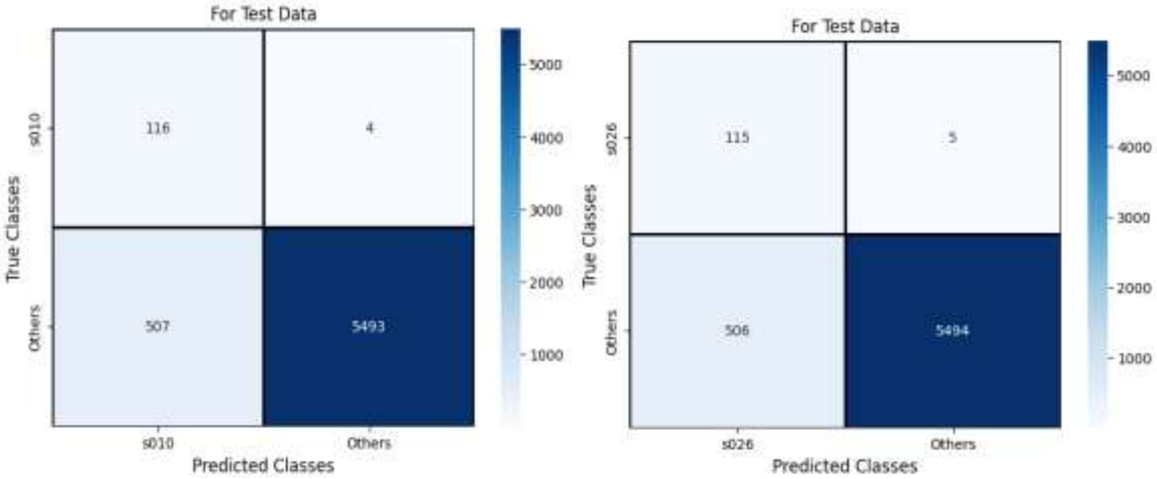

Figure 3 - Confusion matrix for test data

Figure 4 shows the ROC graph according to the most optimal hyperparameter selection for the training data in the DNN model.

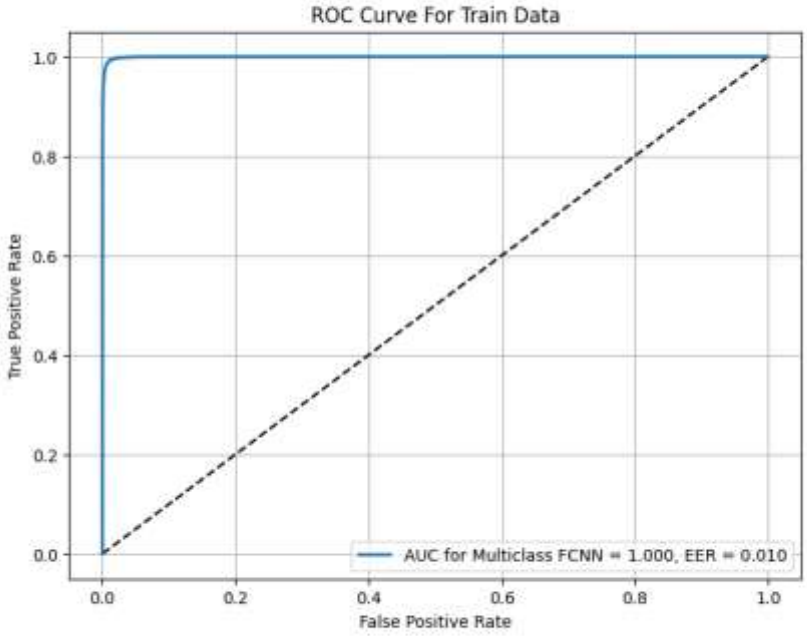

Figure 4 - ROC analysis for training data

Figure 5 shows the ROC graph according to the most optimal hyperparameter selection for the test data in the DNN model

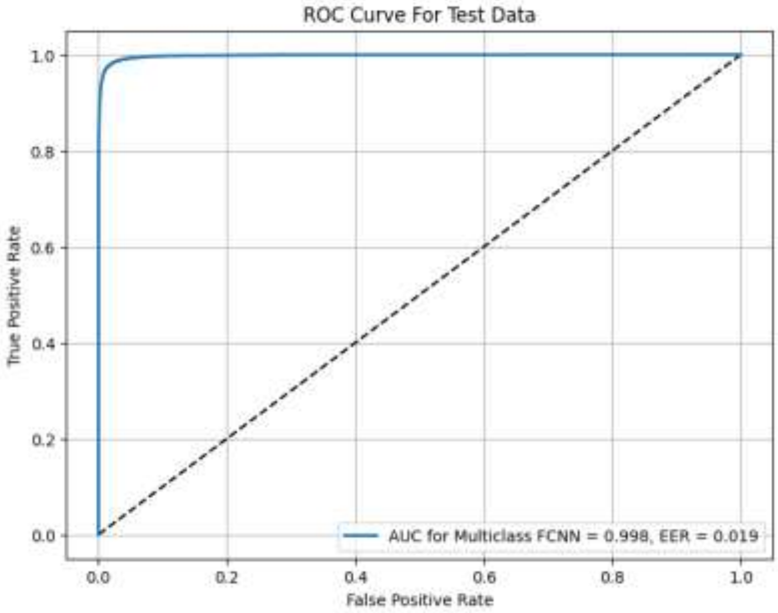

Figure 5 - ROC analysis for test data

The best learning is achieved by updating the weights in the classification accuracy graph given in Figure 6.

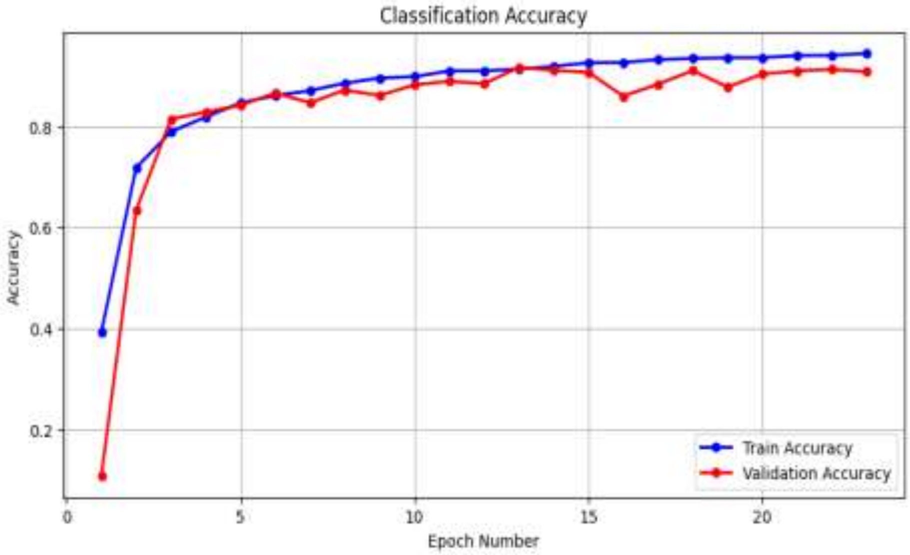

Figure 6 - Classification Accuracy

The change in cross entropy error values for the data set we used is shown according to epoch values in Figure 7.

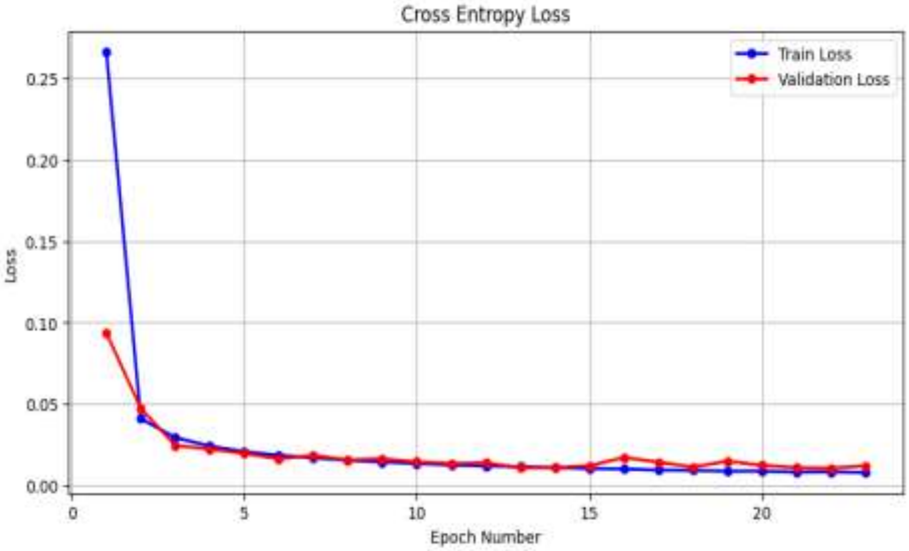

Figure 7 - Cross Entropy Loss

3.2. CNN RESULTS

In our study, the results of the CNN model were taken separately for training and testing, and more detailed analysis was performed with ROC analyses. The complexity matrix of some randomly selected classes for the training data of the CNN model, calculated according to the hyper parameters that give the most optimum result, is shown in Figure 8.

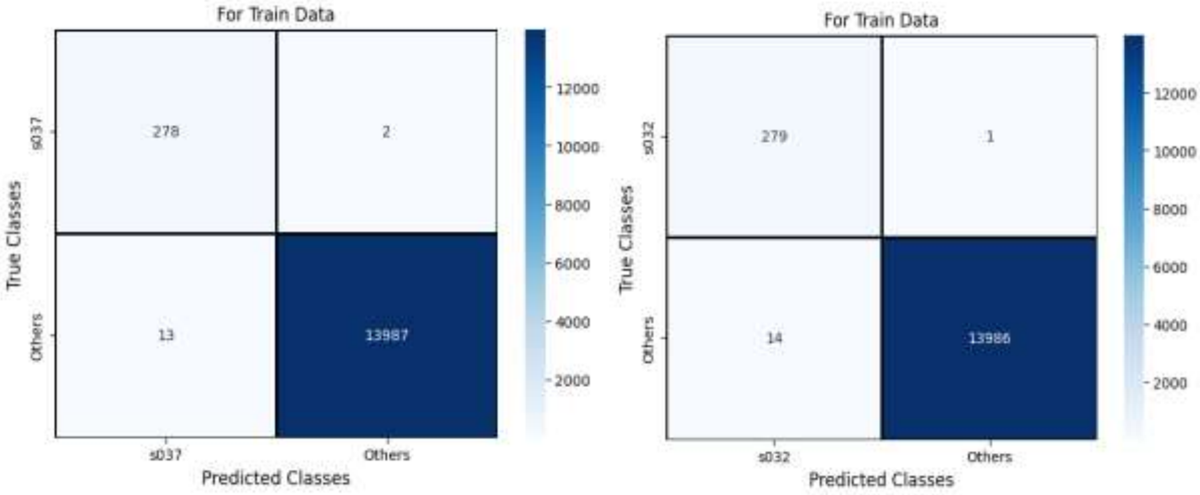

Figure 8 - Confusion matrix for training data

Figure 9 shows the complexity matrices of some randomly selected classes for the test data in the DNN model, according to the most optimal hyperparameter selection.

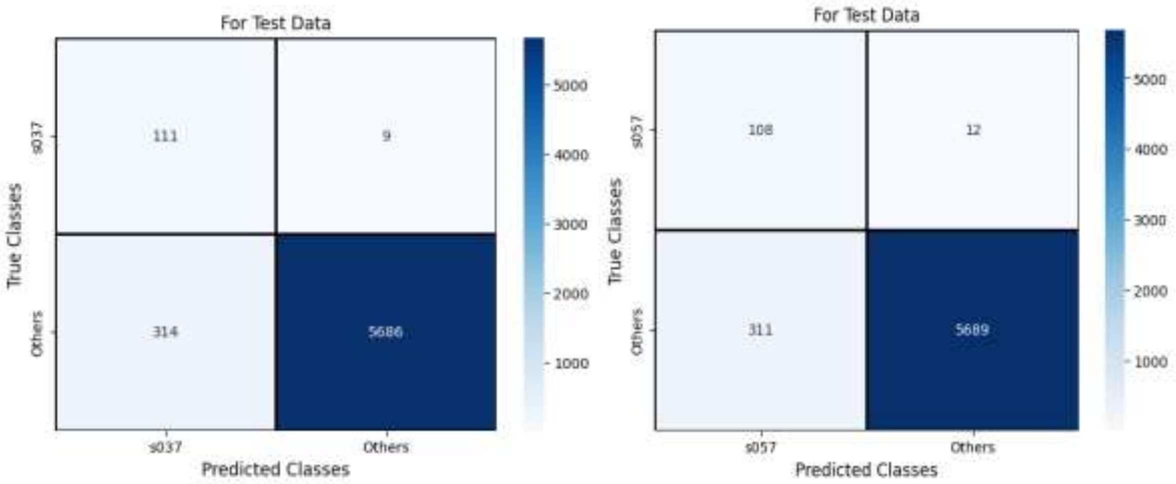

Figure 9 - Confusion matrix for training data

Figure 10 shows the ROC graph according to the most optimal hyperparameter selection for the training data in the DNN model.

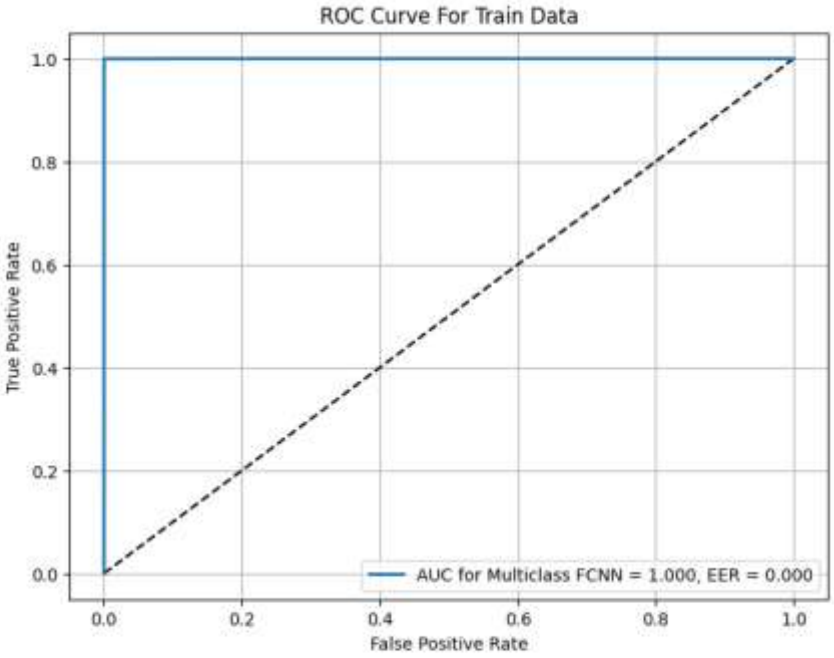

Figure 10 - ROC analysis for training data

Figure 11 shows the ROC graph according to the most optimal hyperparameter selection for the test data in the DNN model.

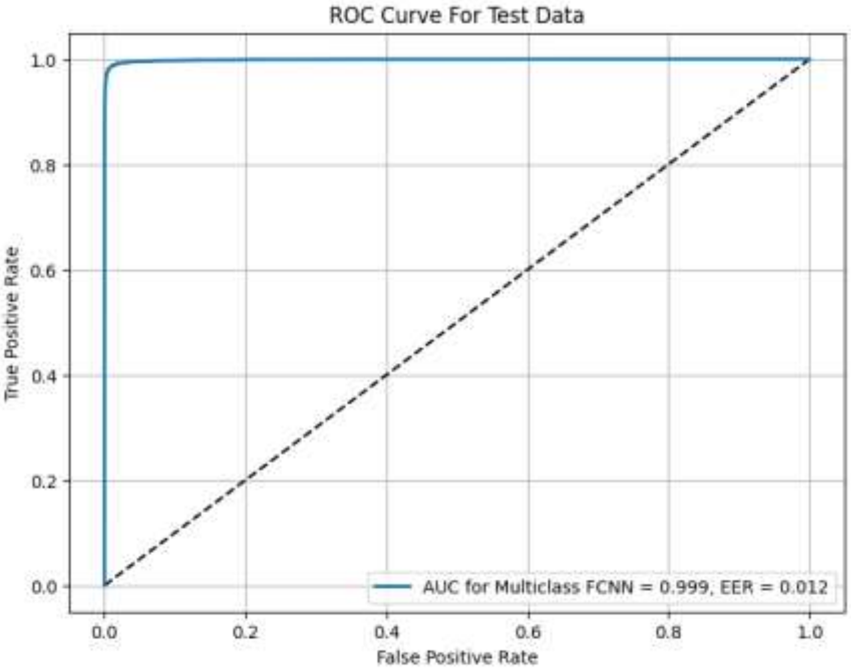

Figure 11 - ROC analysis for test data

The best learning is achieved by updating the weights in the classification accuracy graph given in Figure 12.

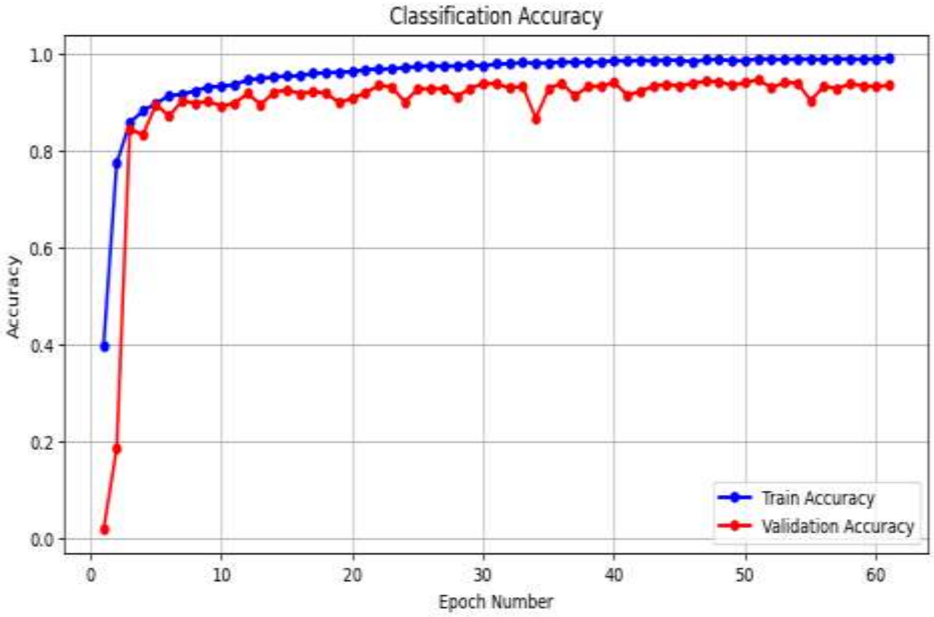

Figure 12 - Classification Accuracy

The change in cross entropy error values for the data set we used is shown according to epoch values in Figure 13.

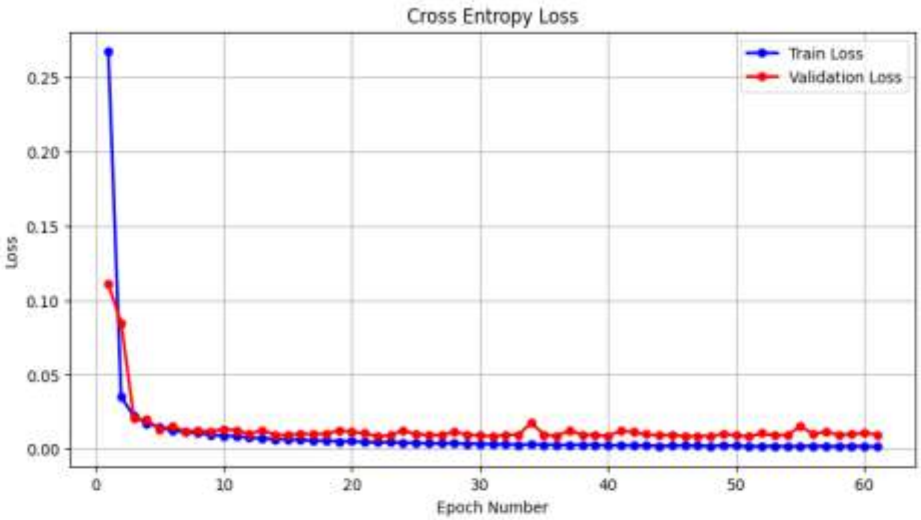

Figure 13 - Cross Entropy Loss

IV. CONCLUSION

With the development of technology, the need for digital transactions such as online shopping has also increased. With the increase in these needs and the increasing reliance on continuous digital transactions, a number of security issues have emerged such as data sharing, data inconsistency, authorization and access to data. In particular, some identification and verification methods are needed to determine whether the users verifying the system are real persons. It is very difficult to identify fake users using the system by performing reliable authentication. In this study, deep learning models with a unique network structure were developed to solve these problems.

Our study was carried out in two steps. In the first step, some preprocessing steps were carried out to ensure that the CMU data used in our study was in the desired format and smooth. This data set consists of 52 users entering their passwords into the system at different time intervals. It includes different writing and behavioral styles of users. Keystroke dynamics are used to ensure password security in the system. In the second step, the accuracy and success of the proposed models were calculated by using different hyperparameters of deep learning models such as DNN and CNN. Training and testing accuracy for DNN achieved 96.98% and 91.99% respectively; CNN achieved 98.90% and 93.51% success in training and testing accuracy, respectively. CNN gave more successful results than the DNN model. Our study was modeled with a different network structure, and the success of these models was demonstrated with classification accuracy and cross entropy loss graphs, and their effects on training and testing success in keystroke dynamics data, where user behavior constantly changes at different time intervals. In addition, the graphs of the accuracy results of both training and test data are shown separately in our study, and the multi-classification results for the data set used are explained in detail. Thus, malicious attackers entering the system are detected with the authentication application and multiple authentication has been developed.

In future studies, different network structures and different deep learning models will be designed and their success will be observed for different authentication systems. Additionally, the proposed models with different evaluation criteria will be analyzed in large data sets.

REFERENCES

1) Ali, H., & Salami, M. J. (2009, March). Keystroke pressure based typing biometrics authentication system by combining ANN and ANFIS-based classifiers. In *2009 5th International Colloquium on Signal Processing & Its Applications* (pp. 198-203). IEEE.

2) Baynath, P., Soyjaudah, K. S., & Khan, M. H. M. (2017, December). Keystroke recognition using chaotic neural network. In *2017 3rd Iranian Conference on Intelligent Systems and Signal Processing (ICSPIS)* (pp. 59-63). IEEE.

3) Anagun, A. S. (2002). Designing a neural network based computer access security system: keystroke dynamics and/or voice patterns. *International Journal of Smart Engineering System Design*, *4*(2), 125-132.

4) Lin, C. H., Liu, J. C., & Lee, K. Y. (2018). On neural networks for biometric authentication based on keystroke dynamics. *Sensors and materials*, *30*(3), 385-396.

5) Mao, R., Wang, X., & Ji, H. (2022, October). ACBM: attention-based CNN and Bi-LSTM model for continuous identity authentication. In *Journal of Physics: Conference Series* (Vol. 2352, No. 1, p. 012005). IOP Publishing.

6) Aversano, L., Bernardi, M. L., Cimitile, M., & Pecori, R. (2021). Continuous authentication using deep neural networks ensemble on keystroke dynamics. *PeerJ Computer Science*, *7*, e525.

7) Kiyani, A. T., Lasebae, A., Ali, K., Rehman, M. U., & Haq, B. (2020). Continuous user authentication featuring keystroke dynamics based on robust recurrent confidence model and ensemble learning approach. *IEEE Access*, *8*, 156177-156189.

8) Çevik, N., Akleylek, S., & Koç, K. Y. (2021, September). Keystroke Dynamics Based Authentication System. In *2021 6th International Conference on Computer Science and Engineering (UBMK)* (pp. 644-649). IEEE.

9) Maharjan, P., Shrestha, K., Bhatta, T., Cho, H., Park, C., Salauddin, M., ... & Park, J. Y. (2021). Keystroke dynamics based hybrid nanogenerators for biometric authentication and identification using artificial intelligence. *Advanced Science*, *8*(15), 2100711.

10) Piugie, Y. B. W., Di Manno, J., Rosenberger, C., & Charrier, C. (2022, September). Keystroke dynamics based user authentication using deep learning neural networks. In *2022 International Conference on Cyberworlds (CW)* (pp. 220-227). IEEE.

11) Lu, X., Zhang, S., Hui, P., & Lio, P. (2020). Continuous authentication by free-text keystroke based on CNN and RNN. *Computers & Security*, *96*, 101861.

12) Andrean, A., Jayabalan, M., & Thiruchelvam, V. (2020). Keystroke dynamics based user authentication using deep multilayer perceptron. *International Journal of Machine Learning and Computing*, *10*(1), 134-139.

13) Çeker, H., & Upadhyaya, S. (2017, December). Sensitivity analysis in keystroke dynamics using convolutional neural networks. In *2017 IEEE workshop on information forensics and security (WIFS)* (pp. 1-6). IEEE.

14) Acien, A., Morales, A., Monaco, J. V., Vera-Rodriguez, R., & Fierrez, J. (2021). TypeNet: Deep learning keystroke biometrics. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *4*(1), 57-70.

15) Piugie, Y. B. W., Di Manno, J., Rosenberger, C., & Charrier, C. (2022, September). Keystroke dynamics based user authentication using deep learning neural networks. In *2022 International Conference on Cyberworlds (CW)* (pp. 220-227). IEEE.

16) Alpar, O. (2017). Frequency spectrograms for biometric keystroke authentication using neural network based classifier. *Knowledge-Based Systems*, *116*, 163-171.

17) Tse, K. W., & Hung, K. (2020, April). User behavioral biometrics identification on mobile platform using multimodal fusion of keystroke and swipe dynamics and recurrent neural network. In *2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE)* (pp. 262-267). IEEE.

18) Shen, X., Ni, Z., Liu, L., Yang, J., & Ahmed, K. (2021). WiPass: 1D-CNN-based smartphone keystroke recognition using WiFi signals. *Pervasive and Mobile Computing*, *73*, 101393.

19) Gabralla, L. A. (2020). Dense Deep Neural Network Architecture for Keystroke Dynamics Authentication in Mobile Phone. *Adv. Sci. Technol. Eng. Syst. J*, *5*(6), 307-314.

20) Dwivedi, C., Kalra, D., Naidu, D., & Aggarwal, S. (2018, November). Keystroke dynamics based biometric authentication: A hybrid classifier approach. In *2018 IEEE symposium series on computational intelligence (SSCI)* (pp. 266-273). IEEE.

21) Xiaofeng, L. U., Shengfei, Z. H. A. N. G., & Shengwei, Y. I. (2018). Free-text keystroke continuous authentication using CNN and RNN. *Journal of Tsinghua University (Science and Technology)*, *58*(12), 1072-1078.