Dynamic Keystroke Technique for a Secure Authentication System based on Deep Belief Nets

Asia Othman Aljahdali
College of Computer Science and Engineering, University of Jeddah, Saudi Arabia
aoaljahdali@uj.edu.sa (corresponding author)

Fursan Thabit
Department of Computer Engineering, Faculty of Engineering, Ege University, Turkey
fursan.thabit@mail.ege.edu.tr

Hanan Aldissi
College of Computer Science and Engineering, University of Jeddah, Saudi Arabia
haldissi.stu@uj.edu.sa

Wafaa Nagro
College of Computer Science and Engineering, University of Jeddah, Saudi Arabia
wnagro.stu@uj.edu.sa

Received: 10 March 2023 | Revised: 9 April 2023 | Accepted: 14 April 2023

 DOI: https://doi.org/10.48084/etasr.5841

ABSTRACT

The rapid growth of electronic assessment in various fields has led to the emergence of issues such as user identity fraud and cheating. One potential solution to these problems is to use a complementary authentication method, such as a behavioral biometric characteristic that is unique to each individual. One promising approach is keystroke dynamics, which involves analyzing the typing patterns of users. In this research, the Deep Belief Networks (DBNs) model is used to implement a dynamic keystroke technique for secure e-assessment. The proposed system extracts various features from the pressure-time measurements, digraphs (dwell time and flight time), trigraphs, and n-graphs, and uses these features to classify the user's identity by applying the DBN algorithm to a dataset collected from participants who typed free text using a standard QWERTY keyboard in a neutral state without inducing specific emotions. The DBN model is designed to detect cheating attempts and is tested on a dataset collected from the proposed e-assessment system using free text. The implementation of the DBN results in an error rate of 5% and an accuracy of 95%, indicating that the system is effective in identifying users' identity and cheating, providing a secure e-assessment approach.

Keywords-keystroke dynamics; Deep Belief Network (DBN); authentication; e-assessment; dwell time; flight time

I. INTRODUCTION

The use of e-assessment has grown rapidly during the recent years. However, there is a growing concern about user authentication. User authentication typically involves three modes: biometrics, possessions, and knowledge. Biometrics refers to unique human characteristics that are difficult to forget, lose, or reproduce, such as fingerprints, face, and iris. Behavioral biometrics, on the other hand, encompasses patterns of human behavior, such as signature, mouse movement, and keystroke dynamics. Keystroke dynamics, based on typing rhythm, is a form of behavioral biometrics that can be used for authentication. Each person's typing rhythm is assumed to be unique, and features such as keystroke duration and finger pressure can be used to create a signature that distinguishes genuine users from imposters. There are various models used to apply keystroke dynamics for authentication, with different accuracy rates. User authentication poses a significant challenge in e-assessment, as institutions strive to improve the credibility of enrolled users and uphold their image and

professionalism. Ensuring the validity of users' identity and detecting fraud, is paramount but challenging due to the complexity of detecting abnormal activities.

This research aims to implement an efficient model that can accurately detect the authenticity of e-users, differentiating between genuine users and impostors, and ensuring robust user authentication to prevent cheating in online examinations. The proposed system utilizes various features, including pressure-time measurements, digraph (dwell time and flight time), tri-graph, and n-graph, extracted from participants who typed a free text using a typical QWERTY keyboard in a neutral state without inducing specific emotions. These features are then used to classify users' identities using the Deep Belief Nets (DBN) algorithm on a collected dataset. By leveraging the DBN model and utilizing multiple features, this research aims to provide a reliable solution for detecting the validity of e-assessment users and for mitigating fraud and cheating, ultimately enhancing the integrity and credibility of the e-assessment process.

A. Problem Statement

The rapid growth of electronic assessment has led to issues such as user identity fraud and cheating, posing a significant challenge to ensure the authenticity of users in e-assessment systems. Traditional authentication methods, such as biometrics, possessions, and knowledge-based approaches, have limitations in accurately detecting fraudulent activities. Therefore, there is a need for an efficient authentication system that can reliably differentiate between genuine and impostor users and prevent cheating in online examinations.

B. Research Objective

The objective of this research is to implement a dynamic keystroke technique for secure authentication in e-assessment systems using DBN. The proposed system aims to extract various features, including pressure-time measurements, digraphs (dwell time and flight time), trigraphs, and n-graphs, from users' typing patterns and utilize the DBN algorithm to accurately classify the user's identity. The goal is to develop a robust and reliable authentication system that can effectively detect the authenticity of e-assessment users and mitigate fraud and cheating.

C. Contribution

This research contributes to the field of secure authentication in e-assessment systems by utilizing keystroke dynamics and DBN algorithm to create a robust and reliable authentication system. The proposed system has the following features:

- Implementation of the Dynamic Keystroke Technique: The proposed system utilizes keystroke dynamics, a behavioral biometric characteristic, as a complementary authentication method to traditional methods. By analyzing users' typing patterns and extracting various features, the system aims to create a unique signature for each user, which can be used to differentiate between genuine and impostor users.
- Utilization of DBN: The proposed system utilizes the DBN algorithm, a type of deep learning model, to accurately classify users' identities. DBN is known for its ability to learn complex patterns from large datasets and has been proven effective in various machine learning tasks. By leveraging the power of DBN, the system aims to achieve high accuracy in identifying users and detecting cheating attempts.
- Multi-Feature Approach: The proposed system extracts multiple features, including pressure-time measurements, digraphs, trigraphs, and n-graphs, from users' typing patterns. This multi-feature approach aims to capture various aspects of users' typing behavior, making the system more robust and reliable in detecting fraudulent activities.
- Error Rate Reduction: The proposed system aims to achieve a low error rate of 5%, indicating its effectiveness in accurately identifying users and detecting cheating attempts. The system's high accuracy of 95% enhances the integrity and credibility of the e-assessment processes, mitigating fraud, and ensuring authenticity.

In conclusion, this research proposes a dynamic keystroke technique for secure authentication in e-assessment systems using DBN, aiming to create a robust and reliable authentication system. The utilization of keystroke dynamics and DBN, along with the multi-feature approach, contributes to the field of secure authentication and has the potential to address the challenges associated with user identity fraud and cheating in e-assessment systems.

II. THE DYNAMIC KEYSTROKE TECHNIQUE

Keystroke dynamics refers to the user's typing rhythm on various digital devices like keyboards, tablets, or mobile device touchscreens, and forms a unique profile (i.e. signature) to clarify each genuine user. The idea behind using keystroke dynamics for user authentication dates back to World War II, where the telegraph machine was used to run the Morse code specified by the rhythm and pace. There are several advantages and limitations to the dynamic keystroke authentication system. Common advantages include the uniqueness of typing patterns for each individual, low deployment cost, reliance on software rather than specialized hardware, and continuous monitoring. However, limitations may arise due to factors such as diversity in typing rhythm, environmental factors, and user injuries, which can result in lower accuracy rates. The dynamic keystroke authentication system typically involves six components, including data collection, feature extraction, feature classification, decision making, retraining, and evaluation. Some research may not include decision making and retraining in the system as shown in Figure 1. The first component in the dynamic keystroke system is data collection, in which data are collected from different input devices. In various systems, gaining data ranges from pressure on a typical keyboard to a sensitive keyboard, such as the mechanical keyboard, smartphone with a touchscreen, or a cellular phone. There are two text input groups: long and short input, the long input as a paragraph, and the short input as the text phrase, username, and password [1].

The second component of the dynamic keystroke system is feature extraction. The data are required to be normalized, processed, and stored for the classification step. Various ways are used for extracting features, the most popular being timing measurements. Basically, keystroke dynamics features depend on the key down, hold, up, and pressure events timing data. When the key is pressed, a timestamp is generated and measured [1]. The generated timestamps are used for calculating the duration and period between keystrokes. The timing features are three: di-graph, tri-graph, and n-graph [3]. Digraph refers to the time latencies between two consecutive key down presses grouped into two categories, including Dwell Time (DT) and Flight Time (FT). Figure 2 shows the differences between DT and FT. DT is the time between pressing and releasing a single key (Hold Time (HT)), and FT is the period between the release of a key and the pressing of the following key (Down-Down Time (DDT) and Up-Down Time (UDT)) [4]. In tri–graphs, the combination of HT to the time delays between every three successive key down presses is considered. N-graphs, are word-specific [3].

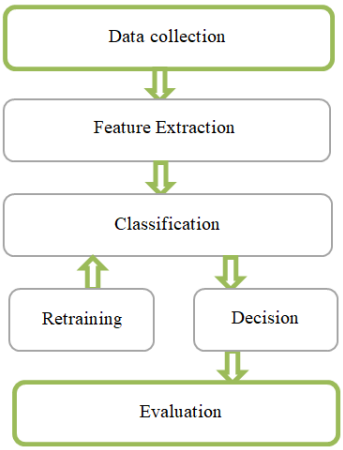

Fig. 1. The general dynamic keystroke authentication system.

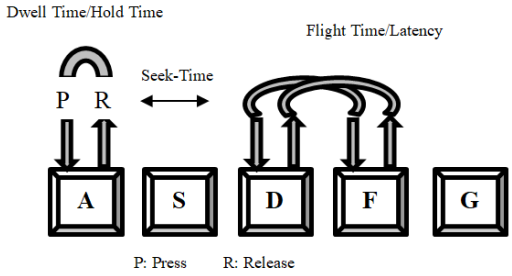

Fig. 2. Dwell time and flight time.

Classification is considered a critical part of any keystroke dynamics system. This component uses the extracting features to make decisions. Statistical and machine-learning methods are used as pattern recognition approaches for increased accuracy. In earlier times, the classification concentrated on statistical approaches, while in modern times, the classification focuses on machine-learning approaches. Researchers in statistical approaches use mean, median and standard deviation measures in keystroke biometrics. While the machine learning approaches use Artificial Neural Networks (ANNs), decision trees, fuzzy logic, and Support Vector Machines (SVMs). Through the decision component, a comparison is established between the previous classification component's output and the design threshold. In authentication, the demandant template is compared to more than one reference, concluding to a final decision to accept or reject the demandant [1]. The retraining component concerns updating the user's reference template to reflect the changes in behavior or environment. Despite this, most researchers do not think about the work on the retention phase. Others suggest an algorithm for this phase that works on renewing the user's reference template due to the changes that occur to the user's typing pattern over time and in different environments [5].

There are basically two main functions for the dynamic keystroke system in the evaluation component: identification and verification. The pretended identity of the user is accepted or denied by the system in the verification stage. In the identification stage, the input pattern is classified into one of the N known classes. The receiver operating characteristic (ROC) curve is used to specify the dynamic keystroke verification system's performance. This curve is used to define the trade-off between the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). FAR, also known as type 2 error rate or false match rate, defines the rate at which the system wrongly accepts a pattern given by an imposter. Lower FAR shows that the system is less likely to accept impostors. FRR, also known as type 1 error rate or false non-match rate, defines the rate at which the system denies a genuine user's pattern. Small FRR shows that the system is less likely to reject genuine users. The Equal Error Rate (EER), also known as the Crossover Error Rate (CER), clarifies the whole system's performance since it refers to the point at which the FAR and FRR are equal. Lower EER means that the system performance becomes better.

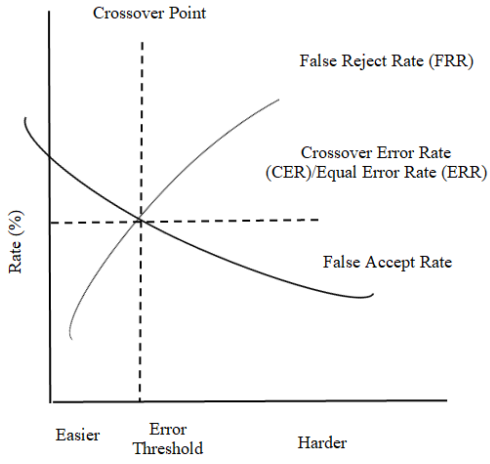

Fig. 3. Relationship between FAR, FRR, and EER.

III. KEYSTROKE MODELLING APPROACHES

A. Support Vector Machines and Artificial Neural Networks

SVM is a machine learning model based on classification algorithms that separates data into two classes. The SVM model can classify new text according to given, labeled training data for each category [6]. The classes are projected into a high-dimensional space and work to get a linear separator between them. "One-class" of SVM variants was developed to detect anomalies. It discovers a separator between the projection and the origin from a single class that presents the data [7]. The utilized ANN consists of three layers: an input layer, an output layer, and a hidden layer that implements the back propagation algorithm. The algorithm memorizes the inter-key delays through a supervised learning mode. The process first initializes the weight matrices between the input and the hidden layers (M1) and between the hidden and the output layers (M2). After some repetitions, the ANN learns the typing pattern of the user. The computed values, including the final M1 and M2, are saved in the user profile, and are later applied to accept or block the user [8].

B. The Gaussian Mixture Model (GMM)

The GMM model is used widely in many statistical modeling tasks. It is a parametric model which uses covariance matrices of Gaussian distributions, mean vectors, and weights of all of the Gaussian components, but considers a nonparametric model once the actual distribution of the data is unknown. Theoretically, the GMM could approximate the arbitrary probability distribution within an appropriate number of mixtures. However, more training data are desired when the number of mixtures is increased to obtain a well-trained model. From the practical side, some measures are used to determine the number of mixtures, which are the amount of the training data, the complexity of the real distribution, and the computation capacity the system can handle. A GMM is a weighted sum of M multivariate Gaussian functions. The probability of a feature vector under the GMM is given in [4]:

$$p(x \mid \lambda) = \sum_{i=1}^{M} p_i b_i(x) \quad (1)$$

where x is a D-dimensional feature vector, $\lambda = \{p_i, \mu_i, \Sigma_i\}$ represents the model parameters, p_i represents the mixture weights for the multivariant Gaussian component densities (x), and μ_i, Σ_i are the mean vector and the covariance matrix for the multi-variant normal distribution.

An incremental GMM model training procedure that began with the single-mixture Gaussian model and used the data to train its parameter was implemented. After that, the single model was divided into two mixture Gaussian models, and the EM (Expectation-Maximization) algorithm was used on the training data to estimate its parameters. The variance floor in GMM is considered a significant parameter. The expected variance will be minimal if there is a tiny sample of the training data. It is not reasonable to estimate the actual variance. In this situation, the floor number is used instead of the estimated variance, which gives the best generalization capability to the model [4].

C. The Gaussian Mixture Model with the Universal Background Model (GMM-UBM)

The UBM is considered a GMM that is trained on a huge quantity of data. The chance of representing a moderate imposter's data will increase for UBM in a positive way once the background subject pool is large enough. So, compared with the genuine user's GMM, the imposter can get a high probability score with UBM. Moreover, the UBM is considered a poor model for the genuine user compared to the GMM because it is trained from a large pool of subjects. From GMM and UBM model scores, a probability ratio test could be processed to produce the authentication decision [4, 9].

D. Deep Belief Nets (DBN)

A DBN is a generative-discriminative hybrid approach in the machine-learning community. It consists of several layers of hidden variables since the DBN is considered a probabilistic generative model. The hidden variables are known as feature detectors because they contain binary values. These hidden layers can be trained one layer at a time, thus, the higher-level layer's input is taken from the lower-level layer's output. The concept of DBN is to create a hierarchical generative model that works to get more sophisticated nonlinear features from the data snapped at each higher-level layer. After that, these pre-trained generative models collapse and work to serve as an initialized ANN for more distinctive parameter fine-tuning. The pre-training of a generative model gives the final model the capability of generalization. Besides that, it simplifies the fine-tuning of the ANN. An ANN quickly falls to local optimals, according to its sensitivity to the model parameter initialization. The DBN is notably helpful in accelerating the ANN training process, not limited only to eschewing the random initialization of ANN parameters [4].

1) Pretraining of RBMs

The DBN training starts with the implementation of a layer-wise unsupervised pretraining of the Restricted Boltzmann Machines (RBMs). The RBMs include two layers: the hidden layer and the visible layer. The visible layer (v) units are adjacent to all hidden layer (h) units with associated weights (W). Connectivity within each layer is not applied. Binary, real, and integer are the kinds of visual layer units that are decided according to the input data type. Binary stochastic variables, $h \in \{0,1\}$ are typically the values of the hidden units. The first layer of RMB uses the Gaussian RBM to model real keystroke timing features. The Gaussian RBM function is [10]:

$$E(v,h;\theta) = \sum_{i=1}^{D} \frac{(v_i - b_i)^2}{2\sigma_i^2} - \sum_{i=1}^{D}\sum_{j=1}^{F} W_{ij} \frac{v_i h_j}{\sigma_i} - \sum_{j=1}^{F} a_j h_j \quad (2)$$

where $\theta = \{W, a, b, \sigma\}$ are parameters specifying the RBM, D is the number of input units, which is equal to the keystroke feature dimension, F is a user-defined parameter specifying the number of hidden units, a is a weight vector for the hidden units, and b and σ are parameters for the input layer.

The input of the higher-level RBMs, or binary RBMs, is taken from the first-layer Gaussian RBM binary output, which is familiar as an automatic feature engineering process. The binary RBMs in the hierarchical generative model include just

binary units for the visible and the hidden layers. RBM's layer-wise maximum likelihood training is computationally intractable since it takes time according to the exponential process. One solution is to apply contrastive divergence [4].

2) Fine Tuning of DBN

The unsupervised pretraining operation output consists of sets of RBMs that could be considered together and appended to a final classification layer to construct an initialized ANN. Figure 4 shows this concept, where both RBMs collapse by sharing the middle units. An additional layer is added to do the process of keystroke classification as a final layer. Final classification parameters could be trained similarly to regular ANN training with back propagation [4].

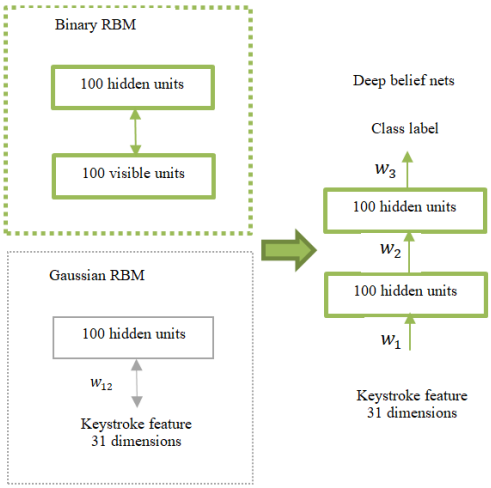

Fig. 4. Two-step training of the DBN for dynamic keystroke authentication. Left: unsupervised training of RBMs, right: converting RBMs into DB.

IV. RELATED WORK

Keystroke dynamics is a behavioral biometric characteristic that can be used to authenticate users based on their typing behavior. Several studies have been conducted on the development of dynamic keystroke authentication systems using various machine learning techniques, including deep learning techniques. These studies aim to improve the accuracy and security of dynamic keystroke authentication systems by exploring different feature extraction methods and machine learning algorithms. In this section, we discuss some of the most relevant studies that have been conducted in this area.

Authors in [4] used a CMU dataset that includes 51 subjects for a static password related to ".tie5Roanl" typed 400 times. The dataset was used to evaluate both the DBN and GMM-UBM models' performances. The experiment resulted in an ERR of 3.5% for the DBN, which was better than the ERR of the GMM-UBM, which was 5.5%. The experiment also compared GMM and GMM-UBM using the same dataset, with GMM resulting in 8.7% ERR, indicating that it was less efficient than the GMM-UBM model. Thus, the DBN model had the most efficient performance compared with other previous models. Authors in [6] used an IDUL dataset consisting of 56 students to detect cheating in online examinations. They applied the SVM model to the dataset, and their experiment resulted in an accuracy rate of 84% and a false positive rate of 8.77%. Authors in [12] proposed a novel keystroke dynamics-based authentication system that used deep learning techniques, specifically triplet loss, to improve security. The system was tested on a dataset consisting of keystroke samples collected from 90 users and achieved an accuracy rate of 99.06%. Authors in [13] explored the use of deep learning techniques, specifically DBNs, to improve the accuracy of keystroke dynamics-based user authentication systems. The proposed system was tested on a dataset consisting of keystroke samples collected from 80 users and achieved an accuracy rate of 99.37%. A novel approach was proposed in [14] to user authentication using keystroke dynamics and deep learning techniques, specifically a Convolutional Neural Network (CNN) and a Long Short-Term Memory (LSTM) network. The proposed system was tested on a dataset consisting of keystroke samples collected from 40 users and achieved an accuracy rate of 99.38%. A secure keystroke dynamics-based authentication system that used DBNs was proposed in [15] to improve the accuracy of user authentication. The system was tested on a dataset consisting of keystroke samples collected from 50 users and achieved an accuracy rate of 99.76%.

Authors in [16] proposed a keystroke dynamics-based user authentication system that used DBNs to improve accuracy and security. The proposed system was tested on a dataset consisting of keystroke samples collected from 60 users and achieved an accuracy rate of 99.32%. The study also explored the impact of various parameters on the accuracy of the proposed system, such as the number of hidden layers in the DBN. A system that used Bidirectional Recurrent Neural Networks (BiRNNs) to improve accuracy was proposed in [17]. The system was tested on a dataset of keystroke samples from 100 users and achieved an accuracy rate of 99.6%. Authors in [18] proposed an ensemble learning approach that combined the outputs of multiple machine learning models, including DBNs and SVMs, to achieve higher accuracy rates. The approach was tested on a dataset of keystroke samples from 80 users and achieved an accuracy rate of 99.83%. Two datasets were examined in [19], one consisting of essay question answers from 81 users and the other consisting of predefined sentences from 168,000 users. The experiment resulted in an error rate (ERR) of 14%, which corresponds to an accuracy rate of 86% for the second dataset. In [20], a system that used soft computing techniques, specifically ANNs and fuzzy logic, to improve accuracy and security was proposed. The system was tested on a dataset of keystroke samples from 50 users and achieved an accuracy rate of 98% [20]. Authors in [21] proposed an enhanced user authentication system that used a multi-level fusion of keystroke dynamics and mouse dynamics. The system was tested on a dataset of keystroke and mouse movement samples from 12 users and achieved an accuracy rate of 99.53% [21]. Authors in [41-43] focused on building models based on genuine users' data only at training time and applying a threshold for each user at testing time to decide on unforeseen data. It has been observed that the Gaussian Mixture Model - Universal Background Model

(GMM-UBM) provided better discrimination capability than GMM when implemented on a large quantity of data, even without access to imposters' data. However, using the SVM approach over a large quantity of unforeseen imposter data did not provide good performance for that type of data.

Table I analyzes various dynamic keystroke authentication models and compares them based on the algorithms used, the dataset type, the extracted features, accuracy, and error rate.

TABLE I. ANALYSIS OF KEYSTROKE DYNAMIC AUTHENTICATION MODELS

Reference	Algorithm	Dataset	Dataset type	Extracted feature	Accuracy	Error rate
[6]	SVM	56 users	Short static text	DT - FT	84%	8.77% false positive rate
[40]	GMM GMM-UBM DBN	51 subjects 400 times	CMU, predefined password	DT - FT	91.3% 94.5% 96.5%	8.7% 5.5% 3.5%
[9]	UBM	168000 users 15 predefined sentences	Predefined sentences	DT - FT	86%	14%

V. THE PROPOSED SOLUTION

In previous studies, dynamic keystroke authentication systems used a dataset of static text (such as predefined passwords or sentences), and extracted features from DT and FT only. The most efficient model identified for keystroke dynamic authentication was a DBN when experimented on CMU (static text). In the proposed system, an e-assessment web application is designed and implemented to collect participants' keystroke datasets with a typical QWERTY keyboard. Di-graph (DT and FT), tri-graph, and n-graph features are extracted by computing the average time of HT-DDT-UDT. The DBN model is used for the classification process on the free-text data entered by participants during the registration process of the proposed e-assessment system. Additionally, a function is introduced to prevent copy-paste from external sources as a measure against cheating. The goal of the system is to detect cheating during online assessment by authenticating participants using keystroke dynamics features. The authentication process consists of the following stages:

1) Participant Registration

Participants enter their information for enrollment and type any text of 12 letters or less five times (Figure 6). This text is used to collect their keystroke dynamics biometric data, which is then stored in the database for later authentication. The participants are also requested to enter their username, password, and email.

2) E-Assessment

After completing the registration process, participants can log into the system and answer questions related to the e-assessment, as shown in Figure 7. On this page, the DBN keystroke model will be executed to perform the classification process and classify the participant as genuine or an imposter. Additionally, the system places constraints to prevent copying answers from external sources and pasting them into the answer field within the e-assessment platform. After the classification process is performed on the assessment page, the system displays the result in a pop-up window as either accepted submission or unauthorized access has been detected.

3) Identity Verification

The system verifies the user's identity by comparing the extracted keystroke dynamics features collected from the current e-assessment answers with the ones that were collected during the registration process and are stored in the database. The system is implemented using PHP and Python programming languages, and Navicat Premium Database is used to develop and manage the system database. Sublime Text, a cross-platform source code editor, is used for coding, which supports various programming and markup languages and provides fast navigation to files and lines, as well as the ability to add functions with plugins [11]. The proposed keystroke dynamic authentication technique can be integrated into any institution, school, or university platform that implements e-assessment to authenticate users.

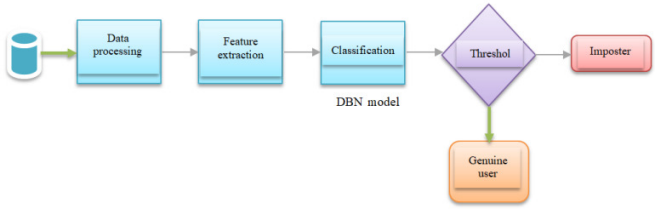

Fig. 5. Data flow diagram.

VI. SYSTEM TESTING AND EXPERIMENTAL RESULTS

This section describes a test conducted on a web application used by graduate students for registration, e-assessment, and identity verification. The test involved 20 graduate students in the first stage and 42 in the second stage aged between 20 and 35, and aimed to assess the application's authentication mechanism and its ability to distinguish between genuine and impostor users.

To collect data for the test, each participant typed a small text 5 times to capture their keystroke patterns. This was done using a QWERTY keyboard in a neutral emotional state. Half samples were used for training and the other half for testing. Randomized impostors were also included in the test to ensure the application's ability to differentiate between genuine and impostor users.

The testing process resulted in an accuracy rate of 95%, meaning that the system correctly identified the user as genuine or impostor 95% of the time. Overall, the test suggests that the application is efficient in identifying genuine users with a low error rate.

Fig. 6. Typing keystroke pattern page.

TABLE II. EXPERIMENTAL RESULTS

Algorithm	Dataset	Features extracted	Accuracy rate	Error rate
DBN	20 users typing 5 times a text of 12 letters or less	(HT-UDT-DDT) DT, FT, tri-graph, n-graph	95%	5%
DBN	42 users typing 200 times a text of 12 letters	(HT-UDT-DDT) DT, FT, tri- graph, n-graph	95%	5%

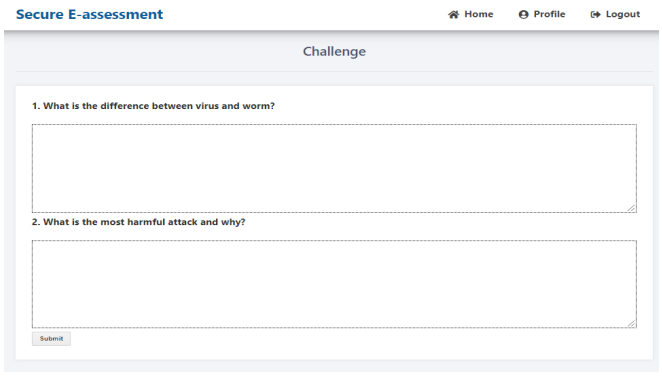

Fig. 7. E-assessment exam page.

VII. DISCUSSION

In our experiment, we aimed to assess the performance of the proposed approach in addressing the three main challenges in Dynamic Keystroke Technique for a Secure Authentication System. These challenges are reducing authentication delay, achieving high verification accuracy, and resisting forgery. To test the authentication delay, we examined short blocks of text with different sizes, including 500, 280, and 140 characters. Our approach achieved very good accuracy on these datasets, surpassing the results of other studies as shown in Table III. While accuracy is typically measured using Type 1 and Type 2 errors, some studies only used the true match rate as their metric. The scientific contribution of the work/results presented in this paper can be summarized as follows:

1. Improved authentication system: the proposed keystroke dynamic technique based on DBNs offers an improved e-assessment authentication system. By analyzing various features extracted from the pressure-time measurements, digraphs, tri-graphs, and n-graphs, the system is able to accurately classify users' identities with an accuracy rate of 95%. This indicates that the system is effective in detecting cheating attempts and providing a secure approach for e-assessments.
2. Enhanced security: the use of keystroke dynamics as a behavioral biometric characteristic adds an additional layer of security to online assessments. Traditional authentication methods such as passwords or pins can be easily compromised, while keystroke dynamics are unique to each individual and difficult to replicate. By implementing the proposed keystroke dynamic technique, the system enhances the security of e-assessment platforms, preventing user identity fraud and cheating.

TABLE III. COMPARATIVE SUMMARY OF STANDARD DEEP KDBRSS

Reference	Authentication	Deep model	Dataset		Device	Performance metric
[23]	Continuous	GRU-BRNN	Fr	P	SP	EER: 8.42% Accuracy: 94.24%, on 5 keystrokes
[24]	Continuous	Bi-LSTM	Fr	B	KB	EER: 8.28% on 30 keystrokes
[25]	One-time	CNN+GRU	Fr	B	KB	Accuracy: 99.31%, EER: 0.069
[26]	One-time	LSTM	Fr	B	KB+ SP	EER: 2.2% and 9.2% for KB and SP
[27]	One-time	CNN+RNN	Fr	B	KB	Accuracy: 98.56% & 91.9% on two datasets
[28]	One-time	Multi-stream RNN	Fx	P	SP	Accuracy: 92.41% and 94.26% for early and late fusion
[29]	Continuous	CNN+RNN	Fr	B	KB	EER: 2.67% and 5.97% on two datasets
[30]	One-time	Siamese RNN	Fr	B	KB	EER: 4.8%
[31]	One-time	CNN	Fx	B	KB	EER: 0.009 and ZM-FAR: 0.027
[32]	One-time	CNN	Fx	P	Mobile	Accuracy: 90.5% and 78.2% for long and short PINs
[33]	One-time	DBN	Fx	P	KB	Accuracy: 98.01%
[34]	One-time	ML-FFNN	Fx	P	KB	Accuracy: 97%
[35]	One-time	CNN	Fx	P	KB	Accuracy: 97%
[36]	Continuous	CNN	Fr	P	KB	Accuracy: 92.58%, FAR: 0.24%, FRR:7.34%
[37]	One-time	ML-FFNN	Fx	B	KB	Accuracy: 92.60%
[38]	One-time	CNN	Fx	B	KB	EER: 2.3%
[39]	One-time	ML-FFNN	Fx	B	KB	Accuracy: 93.59%, EER: 0.030
[40]	One-time	DBN	Fx	B	Mobile	EER: 2.8%
Proposed	One-time	DBN	Fx	B		Accuracy: 95%%, EER: 5%

3. Real-time authentication: the proposed system offers real-time authentication during the e-assessment process. Participants are required to type a text during registration, and their keystroke dynamics are collected and stored. This allows continuous monitoring of user's identity during the assessment process, ensuring that only genuine participants are able to access and answer the questions.
4. Prevention of copy-paste cheating: the proposed system includes a function to prevent copy-paste from external sources as a measure against cheating. This helps to ensure that participants do not copy answers from external sources and paste them into the answer field within the e-assessment platform, further enhancing the integrity of the assessment process and reducing the possibility of cheating.
5. Practical application: the proposed keystroke dynamic authentication technique can be easily integrated into any institution, school, or university platform that implements e-assessments. The system is implemented using php and Python programming languages, which are widely used in web development, making it practical and feasible for implementation in real-world e-assessment scenarios.

In conclusion, the work presented in this paper offers an improved authentication system for e-assessments based on keystroke dynamics and DBNs. The system enhances the security of online assessments, provides real-time authentication, prevents copy-paste cheating, and has practical application potential. The experimental results demonstrate the effectiveness of the proposed system in identifying user identity and detecting cheating attempts, making it a significant contribution to the field of secure authentication for online assessments.

VIII. CONCLUTION AND FUTER WORK

Keystroke dynamics techniques have various uses in different domains. Recently, they have been used in the authentication domain. In the current research, we applied the dynamic keystroke technique in an e-assessment platform to support the building of an authenticated platform. The experimental result shows that applying the DBN model over free text is efficient in cheating detection in e-assessments according to the accuracy rate (95%).

We have encountered some challenges during the implementation of the DBN model on free text data, since the model needs a large amount of data in addition to the time needed to train it. As future work, this application can also be extended to include other types of authentication techniques, such as face recognition, voice recognition, and mouse movement, besides keystroke dynamics.

REFERENCES

[1] M. L. Ali, J. V. Monaco, C. C. Tappert, and M. Qiu, "Keystroke Biometric Systems for User Authentication," *Journal of Signal Processing Systems*, vol. 86, no. 2, pp. 175–190, Mar. 2017, https://doi.org/10.1007/s11265-016-1114-9.

[2] R. S. Gaines, W. Lisowski, S. J. Press, and N. Shapiro, "Authentication by Keystroke Timing: Some Preliminary Results," Rand, Santa Monica, CA, USA, R-256-NSF, 1980.

[3] T. Sim and R. Janakiraman, "Are Digraphs Good for Free-Text Keystroke Dynamics?," in *IEEE Conference on Computer Vision and Pattern Recognition*, Minneapolis, MN, USA, Jun. 2007, pp. 1–6, https://doi.org/10.1109/CVPR.2007.383393.

[4] Y. Deng and Y. Zhong, "Keystroke Dynamics User Authentication Based on Gaussian Mixture Model and Deep Belief Nets," *International Scholarly Research Notices*, vol. 2013, Oct. 2013, Art. no. e565183, https://doi.org/10.1155/2013/565183.

[5] D. Hosseinzadeh and S. Krishnan, "Gaussian Mixture Modeling of Keystroke Patterns for Biometric Applications," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 38, no. 6, pp. 816–826, Aug. 2008, https://doi.org/10.1109/TSMCC.2008.2001696.

[6] T. Eude and C. Chang, "One-class SVM for biometric authentication by keystroke dynamics for remote evaluation," *Computational Intelligence*, vol. 34, no. 1, pp. 145–160, 2018, https://doi.org/10.1111/coin.12122.

[7] K. S. Killourhy and R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," in *IEEE/IFIP International*

Conference on Dependable Systems & Networks, Lisbon, Portugal, Jun. 2009, pp. 125–134, https://doi.org/10.1109/DSN.2009.5270346.

[8] S. Haider, A. Abbas, and A. K. Zaidi, "A multi-technique approach for user identification through keystroke dynamics," in *ieee international conference on systems, man and cybernetics. "cybernetics evolving to systems, humans, organizations, and their complex interactions" (cat. no.0*, Nashville, TN, USA, Oct. 2000, vol. 2, pp. 1336–1341, https://doi.org/10.1109/ICSMC.2000.886039.

[9] R. Mattsson, "Keystroke dynamics for student authentication in online examinations," M.S. thesis, Lulea University of Technology, Lulea, Sweden, 2020.

[10] R. Salakhutdinov, "Learning Deep Generative Models," *Annual Review of Statistics and Its Application*, vol. 2, no. 1, pp. 361–385, 2015, https://doi.org/10.1146/annurev-statistics-010814-020120.

[11] D. Peleg, *Mastering Sublime Text*. Birmingham, UK: Packt Publishing, 2013.

[12] A. Tewari, "Keystroke Dynamics based Recognition Systems using Deep Learning: A Survey." TechRxiv, Apr. 11, 2022, https://doi.org/10.36227/techrxiv.19532269.v1.

[13] Y. B. W. Piugie, J. Di Manno, C. Rosenberger, and C. Charrier, "Keystroke Dynamics based User Authentication using Deep Learning Neural Networks," in *2022 International Conference on Cyberworlds (CW)*, Kanazawa, Japan, Sep. 2022, pp. 220–227, https://doi.org/10.1109/CW55638.2022.00052.

[14] K. Shekhawat and D. P. Bhatt, "A novel approach for user authentication using keystroke dynamics," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 7, pp. 2015–2027, Oct. 2022, https://doi.org/10.1080/09720529.2022.2133241.

[15] Y. Deng and Y. Zhong, "Keystroke Dynamics User Authentication Based on Gaussian Mixture Model and Deep Belief Nets," *International Scholarly Research Notices*, vol. 2013, Oct. 2013, Art. no. e565183, https://doi.org/10.1155/2013/565183.

[16] Y. B. W. Piugie, J. Di Manno, C. Rosenberger, and C. Charrier, "Keystroke Dynamics based User Authentication using Deep Learning Neural Networks," in *International Conference on Cyberworlds*, Kanazawa, Japan, Sep. 2022, pp. 220–227, https://doi.org/10.1109/CW55638.2022.00052.

[17] S. L. Albuquerque, C. J. Miosso, A. F. da Rocha, and P. L. R. Gondim, "Multi-Factor Authentication Protocol Based on Electrocardiography Signals for a Mobile Cloud Computing Environment," in *Mobile Computing Solutions for Healthcare Systems*, R. Sivakumar, D. Velev, B. Alhadidi, S. Vidhya, S. V. Francis, and B. Prabadevi, Eds. Bentham Books, 2023, pp. 62–88.

[18] A. Alsultan, K. Warwick, and H. Wei, "Improving the performance of free-text keystroke dynamics authentication by fusion," *Applied Soft Computing*, vol. 70, pp. 1024–1033, Sep. 2018, https://doi.org/10.1016/j.asoc.2017.11.018.

[19] A. Andrean, M. Jayabalan, and V. Thiruchelvam, "Keystroke Dynamics Based User Authentication using Deep Multilayer Perceptron," *International Journal of Machine Learning and Computing*, vol. 10, no. 1, pp. 134–139, Jan. 2020, https://doi.org/10.18178/ijmlc.2020.10.1.910.

[20] A. Rahman *et al.*, "Multimodal EEG and Keystroke Dynamics Based Biometric System Using Machine Learning Algorithms," *IEEE Access*, vol. 9, pp. 94625–94643, 2021, https://doi.org/10.1109/ACCESS.2021.3092840.

[21] J. Kim, H. Kim, and P. Kang, "Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection," *Applied Soft Computing*, vol. 62, pp. 1077–1087, Jan. 2018, https://doi.org/10.1016/j.asoc.2017.09.045.

[22] I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi, and I. Lai, "Combining Mouse and Keystroke Dynamics Biometrics for Risk-Based Authentication in Web Environments," in *2012 Fourth International Conference on Digital Home*, Guangzhou, China, Aug. 2012, pp. 138–145, https://doi.org/10.1109/ICDH.2012.59.

[23] M. L. Ali, K. Thakur, and M. A. Obaidat, "A Hybrid Method for Keystroke Biometric User Identification," *Electronics*, vol. 11, no. 17, Jan. 2022, Art. no. 2782, https://doi.org/10.3390/electronics11172782.

[24] G. Zhao, Z. Wu, Y. Gao, G. Niu, Z. L. Wang, and B. Zhang, "Multi-Layer Extreme Learning Machine-Based Keystroke Dynamics Identification for Intelligent Keyboard," *IEEE Sensors Journal*, vol. 21, no. 2, pp. 2324–2333, Jan. 2021, https://doi.org/10.1109/JSEN.2020.3019777.

[25] A. Acien, A. Morales, R. Vera-Rodriguez, J. Fierrez, and J. V. Monaco, "TypeNet: Scaling up Keystroke Biometrics," in *IEEE International Joint Conference on Biometrics*, Houston, TX, USA, Sep. 2020, pp. 1–7, https://doi.org/10.1109/IJCB48548.2020.9304908.

[26] A. Acien, A. Morales, J. V. Monaco, R. Vera-Rodriguez, and J. Fierrez, "TypeNet: Deep Learning Keystroke Biometrics," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 4, no. 1, pp. 57–70, Jan. 2022, https://doi.org/10.1109/TBIOM.2021.3112540.

[27] L. Yang, C. Li, R. You, B. Tu, and L. Li, "TKCA: a timely keystroke-based continuous user authentication with short keystroke sequence in uncontrolled settings," *Cybersecurity*, vol. 4, no. 1, May 2021, Art. no. 13, https://doi.org/10.1186/s42400-021-00075-9.

[28] L. Sun *et al.*, "Kollector: Detecting Fraudulent Activities on Mobile Devices Using Deep Learning," *IEEE Transactions on Mobile Computing*, vol. 20, no. 4, pp. 1465–1476, Apr. 2021, https://doi.org/10.1109/TMC.2020.2964226.

[29] J. Li, H.-C. Chang, and M. Stamp, "Free-Text Keystroke Dynamics for User Authentication," Jul. 2021. https://doi.org/10.48550/arXiv.2107.07009.

[30] K.-W. Tse and K. Hung, "User Behavioral Biometrics Identification on Mobile Platform using Multimodal Fusion of Keystroke and Swipe Dynamics and Recurrent Neural Network," in *10th Symposium on Computer Applications & Industrial Electronics*, Kuala Lumpur, Malaysia, Apr. 2020, pp. 262–267, https://doi.org/10.1109/ISCAIE47305.2020.9108839.

[31] X. Lu, S. Zhang, P. Hui, and P. Lio, "Continuous authentication by free-text keystroke based on CNN and RNN," *Computers & Security*, vol. 96, Sep. 2020, Art. no. 101861, https://doi.org/10.1016/j.cose.2020.101861.

[32] N. Altwaijry, "Keystroke Dynamics Analysis for User Authentication Using a Deep Learning Approach," *International Journal of Computer Science and Network Security*, vol. 20, no. 12, pp. 209–216, Dec. 2020, https://doi.org/10.22937/IJCSNS.2020.20.12.23.

[33] E. Maiorana, H. Kalita, and P. Campisi, "Deepkey: Keystroke Dynamics and CNN for Biometric Recognition on Mobile Devices," in *8th European Workshop on Visual Information Processing*, Roma, Italy, Oct. 2019, pp. 181–186, https://doi.org/10.1109/EUVIP47703.2019.8946206.

[34] G. Zhao *et al.*, "Keystroke Dynamics Identification Based on Triboelectric Nanogenerator for Intelligent Keyboard Using Deep Learning Method," *Advanced Materials Technologies*, vol. 4, no. 1, 2019, Art. no. 1800167, https://doi.org/10.1002/admt.201800167.

[35] M. L. Bernardi, M. Cimitile, F. Martinelli, and F. Mercaldo, "Keystroke Analysis for User Identification using Deep Neural Networks," in *International Joint Conference on Neural Networks*, Budapest, Hungary, Jul. 2019, pp. 1–8, https://doi.org/10.1109/IJCNN.2019.8852068.

[36] C.-H. Lin, J.-C. Liu, and K.-Y. Lee, "On Neural Networks for Biometric Authentication Based on Keystroke Dynamics," *Sensors and Materials*, vol. 30, no. 3, pp. 385–396, 2018, https://doi.org/10.18494/SAM.2018.1757.

[37] Y. Muliono, H. Ham, and D. Darmawan, "Keystroke Dynamic Classification using Machine Learning for Password Authorization," *Procedia Computer Science*, vol. 135, pp. 564–569, Jan. 2018, https://doi.org/10.1016/j.procs.2018.08.209.

[38] H. Ceker and S. Upadhyaya, "Transfer learning in long-text keystroke dynamics," in *IEEE International Conference on Identity, Security and Behavior Analysis*, New Delhi, India, Feb. 2017, pp. 1–6, https://doi.org/10.1109/ISBA.2017.7947710.

[39] S. Maheshwary, S. Ganguly, and V. Pudi, "Deep Secure: A Fast and Simple Neural Network based approach for User Authentication and Identification via Keystroke Dynamics," in *First International Workshop on Artificial Intelligence in Security*, Melbourne, VIC, Australia, Aug. 2017, pp. 60–66.

[40] Y. Deng and Y. Zhong, "Keystroke Dynamics Advances for Mobile Devices Using Deep Neural Network," in *Recent Advances in User Authentication Using Keystroke Dynamics Biometrics*, Thrace, Greece: Science Gate Publishing, 2015, pp. 59–70.

[41] A. R. Khan and L. K. Alnwihel, "A Brief Review on Cloud Computing Authentication Frameworks," *Engineering, Technology & Applied Science Research*, vol. 13, no. 1, pp. 9997–10004, Feb. 2023, https://doi.org/10.48084/etasr.5479.

[42] E. S. I. Harba, "Secure Data Encryption Through a Combination of AES, RSA and HMAC," *Engineering, Technology & Applied Science Research*, vol. 7, no. 4, pp. 1781–1785, Aug. 2017, https://doi.org/10.48084/etasr.1272.

[43] S. Hamid, N. Z. Bawany, and S. Khan, "AcSIS: Authentication System Based on Image Splicing," *Engineering, Technology & Applied Science Research*, vol. 9, no. 5, pp. 4808–4812, Oct. 2019, https://doi.org/10.48084/etasr.3060.