Turkish Journal of Computer and Mathematics Education Vol.12 No. 11 (2021), 2382- 2391
Research Article

Touchscreen-based Smartphone Continuous Authentication System (SCAS) using Deep Neural Network

Aws Saood Mohamed Al-Dori [1], Jamal Mohamed Kadhim[2]
[1,2] Department of Computer Science, College of Science, AL-Nahrain University, Baghdad, IRAQ

Email[1]: stcs-asm17@sc.nahrainuniv.edu.iq
Email[2]: drjamal.cs@sc.nahrainuniv.edu.iq

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

ABSTRACT: Due to the huge increasing usage of mobile devices and applications, basic authentication is not a secure choice for a long user session. Therefore, it needs a second layer of protection developed as a seamless and non-intervention security procedure, which is the continuous authentication. A framework analyses behavioral biometrics dataset was designed based on the touch-screen and a user continuous authentication was applied depending on pre-specified acceptance ratio to the portions of the stroke. In this framework, an approach based on a deep learning technique was adopted to train a model able to classify these behavioral data and achieve high accuracy. By comparing with the traditional use of machine learning algorithms that required more processing actions, which it is considered costly from the perspective of execution and the complexity of processing. In general, machine-learning algorithms need to extract statistical features from the raw data before they can work on it directly. The experiences of using machine learning classification algorithms have proven unreliable results when they are using on one behavioral biometrics modality, comparison with our framework that are based on a deep learning technique. The approach designed to apply a deep neural network on behavioral biometric data such as X, Y coordinates; area covered and phone orientation …etc. These features are captured directly from the touchscreen sensor of the smartphone during the user's sessions, to train system able to classify new input data with high accuracy if it is coming from a genuine or fraudulent user, which already was achieved and obtained test accuracy 94.2% with equal error rate (EER 3.46%).

Keywords: AdaMax optimizer, Continuous Authentication, Deep Neural Network, Dropout, Earlystoping.

INTRODUCTION

With the rapid technological advances in the world and the high speeds of the internet spread together with the widest range of smartphones usage. The smartphones became one of the necessary things in our daily life. Because of many features the smartphones contain, in addition to many functions and applications such as social networks, online shopping, mobile games, and private communications and collective, and till now. During the usage of these facilities, the users offer special data like credit card specifics, account credentials and so on, that are usually stored in the smartphones (1). Moreover, if the smartphone gets stolen or lost, this leads to a violation of privacy and steal this important information and the risks involved. Although these devices are secure and private, but are not adequate because of the basic authentication methods that are used such as PIN code and passwords, that are boundaries and defects are stated and recognized in the security field (2). The advanced methods of physical biometrics that are used recently, such as face recognition, fingerprint recognition, and iris recognition to smartphone authentication has reduced user input problems. However, they still have other issues of usability and security (3), for that a new authentication mechanism accurate and easy to use is need. Moreover, the behavior-based authentication solution has recently attracted considerable attention in the market and academic environments. The generality of smartphone users prioritizes security suitability and regards the authentication method more troublesome than other technological issues, like shortage in coverage, energy consuming and so on (4). Recently, the limitations of well-known authentication mechanisms discussed with respect to security and usability. In addition to suggest alternatives to authenticate users in a non-intrusive way, by either minimum or no collaboration through using their behavioral biometrics (5).

RELATED WORK

The purpose of any authentication mechanism is to prevent any unauthorized access to the user's device. The most commonly used authentication schemes for smartphones rely on remembrance challenges, like PIN code, password or even drawing a specified pattern on the touchscreen, where are susceptible to smudge attacks and shoulder-surfing attacks (6). Even with the increasing tendency to authenticate smartphone users by using biometrics recently, such as matching of fingerprint and face recognition (7), they are subject to trials of tricks and broken the authentication security system. In addition to the fact of these mechanisms in apply authentication to the start of the login session only. Therefore, the smartphone will be unsecure during usage.

Because if the smartphone gets stolen during this opened session or sometimes the users put their smartphones in their office during taken a short rest, the intruder may easily take it and access the information he needs. That is commonly occurring in the world, studies stated that about 60 percent of such attacks are done by known peoples they had the chance to get the smart mobile after authentication state (8). Moreover, the increased interesting to the security issues and developing the authentication methods recently, led to emerge the idea of continuous authentication (CA) (9). That after the enrollment phase of users, the system checks the identity of them continuously in non-intervention manner based on the user's biometrics like face recognition by front camera (10), touch screen strokes(11), movement patterns (12) and so on.

1) M. Frank et al, in 2012 (13) starting with the cornerstone of the continuous authentication for smartphones that depends on touch-screen inputs, which are considered as the foundation paper of research in this field. The researcher suggested a system to authenticate the users of smartphones frequently during the usage, according to the behavior of touching the screen of a smartphone. For that, it has been derived a group of 30 behavioral features from the raw-touchscreen records which are already captured from the sensor of the touch-screen. It has proven that the different users qualify to distinguish subspaces of that feature area. In addition, systematic experiments had designed to show how these behavioral patterns have stability over time. For that, it has been collected touch-data from users during interacting with the touch-screen using the basic navigations, such as up-down and left-right scrolling. The researcher proposed a classification system in the term of machine learning, that can learn the touch behavior of a user while the enrollment-phase and have the ability to accept or refuse the user by tracking the interaction with the touchscreen. The researcher had chosen two machine learning (ML) algorithms (KNN and a one-versus-all RBF-SVM), and obtain average equal error rates 2%-3% for inter-session authentication, and around 4% EER while one week after the enrollment-phase. The researcher concluded that the accuracy insufficient for standalone authentication across weeks. Moreover, there is a need to combine this type of modality with other modalities (gait, content behavior, GPS …etc.) to achieve a reliable system.

2) Heather Crawford et al, in 2013 (14) the researcher proposed a continual transparent authentication prototype that merges more than one behavioral biometrics with the basic authentication to execute an easy and continuously authentication method. The tests of security and the ease of use to the suggested framework had appeared that a genuine user of mobile might implement all mobile tasks, and he was required to do basic authenticate 67% less. The researcher choose two behavioral biometrics: keystroke dynamics and speaker verification. The researcher applied five patterns classifiers on the two previous modalities independently for each modality, to determine which pattern classifier provide the lowest error rates. The five classifiers were K-Nearest Neighbor with Euclidean and Manhattan distance measures, Decision Tree, and Naïve Bayes with kernel density and Gaussian measures. The two versions of K-Nearest Neighbor provided the lowest error rates. The study on keystroke dynamics resulted in EER values of approximately 10% and accuracy rates upwards of 80%, while on the speaker verification shows an EER in the 25%. Moreover, the test results have appeared that the impostors dropped in a short time from access on mobile functions as soon as their behavioral biometrics are gathered. These results encouraged the researcher to apply a model of this framework and to supply support for more research in this authentication mechanism on smart phones devices.

3) Cheng Bo et al, in 2013 (15) presented a research paper in which introduced a framework to authenticate users silently and transparently through the use of biometrics for user touch behavior and the use of integrated sensors to capture the precise movement of the device resulting from the user's touch routines. By following the user's touch actions, the researcher builds the owner's touch biometrics model by extracting some key features and then verifying whether the current user is the owner or guest/attacker though applying SVM classification algorithm. When using a smartphone, the user's unique operating mode detected and collected by silently collecting sensor data and touching events. When the users moving, the fine movement of smart phones that results from touching the screen during the use; that recorded as behavioral biometrics, is repressed due to the large-scale user movement that will make this type of biometrics ineffective alone. Addressing that, the researcher has integrated biometrics based on each user's movement together with touch-based biometrics. The researcher conducted comprehensive assessments to the proposed framework on the Android smartphone, and appeared an accuracy of user identification exceeds 99%. The framework could reach over an 80% accuracy within 10 observations for identifying a guest. Overall, in a general scenario, with only one observation, the FAR and FRR are about 20%. Nevertheless, with about 12 observations of various actions, the FAR and FRR are both reduced to nearly zero.

4) Nan Zheng et al, in 2014 (16) presented a research paper comprised that each smartphone user has special behavior while interacting with the touchscreen. This style represents the diversity of rhythm, force and the angle's preferred to these actions. By taking the advantage of the integrated sensors that the smartphones contain, such as accelerometer, gyroscope and touchscreen sensor. The user's printing behavior can be captured transparently and smoothly by extracting the features from these sensors, which are acceleration, pressure, covered area and time of the printing pattern of each user. The researcher suggested a verification framework of the user through a nonintrusive manner to verify if the current user of smartphone is the genuine or an impostor during interacting the user on the touchscreen of the smartphone via the printing state. This classification

approach based on a simple notion of nearest neighbor distance to the training data. A larger distance indicates higher likelihood of being an impostor. Moreover, by testing the behavioral data to 80 users of printing styles to evaluate the effectiveness of the suggested framework. The result of these tests appears that the verification framework obtains equal error rates (EER) between 3.65% and 7.34%. Depending on the test result, the researcher state that the verification framework could be included transparently with the current well-known authentication methods on smartphones.

5) Hui Xu et al, in 2014 (17) presented a research paper stating that current smartphones generally cannot authenticate users during run-time as a continuously manner, and that is poses security and privacy threats. Such as a malicious user can handle the phone if the screen lock is exceeded. To address that, the researcher adopts a continuous and passive authentication mechanism based on a user's touch operations on the touchscreen. This method is appropriate for smartphones because it does not require additional devices or user interface intrusive. He studies how to model multiple types of touch data and perform continuous authentication depending on that. As an initial attempt, he also studied the basics of touch processes as biometrics though justifying their permanence and durability. In addition, a month-long test involving more than 30 users was applied, using touch-screen biometrics as a promising method for continuous authentication. The researcher adopted one of the well-known machine learning algorithm; the Support Vector Machine (SVM), as classifier for the user authentication approach. The test results achieved an EER between 0% to 9.71% depending on the number of operations and the number of observations to each user in the training phase.

6) Stefania Budulan et al, in 2015 (18) the researcher has proposed a method that could be an alternative to the basic authentication mechanisms. In which, the solution offers continuous monitoring to verifying from the user authenticity. Where it has been applied on a dataset of 41 users contain behavioral biometrics of touchscreen, which provides a well beginning to make behavioral profiles for each user whereas are used later to distinguish between the users and classify the strokes to their users. The researcher proposed a framework able to manipulate features extracted from the raw data of the user's touchscreen interactions that captured from the sensor. After the features extracted phase, the researcher applied several models, usually including AdaBoost classifier which is an ensemble method implementing a boosting technique in which many classifiers with weaker performances are built into one stronger classifier, for instance over Decision Tree classifier. The results shown this framework gets an accuracy more than 83%. Moreover, regarding these results the researcher consider this kind of authentication mechanism is workable and could be included as a continuous method of denying the impostors from access to the smartphone applications and information.

7) Rajesh Kumar et al, in 2017 (19) the researcher has been proposed a novel continuous authentication mechanism to authenticate the users of smartphones. The proposed framework depended on the unlabeled unique styles of smartphones movement that have gathered via the smartphone's accelerometer sensor. This data have aggregated from an unlimited environment across five to twelve days. The patterns used of smartphones have been determined as clusters via k-means algorithm. For each user have been created a profile. Multiple Machine Learning (ML) algorithms have been applied to classify the users of these smartphones into genuine user or intruder. The framework performance has been evaluated across different group of 57 users. The results of this evaluation show different averages of the equal error rates depending on the used algorithm, in which the "Logistic Regression, Neural Networks, KNN, SVM, and Random Forest algorithms have gotten 13.7%, 13.5%, 12.1%, 10.7%, and 5.6% respectively".

8) Ehatisham-ul-Haq et al, in 2018 (20) the researcher proposed a novel continuous authentication framework for smartphone users, that verifies the users based on their patterns of physical activities via magnetometer, accelerometer and gyroscope sensors which are implicit within smartphones. The researcher applied many experiments to verify the users and 10 recognize them using three machine-learning classifiers Decision Tree (DT), K-Nearest Neighbor (KNN) and Support Vector Machine (SVM), in addition to six various activities are tested to many locations around the body of the user during normal using. SVM classifier obtained the best result against the other classifiers for the user's verification with a medium accuracy of 97.95%.

DEEP LEARNING OF ARTIFICIAL NEURAL NETWORK

Deep learning is an advanced type of machine learning, where algorithms similar to the human brain called "artificial neural networks" could learning via massive quantities of data (21). In a similar way, as the human learns via its experiences, the deep learning of artificial neural network algorithm could do tasks frequently, gradually for enhancing the results. The term of "Deep learning" comes from the depth of neural networks with respect to the number of hidden layers that it contains. The hidden layers consist of pre-specified number of nodes, which contain weights and bias in addition to non-liner activation functions (NLAFs). The NLAFs such as: Sigmoid, Tanh, ReLU and Leaky ReLU (LReLU) would converts the learned linear mappings into non-linear forms, and send it as a new input feeds to the next node in the next hidden layer, forwarding to the output layer. While at the output layer, another activation functions such as Softmax used to perform predictions. The deep ANN algorithm requires an outsized of data for learning, that is why the increase of the data availability made the deep learning abilities are matured recently (22).

SMARTPHONE AUTHENTICATION

There are two prime kinds of smartphone authentication methods, static and continuous (23). The static type is authentication, which happens only one time at the beginning of sessions during the user, wants to deal with the phone. The continuous type is authentication, which happens automatically during the usage of the smartphone. A considerable characteristic of continuous authentication is that an unattended smartphone will need user verification procedure before permitting to get access. On the other hand, an unattended smartphone, which uses static authentication, may probably provide access to a unauthenticity user. Behavioral biometrics-based authentication is offered as a suitable approach for continuous authentication. Because such an approach could apply in continuous manner with no need specified interaction procedure, just its normal usage of the smartphone. In this paper, a behavioral touchscreen based continuous authentication system was proposed. It used behavioral touchscreen dataset that will explain in the next section.

BEHAVIORAL BIOMETRIC DATASET

An experiment (24) via developing mobile application applied for android smartphones to collect behavioral data though interacting 41 users on the touchscreen of smartphones. The users must read texts and comparing two images to collect this behavioral data during touching the screen. The major objective of this trial was to encourage users for producing much "navigational strokes" in an ordinary way. The experiment called “reading and image viewing behavior on smart phones". In this trial, the touch data (strokes) of users had archived via the sensor of the smartphone touchscreen. Each stroke obtains the following features; (phone ID, user ID, document ID, time [ms], action [an event code (e.g., finger up, finger down, finger move)], phone orientation, x-coordinate, y-coordinate, the finger pressure, the area covered of the finger, finger orientation). Each user had interacted with the smartphone across multiple sessions at different times and the strokes had recorded in an orderly way in a dataset. The features of these strokes had obtained via the standard API of the Android system.

THE PROPOSED SYSTEM

A touchscreen-based Smart Continuous Authentication System (SCAS) was proposed. Deep learning algorithm of Artificial Neural Network (ANN) have adopted to build this system. The proposed system (SCAS) takes the advantage of using deep learning techniques. It is capable to deal with the portions of the stroke (example after example), and introduces each portion of Stroke as input data to the first layer of neural network model for the learning phase. In opposed to the machine learning techniques that required creating features extraction phase, via implement statistical operations on the entire Stroke to produce one sample that represents a one-stroke that used as input data during the learning phase. Moreover, SCAS can be considered as more reality and its training deeper.

The SCAS consists of two main phases:

1- Building model phase.
2- Continuous authentication phase.

In the first phase, the system will train on real dataset collected from 41 users during interacting with touch-screen of mobile phone as described before in the previous section (V.). This dataset contains features extracted from the sensor of the touchscreen, which represents their behavioral biometric. The adopted model of deep neural network (DNN) in this research work consists of two hidden layers, Leaky ReLU (25) activation function at each hidden layer, Softmax activation function with categorical_crossentropy” loss function (26) at the output layer, and AdaMax optimizer (27).

During the process of training, the model requires checking its generalization by validating its performance on the unseen validation set; therefore, to avoid the over-fitting we had used Early Stopping technique (28) and Dropout technique (29). Finally examines its accuracy on the test set, which represents the future new data. This new data need to be classify in an accurate manner. Figure (1) shows the general block diagram of this phase.

Moreover, the model can be deploy in the continuous authentication phase. In the second phase, the SCAS system starts to validate the user identity through his behavioral data that had aggregated during interacting with the touch-screen of the smartphone, about if it is the genuine or impostor user in a continuous manner. To achieve that, a method have developed to predict each sample of stroke and compares with the threshold of the genuine user. If the prediction value greater than the threshold, it will consider as genuine user, else consider as impostor. The process will repeat until the end of the current stroke, then calculating the ratio of accepted examples and comparing with pre-specified ratio called examples acceptance rate (SAR). If it less or equal to this ratio, the stroke will be rejected, otherwise be accepted, as shown in figure (2).

Moreover, it could specified number of the sequences strokes as a threshold called strokes acceptance rate (KAR). KAR will use to determine the user authenticity after some number of consequences strokes and given the decision to resume the session or lucks the touchscreen. If the rejected consequence strokes less than or equal to the threshold (KAR), then the system will luck the touchscreen and will request the user to enter a password or any traditional authentication method that he already used in his smartphone to begin a new session. Figure (2) shows the general block diagram of this phase.

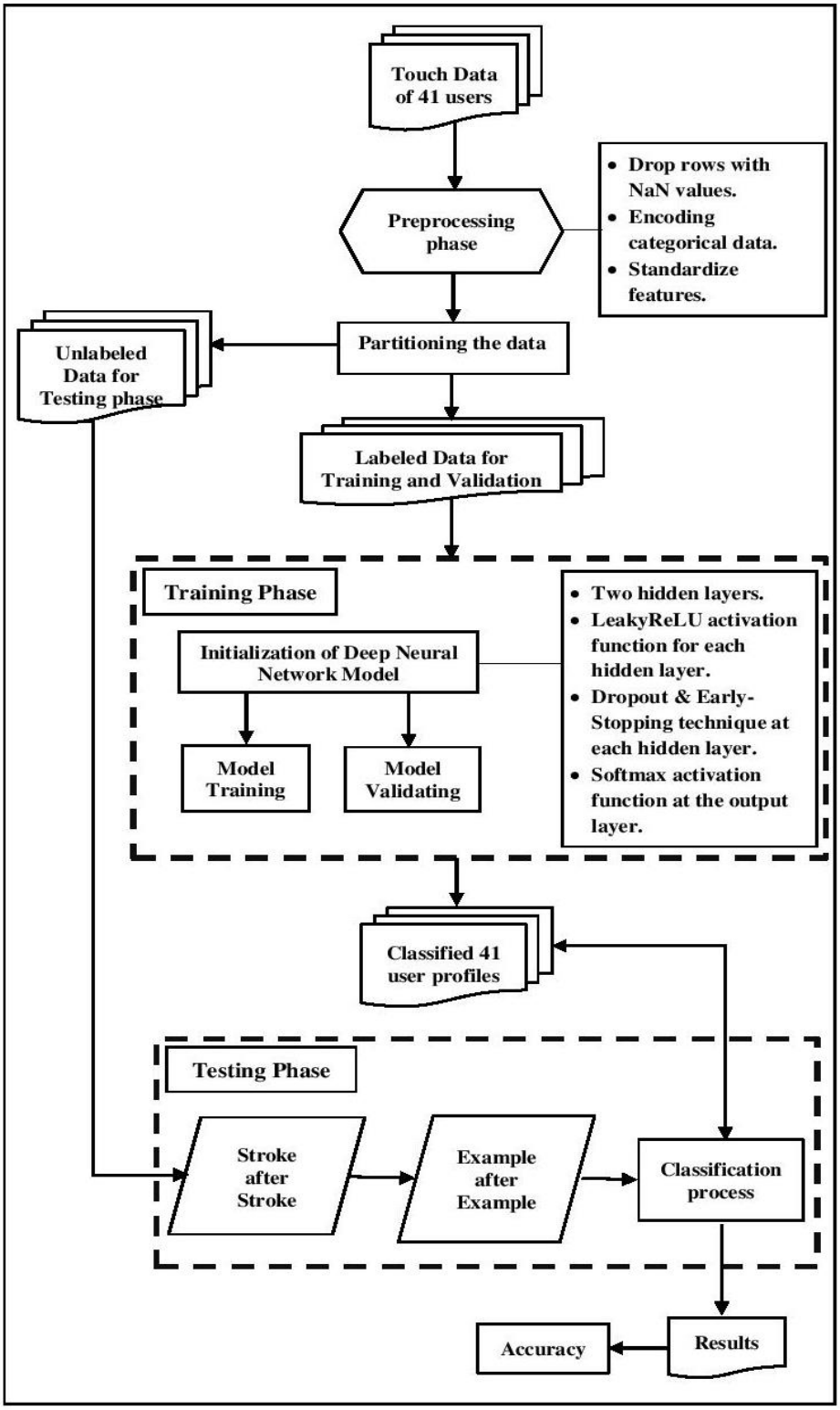

Figure (1) the general block diagram of the building model phase.

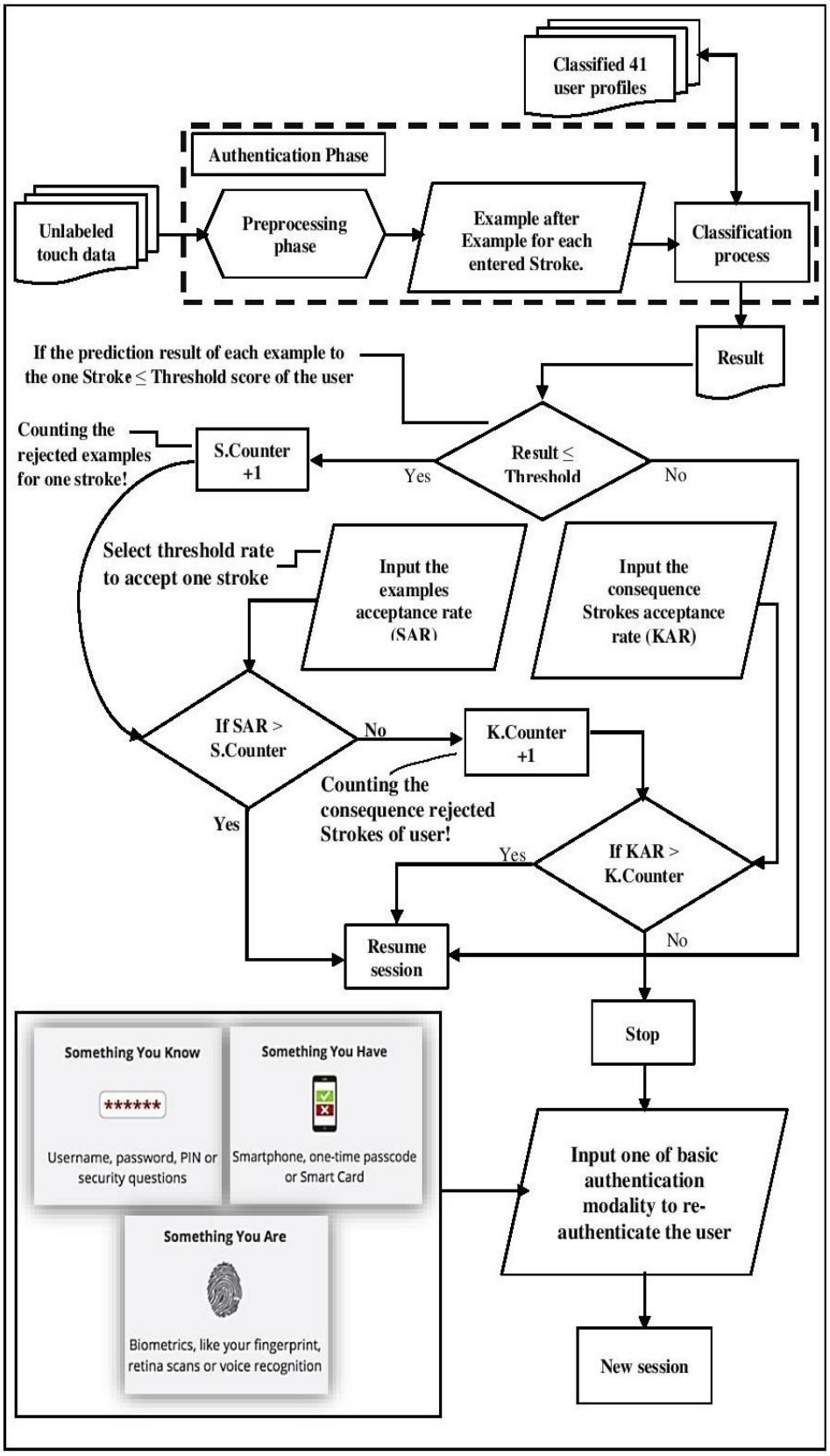

Figure (2) the general block diagram of the continuous authentication phase.

EXPERIMENTAL RESULTS

In this section, we demonstrate the experimental outcomes of adopting a continuous authentication system

(SCAS) by using Deep ANN algorithm that trained on the dataset, which mentioned in section (V). As the SCAS consists of two phases:

Results of Building Model phase:

The novelty of this paper is how the deep neural network algorithm implemented directly on this dataset without extracting new features from it except the preprocessing phase of the dataset, as shown in figure (1). This implementation had done via partitioning the dataset based on the users' strokes into three parts (training, validating, and testing) in a continuous manner among the dataset as shown in table (1). By implementing For-loop on the dataset with Ifs conditions, the first part takes six consequences strokes for training, which had obtained at the end of "For-loop" 638042 examples. The second part is one stroke for validation with 91254 examples, and the third part is two consequences strokes for testing with 182836 examples. This method of partitioning the dataset had provided enough diversity of strokes for the model-building phase across different sessions and situations that had led to building a reliable model.

Table (1) showing how the dataset is splitting into three parts continuously among all the dataset.

User1	S0	S1	S2	S3	S4	S5	S6	S7	S8	S9	S0	S1	S (n)…
User2													
User3													
.													
.													
.													
User 41													

70%	10%	20%
6 strokes for Training	1 stroke for Validation	2 stroke for Testing

In this paper, preprocessing techniques were used from sklearn library in python. Encoding the categorical data by labelbinaize function and scaling the data by Standard scaler function, which they used to avoid the bias in the neural networks during the learning phase toward the big values in the dataset. After that the DNN model was initialized with two hidden layers, each one had 400 node. For each node, a LeakyReLU activation function (AF) was used from Keras library to overcome the linear mappings of neural networks. To initialization weights, a "glorot_uniform" was used because of the experience of studies refer to have good results of this initializer with LeakyReLU AF. At the output layer, "Softmax" AF was used to normalize the outcome of last hidden layer and mapping the results to the multiclass-label of 41 users, in addition to used "categorical_crossentropy" loss function and "AdaMax" optimizer. To avoid the over-fitting problem during the learning phase, two generalization techniques were used. The first one is Early stopping callback had used to stop training when a monitored loss metric has stopped improving (ie.no longer decreasing) as shown in figure (3). The second one is the dropout technique; the best experimental ratio for dropout in this work that it associates together with all previous parameters and hyper-parameters in building our adopted model is "0.4". Finally, excellent results were achieved comparable with the related works, where the accuracy of training up to more than 95%, validating accuracy up to 96% as shown in figure (4), and the average accuracy of testing part up to 94%.

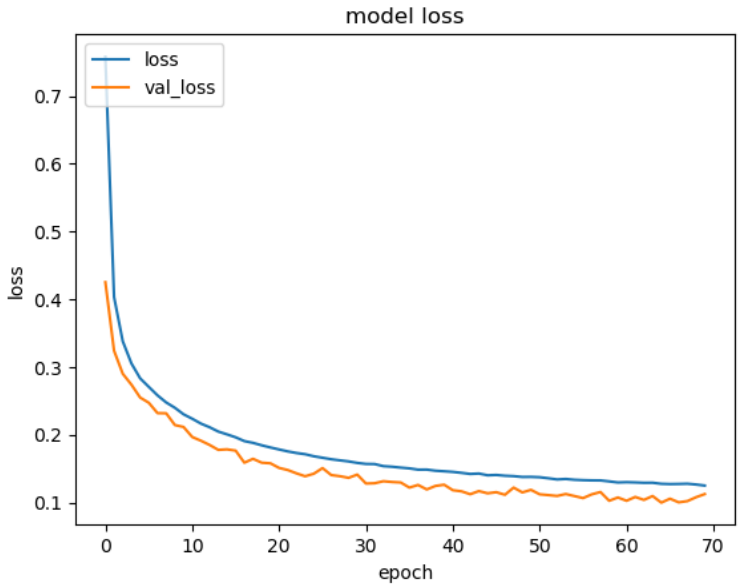

Figure (3): The Loss in Model

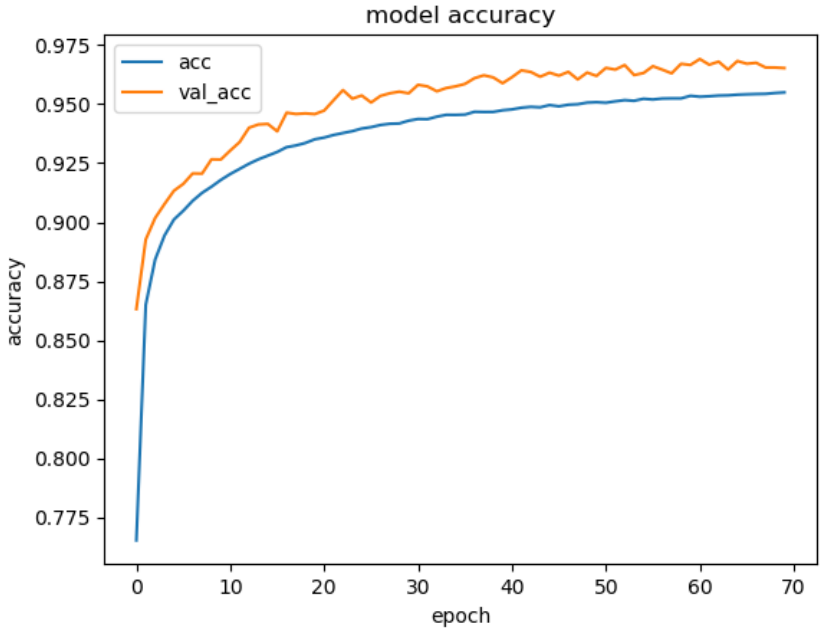

Figure (4): The Model Accuracy

Results of Continuous Authentication phase:

The effectiveness of choosing regulation ratio; examples acceptance rate (SAR), will play a control role in the degree of the model robustness. That means the model will be sensitive to reject the strokes that have one or more examples prediction score that be less than the threshold score of the genuine user. The SAR represents how many examples prediction scores that should fall up of the threshold dividing on the number of examples in that stroke, or in the degree of usability in which the system will be more flexible to accept strokes more. Figure (5) showing the continuous authentication with acceptance ratio rule 1:1, that means if there is one or more example of the stroke have prediction score falls below the threshold score, then the stroke will be rejected. Therefore, we could modify this ratio and making trade-off between the robustness and the usability.

Evaluation the Performance of the Proposed System

One of the well-known approaches to evaluate the performance and the validity of the behavioral biometric security systems is the 'equal error rate (EER)'', that represents the ratio which comes from the false acceptance rate (FAR) and the false rejection rate (FRR) that should be as equal as possible. The reliable systems should keep this value as small as possible.

This approach applied by start with calculating the threshold of each user in the testing part of dataset using the following equation:

$$\text{Threshold} = (\text{mean of impostor score} + \text{mean of genuine score}) / 2 \quad (1)$$

Because in this research work, a generalization of the adopted model was tried and simulating the real-world uses of smartphones. For that, the advantage of the multi-classification problem was taken in the dataset to perform one-versus-all classification. In which, the imposter score and genuine score were calculated depending on the prediction of each example to the strokes; If the current prediction result of the example does not refer to the genuine class label, here will take the current prediction value and add it to the impostor score array. Then adding the prediction value of the genuine class label to the genuine score array. Else, if the current prediction result refers to the genuine class label, here will take the current prediction value and add it to the genuine score array, then subtracting 1 from the current prediction value and adding the result to the impostor score array.
Moreover, it have been calculated the false acceptance rate (FAR) of impostors whom acceding the threshold score of that user, and the false rejected rate (FRR) whom the genuine score falls below of the threshold score of that user. Finally, calculating the equal error rate could obtains from this equation:

$$EER = (FAR+FRR)/2 \quad (2)$$

The adopted model (SCAS) had achieved excellent results comparable with the related works, and obtained around 3.4% EER.

CONCLUSION

After implement of the proposed system via deep learning method, the following conclusions have been adopted based on the practical results:

1. During the increasing ubiquity of sensors in the recent smartphones with their services that provide, the behavioral data of user biometrics can be access easily which are considered the source data to establish continuous authentication systems.
2. The research studies showed that the low values of FAR and FRR with less than 2% to the authentication systems could maintain an authentication period with fewer needs for user intervention to do basic authentication.
3. The methodology of this research has implemented on the behavioral biometrics collected from the sensor of the touchscreen while 41 users touch it during the normal using of their smartphones under application designed especially for this purpose. However, this biometric data classified as one modality data and has investigated to usage under continuous authentication manner and achieved competition results with models has built on multi-modality behavioral data.
4. The results show that applying the deep neural networks on one behavioral biometric modality provides comparable accuracy with other research works that have used machine-learning algorithms with multi-modality. From that, it gains less computational cost with less time to authenticate users, because it has been exceeded the features extraction step from the data that fetched from the smartphone sensors.
5. Using the deep ANN model has been obtained accepted and accurate outputs to the current research. This model achieved 94.2% average 65 testing accuracy on 20% real biometric data, with EER of 3.46% across all sessions.

REFERENCES:

1. Buriro, B. Crispo, F. Delfrari, and K. Wrona, Hold and sign: A novel behavioral biometrics for smartphone user authentication, in Security and Privacy Workshops (SPW), 2016 IEEE, pp. 276–285, IEEE, 2016.
2. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides, “Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption,” Proc. USEC, 2015.
3. V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello.Continuous user authentication on mobile devices: Recent progress and remaining challenges. IEEE Signal Processing Magazine, 33(4):49–61, July 2016.
4. Boakes, Matthew, et al. "Exploring Mobile Biometric Performance through Identification of Core Factors and Relationships." IEEE Transactions on Biometrics, Behavior, and Identity Science (2019).
    A. Jain, A. A. Ross, and K. Nandakumar, Introduction to biometrics. Springer Science & Business Media, 2011.
5. J. Angulo and E. Wästlund, “Exploring touch-screen biometrics for user identification on smart phones,” Priv. Identity Manag. Life, 2012.
6. A.Alzubaidi and J. Kalita, "Authentication of Smartphone Users Using Behavioral Biometrics," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1998-2026, thirdquarter 2016.

7. Ferreira, João, Henrique Santos, and Bernardo Patrão. "Intrusion detection through keystroke dynamics." 10th European Conference on Information Warfare and Security. 2011.
8. Ayeswarya, S., and Jasmine Norman. "A survey on different continuous authentication systems." International Journal of Biometrics 11.1 (2019): 67-99.
9. Abuhamad, Mohammed, et al. "Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Survey." arXiv preprint arXiv:2001.08578 (2020).
10. Montgomery, Melodee S. Touch-based Continuous Authentication Using Deep Neural Net and Genetic Algorithm. Diss. North Carolina Agricultural and Technical State University, 2019.
11. Liang, Yunji, et al. "Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective." IEEE Internet of Things Journal 7.9 (2020): 9128-9143.
12. M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, Touchalytics: on the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication, IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, pp. 136-148, 2012.
13. Heather Crawford, a framework for continuous, transparent mobile device authentication, computers & security 39, 2013, 127-136.
14. Bo, Cheng, Lan Zhang, and Xiang-Yang Li, SilentSense: Silent User Identification via Dynamics of Touch and Movement Behavioral Biometrics, arXiv preprint arXiv: 1309.0073, 2013.
15. Nan Zheng, Kun Bai, Hai Huang and Haining Wang, You are How You Touch: User Verification on Smartphones via Tapping Behaviors, IEEE 22nd International Conference on Network Protocols, 2014.
16. Hui Xu, Yangfan Zhou and Michael R. Lyu, Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones, Symposium on Usable Privacy and Security (SOUPS), 2014, July 9–11, 2014, Menlo Park, CA.
17. Stefania Budulan et al, Continuous User Authentication using Machine Learning on Touch Dynamics, Conference Paper • November 2015.
18. Rajesh Kumar, P. P. Kundu, D. Shukla and V. V. Phoha, "Continuous user authentication via unlabeled phone movement patterns," 2017 IEEE International Joint Conference on Biometrics (IJCB), Denver, CO, 2017, pp. 177-184.
19. Hole, Y., Hole, S. P.-, & Bhaskar, M. P. (2019). The damages of liberal marketing myopia. Restaurant Business, 118(10), 542-556.
20. Ehatisham-ul-Haq, Muhammad, et al. "Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing." Journal of Network and Computer Applications 109 (2018): 24-35.
21. Volaka, Hasan Can, et al. "Towards continuous authentication on mobile phones using deep learning models." Procedia Computer Science 155 (2019): 177-184.
22. Büch, Holger. Continuous Authentication using Inertial-Sensors of Smartphones and Deep Learning. Diss. Robert Bosch GmbH, 2019.
23. Guilherme Miguel, Gonalves Neves, Android Gait Recognition System, 2013.
24. Frank, Mario, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication". IEEE Transactions on Information Forensics and Security, 8(1):136–148, 2013.
25. Nwankpa, Chigozie, et al. "Activation functions: Comparison of trends in practice and research for deep learning." arXiv preprint arXiv:1811.03378 (2018).
26. Zaid Khalaf Hussein, Ban N. Dhannoon. Deep Neural Network with Dropout for Anomaly Detection in Software Defined Networking. nternational Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-11, September 2019.
27. Zeng, Xiangyu, Zhiyong Zhang, and Dong Wang. "AdaMax Online Training for Speech Recognition." 2016.
28. Prechelt, Lutz. "Early stopping-but when?." Neural Networks: Tricks of the trade. Springer, Berlin, Heidelberg, 1998. 55-69.
29. Labach, Alex, Hojjat Salehinejad, and Shahrokh Valaee. "Survey of dropout methods for deep neural networks." arXiv preprint arXiv:1904.13310 (2019).