ISSN 2278-3091
Volume 8, No.1.3, 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse3781.32019.pdf
https://doi.org/10.30534/ijatcse/2019/3781.32019

An Initial Framework of Fuzzy Neural Network Approach for Online Learner Verification Process

Siti Fairuz Nurr Sadikan [1], Azizul Azhar Ramli[1], Shahreen Kasim[1], Hairulnizam Mahdin[1], Mohamad Aizi Salamat[1], Untari Novia Wisesty[2]
[1]1Faculty of Computer and Information Technology, Universiti Tun Hussein Onn Malaysia, 86400 Batu Pahat, Johor Darul Takzim, Malaysia, fairuz.sadikan@gmail.com
[2] School of Computing, Telkom University, 40257 Bandung, West Java, Indonesia

ABSTRACT

Online learning is become more popular among university due to its flexibility and adaptability. The student authentication as online learner is widely seen as a major concern for online assessment. In most cases, there is absent of face-to-face supervision during online assessment, this situation leads the student to use or find help from others in order to get high scores in their result. This paper address the issue related to online assessment. The main objective of this work was to propose the use of online learner verification framework. This proposed solution utilizes the keystroke analysis and activity-based authentication for the online learner authentication. A fuzzy neural network is used to train and validate the online learner's identity. The proposed framework can be implementing in any online learning environment for verifying online learner identity.

Key words : activity based authentication, biometric authentication, fuzzy neural network, keystroke analysis, profile based authentication,.

1. INTRODUCTION

The internet growth has largely evolved in teaching and learning process. The online learning environments are widely implemented by a number of educational institutions in various disciplines due the factor of accessibility and availability.

The teaching and learning component are integrated in online learning environment including the online assessment. Practically, it is often easier to cheat online since the assessments such as online quiz and test are less monitored, and assessment can often be done at any time of day. Then, security is being vital to the credibility of online learning environments. The use of student authentication such as username and password is to ensure the genuine interaction of individual students in the online assessment.

However, this conventional method is not sufficient to verify the identity of an online student [22]. Then, a new mechanism should be applied to this online learning in order to improve the security level along the login session. But the issue of current login method is that only authenticate user at initial login and do not re-authenticate user until the user log out from the system 1.

Thus, this paper proposes the use of verified online learner identity framework by using fuzzy neural network for the online learner authentication during online assessment.

2. AUTHENTICATION

An Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be2. There are four types of authentication methods in online exam namely: (1) Knowledge Based Authentication, (2) Object Based Authentication, (3) Biometric Based Authentication7 and (4) Profile Based Authentication[15], as shown in Figure 1.

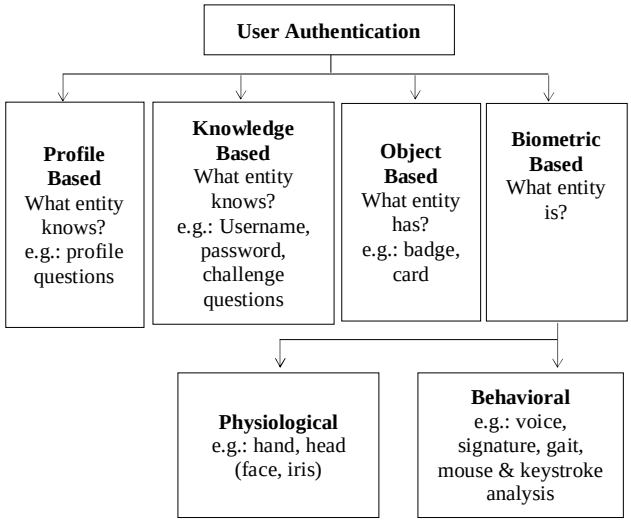

Figure 1: Authentication Models

2.1 Knowledge Based Authentication

Knowledge Based Authentication (KBA) is a current predominant authentication method for online services

because it is memorable and does not require any extra device [7]. Username, password, and challenge questions are examples of this method that require personal knowledge to authenticate individual access to online environment. Password may include a words, phrases, and personal identification numbers (PINs) that are closely kept secrets used for authentication during the login session. But there are much vulnerability of password such as it can be guessed or searched by an attacker. Besides, the long and random, or changing password is difficult to remember for an individual. Thus, it does not provide good compromise detection, and defence against repudiation [1].

2.2 Object Based Authentication

A person possessing character articles is accepted to be true to the framework. The clients are recognized by exhibiting or applying physical items, for example, electronic chip cards, attractive cards, and computerized keys [23]. It stores or produces different passwords and gives bargain identification since its nonappearance is discernible. It additionally gives included security against forswearing of administration assaults [1]. In any case, there are two primary weaknesses of a token[10] which are bother and cost where it additionally can be lost or stolen token10. Additionally, it might require particular reason gadgets to take client contribution for enlistment and validation [23].

2.3 Biometric Based Authentication

Biometric based authentication is the identification of a user that depends on physiological and behavioral characteristic such as what the user is [11]. The examples of physiological characteristic are fingerprint recognition, facial recognition, and iris recognition. On the other hand, voice, signature, lip movement, mouse dynamic, and keystroke dynamic which include any learned movement are examples of behavioural biometric. This authentication is the most secure and convenient authentication tool because it cannot be borrowed; stolen, forgotten and forging one is practically not easy [14].

2.4 Profile Based Authentication

In a profile-based validation framework, a client profile is put away at the verifier and later used to check their confirmation guarantee by producing challenge questions haphazardly. A profile essentially incorporates client explicit data that is protection delicate. This data can relate to individual data, training, exercises, proficient experience, leisure activities, future goals, and learning exercises [22]. It has been utilized notwithstanding username and secret phrase system, which used to bolster understudy confirmation. For the most part, it depends on multi-modular validation which comprises of two layers of verification, for example, username and secret phrase, and challenge questions. At first, a username and secret phrase can be utilized to login into the internet learning condition to do customary learning exercises during the main layer. While during the learning procedure, understudies are suggested with profile conversation starters that are utilized to expand and refine singular understudy's profile. The second layer of confirmation will trigger the test questions, which are produced from the understudy's profile. The profile questions are utilized to gather answers to assemble and refresh the understudy's profile. These test questions are utilized to confirm the understudy's character.

In 2012, author [22], published a paper in which propose the use of profile based authentication framework (PBAF) with the implementation of a user-id and password for the authentication of students during online examinations. Besides, in 2013, author [6], implement the users profile for continuous behaviometric authentication system. Then, in 2014, author [17], implement the hybrid user behavior profiles to serve as a second re-authentication factor together with the username and password. In other hand, author [5] explores the feasibility of automatically extracting passwords from a user's daily activity logs, such as Facebook activity and phone activity. While author [13] also proposed a modified authentication method based on user profiles. Based on the previous study, it shows that the use of user profile can improve the security level of online system. It is because even though users might share their passwords once, or tend to pass their tokens like username and password with their colleagues in certain circumstances, they are generally unwilling to continuously share their daily activities with others.

3. KEYSTROKE AUTHENTICATION

Keystroke analysis has been highlighted as an alternative to securing password [20]. It is divided into two types which are static and dynamic. The static is used to monitor typing behavior of user at specific time which are fixed text mode only. In contrast, the dynamic is use to monitor typing behavior of user throughout the interaction process which are free text mode. The keystroke dynamic monitoring is then divided into another two types of monitoring which are periodic or continuous. The differences between these are the time of monitoring during logged in session, where continuous will extend to data capturing to the entire duration of logged in session as illustrated in Figure 2.

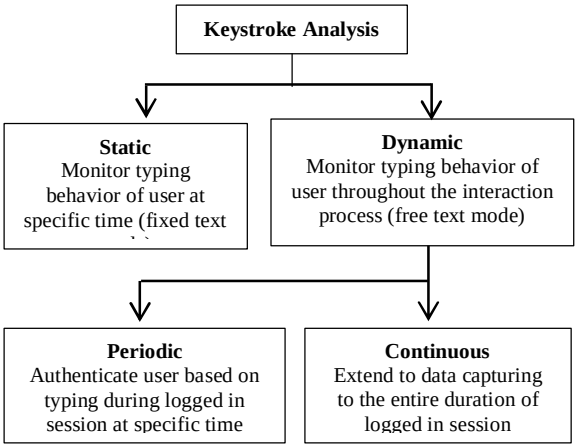

Figure 2: Types of Keystroke Analysis

This keystroke analysis can be constructed from various typing features such as pressure applied on the keys, the

duration between successive key pressed, typing speed, and finger position on the keys. Besides, keystroke dynamics proved most appropriate for continuous behaviometric authentication [6].

4. KEYSTROKE ANALYSIS METHOD

There is various analysis method of keystroke dynamic which can be broadly categorized into statistical approach and machine learning approach [24]. A statistical approach was found to be the first technique used to analyzed keystroke dynamic [8]. This approach is common and popular due to simplicity and ease of implementation. The inclusive statistical measures encompass k-nearest neighbor, standard deviation, statistical t-test, mean and median [4].

However, previous studies have primarily concentrated this approach was mostly applied for static keystroke analysis or fixed text analysis. In other hand, machine learning approach is used to classify and identify a pattern and make the correct conclusion based on the provided data. The sub domain includes neural networks, evolutionary computing, decision tree and fuzzy logic. Among these sub domains, neural networks are widely studied to be capable of learning nonlinear models of data.

Recently, various artificial neural networks (ANNs) have been applied to the keystroke classification problem, including multilayer perceptron4, back propagation neural network [25], and Art-2 neural network [8]. In 2017, author [24], uses K-Nearest Neighbor as the clustering algorithm, which is a non-parametric algorithm for classification for demo banking application.

As indicated by the creator [24], ANNs can perceive complex uproarious examples however it has their own confinements that limit them as a substitute for conventional techniques, for example, factual relapse, design acknowledgment, and time arrangement examination. Besides, neural systems have been upgraded by joining it with different strategies, for example, fluffy rationale, wavelet-based neural system and bolster vector machines. Based on previous research, several studies have revealed that better results can be produced with the help of neural networks. However it requires the user keystroke pattern to train the network and it is almost impractical to obtain user keystroke pattern at the early enrollment stage [4]. By consolidating neural system and fluffy rationale, execution of framework is improved where it permit the utilization of neural system topology together with fluffy rationale.

In recent years, there has been an increasing interest in fuzzy neural network approach where author [3] used neuro-fuzzy approach for credit card fraud detection; author [19] used hybrid fuzzy C-Means clustering algorithm and Multi-Layer feed forward neural network with back-propagation learning algorithm to analyzed browsing patterns of users to extract information in web server; author [12] used hybrid approach based on neural networks and fuzzy logic for intrusion detection system modeling using Self-Organizing Map; author [16] used Neuro-Fuzzy Interface System for neuro fuzzy based attack detection; author [18] also used Adaptive Neuro-Fuzzy Inference System which is a hybrid approach based on neural networks and fuzzy logic for fraud detection in e-Commerce transactions; author [9] used Adaptive Neuro-Fuzzy Inference System for domestic water usage prediction; and author [26] used Adaptive neuro-fuzzy inference system for continuous implicit authentication for mobile devices. Previous research has shown that the fuzzy neural network can be used for continuous authentication. Therefore, fuzzy neural network approach is used in verifying online learner identity.

5. PROPOSED FRAMEWORK

In the proposed framework of online learner verification, generally it comprises of two layers of authentication such as username and password, and challenge question which are presented in Figure 3.

It very well may be developed from different composing highlights, for example, composing speed, the span between progressive key squeezed, weight connected on the keys, and finger position on the keys. Furthermore, keystroke elements demonstrated most suitable for persistent behavior metric verification [6].

A. Phase 1: Initial Authentication And Verification

The first phase is used for initial verification and screening where the student details such as username and password are been checked and user authenticity is then verified.

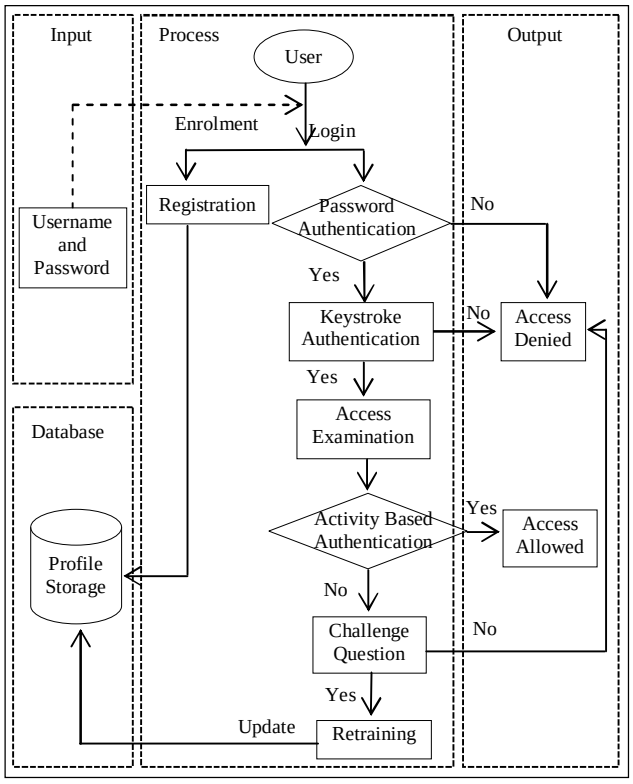

Figure 3: Online Learner Verification Framework

1) Step 1: Enrolment

This step is for the first time login where the users are needed to re-enter their username and password for a few times to register their profile into the database system. This step will use the static keystroke analysis and it is very important to gain the user typing pattern. Then the user typing pattern will be stored in student profile database also called profile storage.

2) Step 2: Login

This step used to access how the information was entered during enrolment process. If the user authenticated, it will redirect to access examination where access examination begin to monitor the user.

B. Phase 2: Behavioural Analysis Phase

In online learning activities, it carries out similar types of activity. It can be viewed as a part of cluster by using Fuzzy C-means for clustering algorithm. So, in this phase an access examination was used to identify the pattern of user history or their pass activity based on activity based authentication. For an example the types of assessment such as download and view notes, read an announcement, read and participate in forum discussion, submitting assignment and etc. All of the assignment can be divided into two types which activity on newly semester, and end of the semester. Besides the registered subject also can differentiate the type of activity such as mathematical subject may require other assessment compared programming subject.

C. Phase 3: Learning Phase

If the pattern of user history or their pass activity failed, then the user will be declared as suspicious interaction by the logged user and this user will move on the suspicious table which implements feed forward neural network analysis with back propagation. The user will be prompted with the challenge question. The question will be based on the user history or their pass activity such as: 1) When is your last logged session? 2) What is the score in your previous quiz? 3) How many file have been downloaded on your last session? and 4) What is your last activity?

The user needs to pass the challenge question. If the user passed, then the systems will retraining using feed forward neural network to get new pattern of user's activity. Otherwise will be considered access denied.

Table 1 provides the summary of Online Learner Verification Framework which consisting of three phases 1, 2 and 3. The step 1 and 2 which are enrolment and login are occurs at phase 1. In other hand, step 3 and 4 which are behavioural analysis and activity based authentication take an action in phase 2. In the last step which is step 5 is used to update the learner profile for the online learning.

Table 1: Summary of Framework

Phase	Steps	Explaination	Output
Phase 1	Step 1	Enrollment: *Registration*	Create User Profile
	Step 2	Login: *Password authentication*	Access Denied /Allowed
Phase 2	Step 3	Behavioural Analysis: *Keystroke authentication*	Monitoring Result
	Step 4	Activity Based: *Challenge Question*	Access Denied /Allowed
Phase 3	Step 5	Learning *Retraining*	Update Profile

6. CONCLUSION

This paper shows that the combination of keystroke authentication with activity based authentication can enhance the level of security in current online assessment. The new concept of fuzzy neural network approach also has been introduced in this study by implementing Fuzzy C-means and feed forward neural network analysis with back propagation for clustering and training purpose in order to get pattern of learner's activity. The combination of analysis techniques placed in the framework has the potential to provide a significant improvement in online learning environment for better security.

Lastly, future work will focus on the development based on the framework for further examine the level of performance that can be achieved. To accompany this work, a prototype will also be developed to enable an end-user evaluation so that the user acceptance an operational performance can be established.

ACKNOWLEDGEMENT

The authors would like to thank the Centre for Graduate Studies Universiti Tun Hussein Onn Malaysia for partly sponsored this research**.**

REFERENCES

1. Agashe, N. M., & Sonali Nimbhorkar. (2015). **A Survey Paper on Continuous Authentication by Multimodal Bio-metric. International Journal of Advanced Research in Com-puter Engineering & Technology (IJARCET),** 4(11), 4247–4253.
2. Bailie, J., & Jortberg, M. (2009). **Online Learner Authentication: Verifying The Identity of Online Users**. Journal of Online Learning and Teaching, 5(2), 25.
3. Behera, T. K., & Panigrahi, S. (2015). **Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering & Neural Network**. In 2015 Second International Conference on Advances in Computing and Communication Engineering (pp. 494–499). https://doi.org/10.1109/ICACCE.2015.33
4. Borgaonkar, A., Salunke, A., Gupta, N., & Sharma, V. (2017). **User Authentication Through Keystroke Dynamics Using KNN**. Journal of Multidisciplinary

Engineering Sci-ence and Technology (JMEST), 5(4), 367–397.

5. Dandapat, S. K., Pradhan, S., Mitra, B., Choudhury, R. R., & Ganguly, N. (2015). ActivPass: **Your Daily Activity is Your Password. Proceedings of the ACM CHI'15** Conference on Human Factors in Computing Systems, 1, 2325–2334. https://doi.org/10.1145/2702123.2702457
6. Deutschmann, I., Nordstrom, P., & Nilsson, L. (2013). **Con-tinuous Authentication Using Behavioral Biometrics**. IT Professional, 15(4), 12–15. https://doi.org/10.1109/MITP.2013.50
7. Han, G., Yu, Y., Li, X., Chen, K., & Li, H. (2017). **Charac-terizing The Semantics of Passwords: The role of Pinyin for Chinese Netizens**. Computer Standards & Interfaces, 54, 20–28. https://doi.org/10.1016/j.csi.2016.10.006
8. Harun, N., Dlay, S. S., & Woo, W. L. (2010). **Performance of Keystroke Biometrics Authentication System Using Multi-layer Perceptron Neural Network (MLP NN)**. In 7th International Symposium on Communication Systems, Networks & Digital Signal Processing (pp. 711–714). https://doi.org/10.1109/ICCCE.2010.5556852
9. J, J., & Sankaran, S. (2017). **A Neuro-Fuzzy Approach for Domestic Water Usage Prediction**. In 2017 IEEE Region 10 Symposium (TENSYMP).
10. Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: **A Tool For Information Security**. IEEE Transactions on Information Forensics and Security, 1(2), 125–143. https://doi.org/10.1109/TIFS.2006.873653
11. Karim, N. A., & Shukur, Z. (2015). **Review of User Authentication Methods in Online Examination**. Asian Journal of In-formation Technology, 14(5), 166–175.
12. [12] Midzic, A., Avdagic, Z., & Omanovic, S. (2016). Intrusion Detection System Modeling Based on Neural Networks and Fuzzy Logic. IEEE 20th Jubilee International Conference on Intelligent Engineering Systems (INES) (pp. 189–194). https://doi.org/10.1109/INES.2016.7555118
13. Naidu, R. C. A., Meghana, K., Avadhani, P. S., & Rao, I. U. M. (2016). **New Approach of Authentication Method Based on Profiles.** International Conference On Recent Advances in Information Technology, 347–352. https://doi.org/10.1109/RAIT.2016.7507929
14. Patil, R. A., & Renke, A. L. (2016**). Keystroke Dynamics for User Authentication and Identification by using Typing Rhythm.** International Journal of Computer Applications, 144(9), 27–33. https://doi.org/10.5120/ijca2016910432
15. Ramu, T., & Arivoli, T. (2013). **A Framework of Secure Biometric Based Online Exam Authentication: An Alternative To Traditional Exam**. International Journal of Scientific and Engineering Research, 4(11), 52–60.
16. Saoreen Rahman, Mamun, S. Al, Ahmed, M. U., & Kaiser, M. S. (2016). **PRY / MAC Layer Attack Detection System Using Neuro-Fuzzy Algorithm for loT Network. In International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)** (pp. 2531–2536). IEEE. https://doi.org/10.1109/ICEEOT.2016.7755150
17. Selcuk Uluagac, A., Liu, W., & Beyah, R. (2014**). A Multi-Factor Re-authentication Framework with User Privacy.** 2014 IEEE Conference on Communications and Network Security, CNS 2014, 504–505. https://doi.org/10.1109/CNS.2014.6997526
18. Shaji, J., & Panchal, D. (2017). **Improved Fraud Detection in e-Commerce Transactions.** In 2017 2nd International Confer-ence on Communication Systems, Computing and IT Applications (CSCITA) (pp. 121–126). IEEE. https://doi.org/10.1109/CSCITA.2017.8066537
19. Shivaprasad, G., Reddy, N. V. S., Acharya, U. D., & Aithal, P. K. (2015). **Neuro-Fuzzy Based Hybrid Model for Web Usage Mining. In Eleventh International Multi-Conference on Information Processing-2015** (IMCIP-2015) Neuro-Fuzzy (Vol. 54, pp. 327–334). Elsevier B.V. https://doi.org/10.1016/j.procs.2015.06.038
20. Singh, B., Sonawane, S., Shah, Y., & Singh, V. (2017). **Literature Survey on Keystroke Dynamics for User Authentication. International Journal on Recent and Innovation Trends in Computing and Communication,** 5(5), 280–282.
21. Trivedi, J. A. (2014). **Voice Identification System Using Neuro-Fuzzy Approach**. International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014), 2(3), 300–301.
22. Ullah, A., Xiao, H., & Lilley, M. (2012). **Profile Based Stu-dent Authentication in Online Examination**. International Conference on Information Society (I-Society), 109–113.
23. Ullah, A., Xiao, H., Lilley, M., & Barker, T. (2012). **Using Challenge Questions for Student Authentication in Online Examination**. International Journal of Infomomics, 5(3), 631–639. https://doi.org/10.20533/iji.1742.4712.2012.0072
24. Vinayakvitthal, L., & Charniya, N. N. (2015). **Review of Advances in Neural Network Based Biometric Authentication**. In International Conference on Communications and Signal Processing (ICCSP) (pp. 735–740). IEEE ICCSP 2015. https://doi.org/10.1109/ICCSP.2015.7322587
25. Wankhede, S. B., & Verma, S. (2014). **Keystroke Dynamics Authentication System Using Neural Network**. International Journal of Innovative Research and Development, 3(1), 157–164.
26. Yao, F., Yerima, S. Y., Kang, B., & Sezer, S. (2017). **Continuous Implicit Authentication for Mobile Devices based on Adaptive Neuro-Fuzzy Inference System**. In International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2017). https://doi.org/10.1109/CyberSecPODS.2017.8074846