RESEARCH ARTICLE | NOVEMBER 11 2019

A survey paper on keystroke dynamics authentication for current applications FREE

Siti Fairuz Nurr Sadikan ✉; Azizul Azhar Ramli; Mohd Farhan Md. Fudzee

AIP Conf. Proc. 2173, 020010 (2019)
https://doi.org/10.1063/1.5133925

A Survey Paper on Keystroke Dynamics Authentication for Current Applications

Siti Fairuz Nurr Sadikan[a)], Azizul Azhar Ramli[b)] and Mohd Farhan Md. Fudzee[c)]

Faculty of Computer and Information Technology, Universiti Tun Hussein Onn Malaysia, 86400 Batu Pahat, Johor, Malaysia.

[a)] Corresponding author: fairuz.sadikan@gmail.com
[b)] azizulr@uthm.edu.my
[c)] farhan@uthm.edu.my

Abstract. Online learning is a common tool among university students that depends solely on the Internet medium. However, the lack of monitoring during examination sessions has resulted in the rising cases of online cheating among the students. As such, better mechanisms to replace the use of password authentication are needed to enhance the level of security for the online learning assessment. Keystroke dynamics is one of the most popular methods used, because it does not require any extra devices other than the keyboard. In addition, it can be used as a tool to secure online learning system, although the username and password are known to the user. This paper aimed to comprehensively investigate authentication systems, specifically the keystroke dynamic authentication system for current applications. Besides, the applications and the keystroke benchmarking dataset were also reviewed to have a better insight about their security and usability and to improve the level of security in the current online learning environment.

INTRODUCTION

Online learning is becoming more popular among university students due to its flexibility and adaptability, thus allowing learning to be done anytime and anywhere. Besides, it facilitates asynchronous communication, such as online tests and grading and enables monitoring of students to be done in forum and other assessment tasks. References [14] shows that, 93.17% graduate students in universities are generally positive about their experiences with online courses. The learners' environment in online learning, integrated with dependability and security, interrelates with trust, as dependability is subjective, thus reflecting the learners' level of trust towards the system [41]. Previously, a simple username and a password were implemented as one of the verification methods in online learning. Although innovative ways to authenticate users are increasingly growing in numbers of, password based authentication (PBA) remains steadily as one of the most preferred methods of all [42], the reasons being its ease of getting memorized at no cost and users' ability to use them in their daily life. However, passwords are easily accessible as users tend to pass their tokens to their colleagues in certain circumstances [28]. Based on the research conducted by [31], 54% of the students disagreed that cheating is difficult in online assessments, while only 33% agreed. Besides, a study about online cheating found that, 72.5% of students were reported to cheat when taking online quizzes and examinations [26]. This reflects the rampant bad habits associated with online cheating among the students. Hence, a new mechanism should be developed and applied to online learning to enhance the security level during the login session [36]. As time changes, various authentication methods have been introduced, some in biological, while others in graphical passwords [6]. Along with the use of passwords, these methods provide an even higher level of security for user logins [27]. Unfortunately, the issue of the current login method is that, the user is required to authenticate only at the initial login and no re- authentication is needed until the user logs out from the system [2]. Thus, this paper aimed to comprehensively investigate authentication systems, specifically keystroke dynamic authentication system, to gain a better understanding about their security and usability. The keystroke dynamic verifies the user by its typing pattern, because it is unique for each user. This method contains lots of advantages, compared to the other biometrics,

Advances in Electrical and Electronic Engineering: From Theory to Applications (Series 2)
AIP Conf. Proc. 2173, 020010-1–020010-11; https://doi.org/10.1063/1.5133925
Published by AIP Publishing. 978-0-7354-1920-9/$30.00

in terms of cost of implementation, higher distribution and better unobtrusiveness. It also can secure the system even if the username and password of another user are known to a particular user. Therefore, the level of security in current online learning environment can be improved.

This paper is divided into six (6) sections. Section 1 is about the introduction to the study, while section 2 contains related information on authentication. In section 3, the types of keystroke dynamics analysis are presented. The related keystroke analysis applications used by other researchers are described in section 4, before the classification is explained in Section 5. Meanwhile, benchmarked keystroke dataset is presented in section 6. Finally, section 7 provides the summary of the study.

AUTHENTICATION

Authentication is a process of verifying a user's legitimate right before secure resources can be released [50]. According to [36], there are four types of authentication methods, namely, Knowledge Based Authentication (KBA), Object Based Authentication (OBA), Biometric Based Authentication (BBA) and Profile Based Authentication, as shown in Fig. 1.

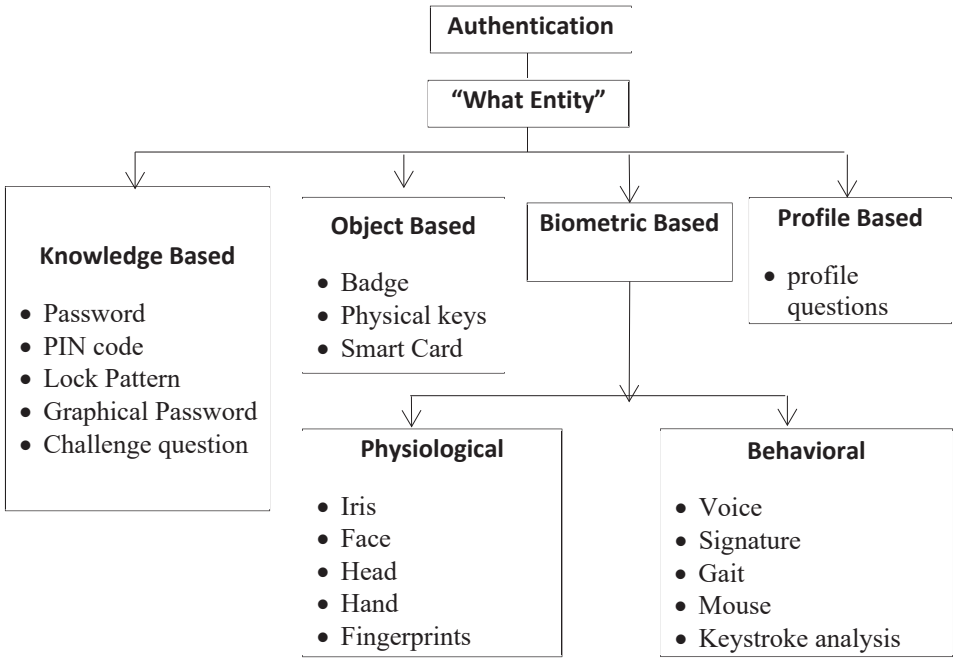

FIGURE 1. Types of authentication

Knowledge Based Authentication

Knowledge Based Authentication is the current predominant authentication method used for online services because it is memorable and it does not require any extra device [17]. The examples of this method are username, password, and challenge questions that require personal knowledge to authenticate individual access to online environment. It may include a single word, personal identification numbers (PINs) and phrases which are very closely kept secrets used for creating passwords. However, there is much vulnerability of password, for example, it is exposed to being searched or guessed by an attacker. Besides, the long and random, or changing password is difficult to remember. Thus, it does not provide a good compromise detection, and defense against repudiation [2].

Object Based Authentication

Generally, an individual in possession of identity objects is believed to be a genuine user to the system. Accordingly, users' identification is done by presenting or applying physical objects, such as magnetic cards, electronic chip cards and digital keys [52]. These objects store or generate multiple passwords and provide compromise detection since their absence is observable. They also provide added protection against denial of service attacks [2]. However, there are two main disadvantages of this authentication; it is inconvenient to carry along and it can be costly as it can be easily lost or stolen [20]. Besides, special-purpose devices also may be required to take record input for registration and authentication [52].

Profile Based Authentication

In a profile-based authentication system, a user profile, later to be used to verify users' authentication claim by generating challenge questions randomly, is stored at the verifier. A profile normally includes user specific information that is privacy-sensitive, for examples, personal details, education, activities, hobbies, professional experience, future plans, and learning programs [52]. This authentication is used in addition to the username and password technique, to supports student authentication.

Profile Based Authentication is based on multi-modal authentication which consists of two layers of authentication, namely, usernames and passwords, and challenge questions. Usernames and passwords are initially used to login into the online learning environment, before regular learning activities can take place during the first layer. During the learning process, students are posed with profile questions, so that, their individual profiles can be extended and refined. The second layer of authentication will trigger challenge questions generated from the students' individual profiles. Subsequently, profile questions will be asked to collect answers which are later to be used to build and update the students' individual profiles. Students' identities are verified by using the challenge questions.

Biometric Based Authentication

Biometric based authentication is used for user identification, based on physiological and behavioral characteristics, such as who the user is [21]. Some examples of physiological characteristics are fingerprint recognition, facial recognition, and iris recognition, behavioral characteristics include signature recognition, speech recognition and keystroke dynamics. Biometric based authentication is the most accurate [56], secure and convenient authentication tool, because it cannot be borrowed, stolen, forgotten and forging one is practically not easy [32]. However, it is also considered to be the most intrusive and expensive and a special hardware is required. Table 1 presents the summary of advantages and disadvantages of authentication types with the appropriate examples.

TABLE 1. Summary of advantages and disadvantages of authentication types

Types	Example	Advantages	Disadvantages
Knowledge	Password, PIN code, Lock Pattern, Graphical Password, Challenge question	Effortless, High acceptance	Can be passed on, easily forgotten, and shoulder surfing
Object	Badge, Physical keys, Smart Card	Cheap, Simple deployment	Loss and theft
Biometric	Physiological: Iris, Retinal, Face, Head, Hand signature, Fingerprints	Deter sharing Unique unforgettable	Costly, additional hardware required and invasive
	Behavioral: Voice, Signature, Gait, Mouse, Fingerprint, Keystroke analysis	Most accurate and convenient method	Can be used without any extra devices
Profile	Profile questions	Effortless High acceptance	Can be passed on

A number of studies have proposed advanced authentication mechanisms that can provide continuous authentication in online learning to the users by using biometrics. As in [55], facial biometrics provides competitive authentication methods and advances which ensure reliability and effectiveness to e-learning systems. Meanwhile, [33] proposed the use of Image Processing Based E-Learning approach which enables the online learners to be detected through the image processing method before all the interactions are verified using the proposed infrastructure. Besides, [18] used telephone-based oral examinations which can be used to verify a student's ability in relation to online test results and submitted assignments. This study has been proven to be sufficiently accurate to act as an effective deterrent against plagiarism.

On the other hand, [53] proposed the use of Profile Based Authentication Framework (PBAF) in a real online learning course with summative online examinations embedded. The PBAF collects answers to text-based personal and image questions during examinations for authentication purposes.

Based on the previous study, keystroke dynamics is the most popular method, because it only requires a keyboard with no extra devices [38]. Furthermore, it is inexpensive to implement, more distributed and more unobtrusive, compared to the other biometrics, while replications of the collected data are easy in cases where devices are not available. This type of authentication also can collect the data from anywhere through the internet and the software can be distributed via the client-server method, while no special training is needed for the users. Thus, this keystroke dynamics can be considered as the best tools to secure systems even if the user knows the username and password. Table 2 shows the summary of biometrics technologies.

TABLE 2. The summary of biometrics technologies

Types	Description	Advantages/Disadvantages
Fingerprint	Performs analysis of pattern found on fingertips	Highly accurate method but very costly
Hand Geometry	Evaluates unique hand characteristics, including length of the finger, its surface and thickness	Highly accurate method but very costly
Face Recognition	Analyzes unique facial characteristics of eyes, lips, nose, etc.	Very costly
Voice Recognition	Captures unique voice features, including pitch, frequency and tone	Additional hardware required and Invasive
Retinal Recognition	Identifies unique blood vessel pattern at the rear part of the eye by directing infrared light of low-intensity through pupil	Quite accurate but very costly
Iris Scanning	Analyzes the fleck pattern on the iris, which are on the eye surface.	Expensive
Hand Signature	Analyzes how a user signs the name, including velocity, speed, and pressure.	Additional hardware required and Invasive
Keystroke Dynamics	Analyzes how a user types on the terminal, done by monitoring the keyboard input.	Inexpensive, no extra devices required, non-invasive

KEYSTROKE DYNAMIC AUTHENTICATION

Keystroke Dynamics Authentication (KDA) has been increasingly highlighted as an alternative to securing passwords [44]. In fact, it is considered to be a more efficient way to authenticate the user while providing better security, compared to the other methods [56]. A typical KDA comprises a number of components, namely, data acquisition, feature extraction [39], classification or matching, decision, and retraining [50].

During the data acquisition stage, KDA data is collected from a number of input devices, including normal computer keyboard, virtual keyboard, customized pressure sensitive keyboard, numeric keyboard, cellular phone keyboard, smart phone keyboard and etc. The collected data of typing features is subsequently extracted to build the model that will be used to verify the claimed user. This KDA can be constructed using a variety of typing features, for examples, pressure applied on the keys, the duration taken between successive keys pressed, typing speed, and finger position on the keys. The basic features used in KDA are Single Key Action and Key Diagraph Action as in [30]. The single key action feature is the hold time of a given key, while the key diagraph action features include the Total Duration, which is the lapse between the first and the second key presses (Down- Down Time), the lapse between

the first key release and the second key press (Up-Down Time), and the lapse between the first and the second key releases (Up-Up Time) of a particular key diagraph.

Meanwhile, feature extraction is used to process and store a reference template for future applications. During this stage, dimension reduction, feature selection, and outlier detection may be required to increase the quality of feature data.

The classification or matching stage is used to categorize for making decision. Previous researchers have applied various algorithms to achieve the common goal, which is to increase the accuracy of the system. This stage can be divided into two categories, namely, statistical and machine learning approaches, presented in details in the following section.

In the decision stage, a final decision will be made, either a user is legitimate or otherwise, for a login into the session, based on the results of classification or matching algorithm.

The retraining stage is vital to regularly renew the stored reference template used to reflect the ongoing changes that may be affected due to the variability of user typing pattern discussed in the previous section.

KDA CLASSIFICATION

KDA classification can be broadly categorized into statistical approach and machine learning approach [49].

Statistical Approach

Statistical approach is the common choice, both at the infancy stage of keystroke dynamics research and in present work [49]. Its popularity is mainly due to its simplicity, low overhead and ease of implementation. Previous studies have primarily concentrated on statistical approach, mostly applied for static keystroke analysis as in [32]. The static keystroke is used to monitor the typing behavior of users at a specific time which is fixed text mode only [36]. The common generic statistical measures are mean, median, standard deviation and statistical t-test [49]. Previously, [32] utilized mean and average time for pressing time, dwell time and total password.

Machine Learning Approach

Over the years, the current machine learning and classification techniques have been extensively utilized in KDA research. A machine learning approach is used to classify and identify a pattern and make the correct conclusion based on the provided data. Based on [62], numerous metrics, including the the Manhattan distance, Euclidean distance, and the Mahalanobis distance have been studied. On the other hand, both classical and advanced classifiers include K-means methods, Bayesian classifiers, K-Nearest Neighbor (KNN) classifiers, support vector machines (SVMs), Fuzzy logic, and neural networks.

Recently, various artificial neural networks (ANNs) have been applied for variety of applications, especially in keystroke classification problems, using their ability to recognize complex noisy patterns. In the past, these networks have been extensively used in keystroke dynamics [1], [12], [40], [56] and [60]. However, neural networks have their own limitations, rendering them unable to become a substitute of traditional methods, such as statistical regression, time series analysis and pattern recognition.

The fact that neural network is not able to train well results in their lower detection accuracy due to this limitation [35]. Different hybrid approaches have been explored in the past to overcome the drawbacks of any one individual method, and neural network, together with fuzzy logic are used to complement each other; neural networks are good at being able to classify unseen data points, whereas fuzzy clustering enables the algorithm to generalize well [51]. By combining neural network and fuzzy logic, the system performance is improved.

In recent years, there has been a steadily growing interest in fuzzy neural network approach for other application as in [8], [19], [24], [29], [37], [48], [51], [56], [59] and [61].

KDA APPLICATION

In the recent years, KDA has been an active area of research [4] and becoming more popular among the researchers, thus making it a rapidly growing field [62], due to its advantages in terms of cost and ease of being integrated with existing security systems [4]. It has a high demand in securing access control for most applications, including public and private sectors. KDA is also useful in providing the cloud security, because security is an important concern for

any applications, especially those residing in the cloud [32]. This section reviews a trend of KDA applications, generally divided into few categories, namely. mobile devices, banking sector, health, and online learning.

KDA for Mobile Devices

The use of mobile devices in daily task, for example, mobile learning is becoming more common. Mobile learning has an array of features which cannot be neglected because of its being highly portable, contextual and personal [43]. The fact that, mobile devices have become indispensable in modern life, has caused mobile security to become much more important [61].

Based on a previous study, [50] focused on the use and creation of a touch dynamics dataset to find out the benefits of having touch dynamics and a PIN-based authentication method integrated together, to securely identify and authenticate a claimed identity for mobile devices. References [45] investigated the effectiveness of sensor-enhanced keystroke dynamics, which considered a recently introduced mobile biometric authentication mechanism which combines a particularly rich set of features. This study considered different kinds of attacks, focusing on advanced attacks drawn from statistics of general population. Attacks, such as these, have already been shown to be effective in significantly affecting the accuracy of the majority of the art biometric authentication systems. The study implemented a statistical attack against sensor-enhanced keystroke dynamics and evaluated the impacts caused on detection accuracy. In an initiative to enhance mobile security, an adaptive neuro-fuzzy inference system (ANFIS) which is based on implicit authentication system is proposed as in [61] to provide authentication in a continuous and transparent manner. The analysis for the study was conducted using behavioral data collected for 12 weeks from different Android users. The results obtained revealed that, ANFIS is a feasible and efficient method for implicit authentication, with an average of 95% user recognition rate.

KDA for Banking Sector

Credit card has increasingly become the most popular means of payment for both daily and online purchases [8]. Thus, the cases of fraud related to it are also on the rise, especially on online banking. A previous study focused on analysing the spending behavior among credit card users, viewed in term of the deviation from their past usage patterns, so as to ascertain if the transactions are fraudulent or genuine. Learning is also conducted on the suspicious transactions keep the misclassification of transactions at the minimum as in [8].

References [54] investigated keystroke dynamics and the possibility of its use as a tool to prevent or detect fraud in the banking industry. The results showed that, keystroke dynamics are capable of providing impressive accuracy rates for user identification with low costs of deployment and minimal change to users, making this technology an attractive investment for banks.

Besides, [11] looked forward to a number of processes for keystroke biometrics to enhance user authentication for banking transaction system. In this study, a keystroke-dynamics dataset was collected to create a repeatable evaluation procedure and to gauge the performance of a range of detectors, so that the results can be compared more precisely. All the four keystroke latencies and dwell time are used for making the dataset, which is used to suit the degree of variance of the user and to detect the authorization of the user.

KDA for Health

Keystroke dynamics can be affected by external factors, such as environmental conditions, type of keyboard device, injury and also emotional state. The injury, fatigue, or distraction might result in variation of typing rhythm [49]. This has influence the number of research increased in this field. References [25] conducted a study to investigate the source of variance commonly found in keystroke typing patterns resulting from emotions. The experimental results obtained showed a significant effect of emotion ($p < .001$) in the keystroke latency, accuracy rate of the keyboard typing and keystroke duration. Nonetheless, compared to the individual variability, the size of the emotional effect is insignificant.

Meanwhile, [13] conducted a research to ascertain user emotion by analysing the rhythms of their typing patterns on a standard keyboard. In the research, keystrokes produced by the participants and their states of emotions were collected via self-reports, before the keystroke features were extracted. The results from this research included 2-level classifiers for confidence, nervousness, hesitance, relaxation, tiredness and sadness, with accuracies in the range of 77 to 88%. Besides, it showed promises for anger and excitement, with accuracies as high as 84%.

Besides, [5] took an initial step toward addressing gaps in contributing to students' success by building a predictive model of student affect on writing when using multiple sources. This study used text indices, keystroke analyses and individual difference measures in predicting engagement as well as boredom in a total of 132 writing sessions. The results suggested that, these three categories of indices were proven to be effective in modelling students' affective states during writing. Other research as in [9] explore a combination keystroke timing statistics with task appraisal and stable traits to identify a user's effective emotion or state to enhance either the human or computer interaction.

KDA for Online Learning

A study by [46] investigated the use of stylometry biometrics and keystroke for the development of a robust system used to authenticate (verify) online test takers. Following this, statistics on the performance of stylometry, keystroke and combined keystroke-stylometry systems were deduced, based on data obtained from 40 test-taking students enrolled in a university course. Meanwhile, [3] conducted a research to determine the extent the users' identity can be established every time they use online resources, such as e-learning environments, when context features are evaluated. In the study, the template of the user was built using the latency between successive keystrokes, and the context of the written words, taking into account the location a particular letter stroke has taken place. Other contextual features have also been investigated to determine the ones that could help ascertain the identity of a user better. On the other hand, [10] the classification system for early detection of poor performers is based on student effort data, such as the complexity of the programs they write, and it shows how further improvements can be achieved by the use of low-level keystroke analytics. Meanwhile, [34] focused on the importance of stress in the learning process. This study implemented keystrokes and clicks to measure stress among e-learning users.

KDA BENCHMARKING DATASET

This section reviews a benchmarking dataset of KDA. The presently available keystroke dynamics datasets can be classified into two categories, namely, short text and long text, as shown in Fig. 2. The short texts, either uniquely identified or chosen by users, are mainly based on passwords. The long text datasets can also be classified into two categories, namely, fixed texts and free style typing, based on the type of activities involved. They mostly serve for continuous or active authentication purposes. According to [47], it is an important criterion to separate short and long texts, since all digraph statistics can be captured by the system, and a user can be transparently authenticated by typing any arbitrary text in long text data. Short text data is based on only sequence and length of the characters in the password, before the users are prompted to key in the exact phrase in each attempt.

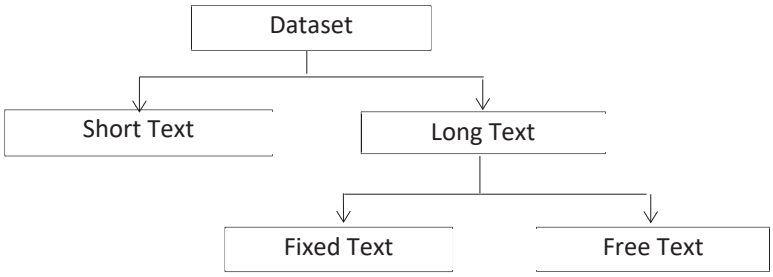

FIGURE 2. Type of KDA benchmarking dataset

The standard and publicly available keystroke dynamic datasets remain limited in number, compared to other disciplines [4], while certain datasets are not meant for public access. Based on previous literature reviews, there are a few benchmarking datasets available in keystroke dynamics field, such as CMU static Keystroke Benchmark Dataset (1) by [22], CMU Dynamic Keystroke Benchmark Dataset (2) by [23], GREYC Static Keystroke Benchmark Dataset (3) by [15], University at Buffalo's Static Keystroke Dataset (4) by [47], Clarkson University Mixed Keystroke Dynamic Dataset (5) by [58], and Web-GREYC Keystroke Dynamic Dataset (6) by [16]. The summary of KDA Benchmarking Dataset is presented in Table 3.

TABLE 3. Summary of KDA benchmarking dataset

No.	Type	Description	Url
1	Short text	51 users typed the text ".tie5Ronal" as password in eight sessions	Not available
2	Long, and free text	20 users provided 40 samples of free typing (a total of 20 subjects, 2 samples per subject)	http://www.cs.cmu.edu/keystroke/laser-2012/
3	Long and free text	133 users typed the text "greyc laboratory" using two different keyboards on the same computer in a period of two months.	http://www.ecole.ensicaen.fr/~rosenber/keystroke.html
4	Long and fixed text	148 subjects, involving two activities, answering survey questions and transcribing fixed text	http://cubs.buffalo.edu/research/datasets.
5	Long, fixed, and free texts	Contain passwords, transcription, and free texts from 39 users with two data sessions , approximately one hour each, on two separate days.	http://clarkson.edu/citer/research/collections/index.html
6	Short text	118 users typed imposed and free login or passwords within one year.	http://www.epaymentbiometrics.ensicaen.fr/index.php/app/resources/ 84.

Dataset 1 contains a very large number of samples. However, its time interval may be too small to track variability on a long period. This dataset is the only database which contains sufficient number of samples and users to give results which are statistically significant [16]. However, this research has only been used by the researchers themselves, and not by the community. Meanwhile, Dataset 2 provides keystroke data for free text and transcribed text. In the same study, the users provided a total of 40 samples of free typing for 20 subjects, 2 samples per subject and another 40 samples of transcription typing. Dataset 3, despite containing 133 users, the highest compared to the other datasets; its number of samples and sessions is too small to track variability through time. Dataset 4, the largest, compared to all publicly accessible keystroke dataset for long texts [47], includes two activities, namely, answering survey questions and transcribing fixed text, characterized to indicate temporal aspects of typing patterns and the effect caused by keyboard variability. Among all public ones, Dataset 5 is the largest in terms of the amount of text per subject. This dataset is also unique as it contains fixed, free, and transcribed texts together with video of facial expressions and hand movements. Lastly, Dataset 6 has the biggest number of different passwords and it is considered to be the most realistic keystroke dynamics dataset.

Furthermore, in order to assess the performance of this KDA, the performance metric is used. The most commonly used performance metric are false acceptance rate (FAR), false rejection rate (FRR) [63]. The FAR is the percentage of impostors who have accurately gained access to the system. In other hand, the FRR is the percentage of legitimate users who have been inaccurately access to the system [6]. The other commonly used performance metric is the Equal Error Rate (EER) where lower EER values indicate a more secure the system. It is often difficult to compare the result from previous studies because there are many different performance measures used in their system [6]. Besides, there is no standardizing form during the data collection process in these different experiments. It is because some procedure, environment and variation condition among study participant might result in different performance.

CONCLUSION

KDA facilitates a cost-effective and simple way for securing any computer application and devices. It also can continually monitor a user's typing behavior for the entire session without interruptions. Currently, KDA is still evolving due to its advantages and simplicity. Thus, this paper discussed its concept, types of biometrics, and classification. Besides, the different applications of keystroke dynamics and keystroke benchmarking dataset were also reviewed. It is recommended that, future work on KDA focus on online learning to improve the security of online learning environment.

ACKNOWLEDGEMENTS

This research was sponsored under the grant Reference Number: TIER1/2007 (Vot U896), a UTHM research grant by Universiti Tun Hussein Onn Malaysia and Gates IT Sdn. Bhd.

REFERENCES

[1] M. B. Abisado, B. D. Gerardo and A. C. Fajardo, "Towards keystroke analysis using neural network for multi - factor authentication of learner recognition in on - line examination." In *Manila International Conference on Trends in Engineering and Technology* (2017), 71–74.

[2] N. M. Agashe and N. Sonali, "A survey paper on continuous authentication by multimodal biometric." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 4, No. 11, 4247–4253, (2015).

[3] D. J. Aleix, A. M. M. Josea and S. P. Eugenia, "Using keystroke dynamics and context features to assess authorship in online learning environments" In 11th *International Technology, Education and Development Conference* (INTED, 2017), 3167–3176.

[4] M. L. Ali, V. M. John, C. T. Charles and Q. Meikang, "Keystroke biometric systems for user authentication" Journal of Signal Processing Systems, 86(2–3), 175–190. (2017).

[5] A. Laura, M. Caitlin, E. J. Matthew, M. Danielle, C. Scott and D. Sidney, "Investigating boredom and engagement during writing using multiple sources of information." In *Proceedings of the Sixth International Conference on Learning Analytics & Knowledge* (New York: ACM New York, NY, USA, 2016), pp. 114–123.

[6] A. Arwa and W. Kevin, "Keystroke dynamics authentication: A survey of free-text methods." Int. J. Comput. Sci., Vol. 10, Issue 4, No 1, 1–10, (2013).

[7] H. B. Mohammadreza, N. Mehrbaksh, I. Othman, Z. F. Ali and S. Sarminah, "Authentication systems: A Literature Review and Classification" Telematics and Informatics, Vol. 35, Issue 5, 1491–1511, (2018).

[8] K. B. Tanmay and P. Suvasini, "Credit card fraud detection: A hybrid approach using fuzzy clustering & neural network." In 2nd *International Conference on Advances in Computing and Communication Engineering* (IEEE, 2015), 494–499.

[9] B. Robert and D. Sidney, "Detecting boredom and engagement during writing with keystroke analysis, task appraisals, and stable traits." In *Proceedings of the 2013 International Conference on Intelligent User Interfaces* (2013), 225–234.

[10] C. Kevin, "Using keystroke analytics to improve pass–fail classifiers", Journal of Learning Analytics, Vol. 4, No. 2, 189–211, (2017).

[11] N. Chourasia, "Authentication of the user by keystroke dynamics for banking transaction system." *Proceedings of International Conference on Advances in Engineering & Technology* (2014), 41–45.

[12] D. Menal, "User authentication mechanism based on neural networks." International Journal of Computer Science and Mobile Computing, Vol. 5, Issue. 5, 563 – 566, (2016).

[13] E. Clayton, L. Michael and L. M. Regan "Identifying emotional states using keystroke dynamics.", In *Proceedings of the 2011 Annual Conference on Human factors in Computing systems* (2011), 715–724.

[14] F. L. Vonne, S. B. Karen and B. Jack, "Graduate students' perceptions of online learning." Research in Higher Education Journal, Vol. 27, Issue 27, 1–13, (2015).

[15] G. Romain, E. A. Mohamad and R. Christophe, "GREYC keystroke: A benchmark for keystroke dynamics biometric systems", In *IEEE 3rd International Conference on Biometrics: Theory, Applications and Systems*, (2009).

[16] G. Romain, E. A. Mohamad and R. Christophe, "Web-based benchmark for keystroke dynamics biometric systems: A statistical analysis." In *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (2012), 11–15.

[17] H. Gang, Y. Yu, L. Xiangxue, C. Kefei and L. Hui, "Characterizing the semantics of passwords: The role of pinyin for chinese netizens", Computer Standards & Interfaces, Vol. 54, Part 1, 20–28. (2017).

[18] P. H. Barry and R. John, "Student authentication for oral assessment in distance learning programs" IEEE Transactions on Learning Technologies, Vol, 1, Issues 3, 165–175, (2008).

[19] J. Jithish and S. Sriram, "A neuro-fuzzy approach for domestic water usage prediction" In *2017 IEEE Region 10 Symposium* (IEEE, 2017).

[20] A.K. Jain, A. Ross and S. Pankanti, "Biometrics: A tool for information security." IEEE Transactions on Information Forensics and Security, Vol. 1, Issue 2, 125–143, (2006).
[21] A. K. Nader and S. Zarina, "Review of user authentication methods in online examination" Asian Journal of Information Technology, Vol. 14, Issue 5, 166–175. (2015).
[22] K. Kevin and M. Roy, *Why Did My Detector Do That?! Predicting Keystroke-Dynamics Error Rates*, (Springer, Berlin, Heidelberg, 2010), 256-257.
[23] S. K. Kevin and R. Maxion, "Free vs. transcribed text for keystroke-dynamics evaluations." In *Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results* (2012), 1–8.
[24] K. Rajeev and M. K. Sharma, "Advanced neuro-fuzzy approach for social media mining methods using cloud." International Journal of Computer Applications, Vol. 137, Issue 10, 56–58, (2016).
[25] L. Poming, T. Wei-Hsuan, and R. H. Tzu-Chien, "The influence of emotion on keyboard typing: An e xperimental study using auditory stimuli." BioMedical Engineering OnLine, Vol. 3, Issue 1, 81–92. (2014).
[26] M. L. Frank and A. S. Mark, "The impact of an honor code on cheating in online courses." MERLOT Journal of Online Learning and Teaching, Vol. 7, Issue 2, 179–184, (2011).
[27] T. Matthews, "Passwords are not enough." In Computer Fraud and Security, Vol. 2012, 18–20, (2012).
[28] M. Václav and Ř. Zdeněk, *Advanced Communications and Multimedia Security* (Springer, Boston, MA, 2002). 1–13.
[29] M. Admir, A. Zikrija and O. Samir, "Intrusion detection system modeling based on neural networks and fuzzy logic." In *2016 IEEE 20th Jubilee International Conference on Intelligent Engineering Systems (INES)* (IEEE, 2016), 189–194.
[30] M. Soumik and B. Patrick, "A study on continuous authentication using a combination of keystroke and mouse biometrics." Neurocomputing 230, 1–22, (2017).
[31] Ö. M. Yasar, E. Ismail Ertürk and S. Refik, "Students' perceptions of online assessment: A case study." Journal of Distance Education, Vol. 19, No. 2, 77–92, (2004).
[32] A. P. Rohit and L. R. Amar, "Keystroke dynamics for user authentication and identification by using typing rhythm." International Journal of Computer Applications, Vol. 144, No. 9, 27–33, (2016).
[33] R. Sucianna, S. Sasmoko, Noerlina and H. Hanry, "Image processing model based e-learning for students authentication." *In International Conference on Information Management and Technology* (ICIMTech, 2017), 187–191.
[34] R. Manuel, G. Sérgio, C. Davide, N. Paulo and F. Florentino, "Keystrokes and clicks: Measuring stress on e-learning students." *In Second International Symposium Management Intelligent Systems* (2013), Vol. 220, 119–126.
[35] S.Shraddha, " Intrusion detection using artificial neural network." Advances in Neural Networks, Fuzzy Systems and Artificial Intelligence Intrusion, (1), 209–217, (2014).
[36] S. F. N. Sadikan, A. A. Ramli, S. Kasim, H. Mahdin, A. Salamat, and U. N. Wisesty, "An Initial Framework of Fuzzy Neural Network Approach for Online Learner Verification Process." In *5th International Research and Innovation Summit* (IRIS5, 2017), Vol. 5, 1–5.
[37] R. Saoreen, A. M. Shamim, U. A. Mahtab and K. M. Shamim, "PHY / MAC Layer Attack Detection System Using Neuro-Fuzzy Algorithm for loT Network. In International Conference on Electrical, Electronics, and Optimization Techniques (IEEE, 2016), 2531–2536.
[38] Sawant, M. M., Nagargoje, Y., Bora, D., Shelke, S., & Borate, V. (2013). Keystroke Dynamics: Review Paper. International Journal of Advanced Research in Computer and Communication Engineering, 2(10), 4018–4020. Retrieved from www.ijarcce.com
[39] H. S. Shaimaa, J. S. Riyadh and O. K Mina, "Keystroke Dynamics Authentication Based on Principal Component Analysis and Neural Network." *International Journal of Scientific and Engineering Research*, (2014a). 5(6), pp. 830–837.
[40] H. S. Shaimaa, J. S. Riyadh and O. K Mina, "Keystroke Dynamics Authentication Based on Principal Component Analysis and Neural Network." *International Journal of Scientific and Engineering Research* (2014b), 5(6), pp. 830–837.
[41] M. Sheila, M. A. Faizal and S. Shahrin, "Learner centric in M-learning: Integration of security, dependability and trust." *10th International Conference Mobile Learning* (2014), 318–322.
[42] C. Shen, T. Yu, H. Xu, G. Yang and X. Guan, "User practice in password security: An empirical study of real-life passwords in the wild." Computers and Security, 61, 130–141, (2016).
[43] Y. E. Shih, and D. Mills, "Setting the new standard with mobile computing in online learning." International Review of Research in Open and Distance Learning, Vol 8, No. 2, 1–16, (2007).

[44] S. Brajesh, S. Saurabh, S. Yash and S. Vaishakh, "Literature survey on keystroke dynamics for user authentication." International Journal on Recent and Innovation Trends in Computing and Communication, Vol. 5, No. 5, 280–282, (2017).
[45] D. S. Valeriu, S. Riccardo and C. Mauro "On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks." In *Proceedings of the Sixth ACM on Conference on Data and Application Security and Privacy* (2016), 105–112.
[46] C. S. John, M. Vinnie, C. Sung-Hyuk and C. T. Charles. "An investigation of keystroke and stylometry traits for authenticating online test takers." In *International Joint Conference on Biometrics* (2011), 1–7.
[47] S. Yan, C. Hayreddin and U. Shambhu, "Shared keystroke dataset for continuous authentication." In *International Workshop on Information Forensics and Security* (2017), 0–5.
[48] T. Fatma, W. Naoufel, A. Hussain, and S. S. Rachid, "Lung cancer detection by using artificial neural network and fuzzy clustering methods." American Journal of Biomedical Engineering, Vol. 2, No. 3, 136–142. (2012).
[49] S. T. Pin, B. J. T Andrew and Y. Shigang. "A survey of keystroke dynamics biometrics." The Scientific World Journal (2013).
[50] S. T. Pin, Z. Ning, B. J. T. Andrew and C. Ke. "Recognizing your touch: Towards strengthening mobile device authentication via touch dynamics integration." In *Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia* (2015), 108–116.
[51] J. A. Trivedi,"Voice identification system using neuro-fuzzy approach." International Journal of Advanced Research in Computer Science & Technology, Vol. 2, No. 3, 300–301, (2014)
[52] U. Abrar, X. Hannan, L. Mariana and B. Trevor, "Using challenge questions for student authentication in online examination." International Journal of Infomomics, Vol. 5, No.3, 631–639, (2012).
[53] U. Abrar, X. Hannan Xiao, L Mariana and B. Trevor, "Privacy and usability of image and text based challenge questions authentication in online examination." In *The International Conference on Education Technologies and Computers* (2014), 24–29.
[54] K. U. Ahmad and H. S. Mahmood "Strengthening e-banking security using keystroke dynamics." Journal of Internet Banking and Commerce, Vo. 18, No. 3, 1–14, (2013).
[55] V. Jasmine, V. Jacinto and G. Yvette, "A review on facial recognition for online learning authentication." In *Proceedings - 8th International Conference on Bio-Science and Bio-Technology*, (2015), 16–19.
[56] R. Vinayak and K. Arora,"A survey of user authentication using keystroke dynamics." International Journal of Scientific Research Engineering & Technology (IJSRET), Vol. 4, No. 4, 378–384, (2015).
[57] L. Vinayakvitthal, and N. N. Charniya, "Review of advances in neural network based biometric authentication." In *IEEE International Conference on Communications and Signal Processing* (2015), 735–740.
[58] E. Vural, J. Huang, D. Hou and S. Schuckers, "Shared research dataset to support development of keystroke authentication." In *International Joint Conference on Biometrics* (2014).
[59] G. Wang, J. Hao, J. Ma and L. Huang, "A new approach to intrusion detection using artificial neural networks and fuzzy clustering." Expert Systems with Applications, Vol. 37, No. 9, 6225–6232. (2010).
[60] S. B. Wankhede and S. Verma, "Keystroke dynamics authentication system using neural network." International Journal of Innovative Research and Development, Vol. 3, No.1, 157–164. (2014).
[61] F. Yao, S. Y. Yerima, B. Kang and S. Sezer, "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, London, UK: IEEE 2017).
[62] Y. Zhong, Y. Deng and A. K. Jain, "Keystroke dynamics for user authentication." *Computer Vision and Pattern Recognition Workshops (CVPRW), 2012 IEEE Computer Society Conference* (2012), 117–123.
[63] Y. Zhong and Y. Deng. (2015). "A survey on keystroke dynamics biometrics: Approaches, advances, and evaluations" (2015), 1–22.