Nano World Journal

https://doi.org/10.17756/nwj.2022-s1-020

Review Article

Open Access

Nanotechnology and Sensor Technology in Keystroke Dynamics

Kirty Shekhawat and Devershi Pallavi Bhatt*

Department of Computer Applications, Manipal University Jaipur, India

***Correspondence to:**
Devershi Pallavi Bhatt
Department of Computer Applications,
Manipal University Jaipur, India
E-mail: bhattdevershi@gmail.com

Received: August 23, 2022
Accepted: October 27, 2022
Published: October 29, 2022

Citation: Shekhawat K, Bhatt DP. 2022. Nanotechnology and Sensor Technology in Keystroke Dynamics. *NanoWorld J* 8(S1): S111-S119.

Published by United Scientific Group

Abstract

Passwords are the most used method for user authentication and accessing sensitive information from the internet. The increased popularity of the internet has elevated cybercrimes and has promoted other malicious uses. Security frameworks, essentially biometric frameworks are being developed in response to ever-increasing security threats. An advantage of using behavioral biometrics over physiological biometrics is that it can be used for surveillance also. The behavioral biometric that uses typing patterns to identify a person is called keystroke dynamics (KD). In KD, certain features are extracted that usually depend upon the time which the keys are held down and between latency of different keys. KD is the most sought-after authentication protocol as it is non-disruptive in nature, affordable, and seamless integration with existing technology without additional hardware. However, user authentication by KD shows less precision as compared to other biometric techniques. Research has been conducted for data acquisition, feature selection, and classification by machine learning (ML). The accuracy of keystroke biometrics is not equivalent too their biometric techniques such as hand geometry and iris recognition. Biomimetic nanotechnology is a new discipline inside the region of nano structuring and especially nanorobotics. This is because user consistency and uniqueness are difficult to achieve in keystroke biometrics. Integration of keystroke biometrics with sensor technology for better accuracy is less explored. The aim of this paper was to provide an insight into nano technology and sensor technology used in KD.

Keywords

Keystroke dynamics, Nanotechnology, Passwords, Sensors, User authentication, Nanotechnology

Introduction

Internet has become an indispensable part of our lives. According to a survey conducted by PEW Research Center in 2005-2016, the number of people using online platforms has increased from 5% to 69% in the USA [1]. Person-to-person communication stages might give ease in availability; however, the advancement in technology also opens entryways for criminals who use it to further their potential benefit. Security is a huge concern in this age of massive information transfer and storage. But to date, usernames and passwords are used to protect sensitive information [2]. Two factor authentication services such as One Time Password are also being used for superior security. Static usernames and passwords provide a simple and scalable model but are highly vulnerable to advanced security threats such as Brute Force attacks, Dictionary attacks, and data leaks.

On the other hand, two-factor authentication systems provide better security but at the cost of increased complexity. A lightweight cryptographic algorithm for en-

ergy efficient applications is discussed in [3]. A convenient and efficient solution to the scenario can be provided by Biometric security systems [4] in Biometric security authentication and access control [5]."Nanotechnology in the Security Systems" includes sensors, biosensors, security systems, nanotechnology, and nanomaterials. The characteristics may be physiological traits or behavioral traits. Physiological biometric systems are based on physical appearance such as fingerprint recognition, face recognition, palm print, etc. [6]. Behavioral biometrics are related to the behavior of the person such as gait, typing rhythm, and voice recognition [7]. Biometric security is preferred over conventional as well as advanced cryptographic security systems as these systems provide increased convenience and accuracy and eliminate the need for remembering passwords.

Behavioral biometrics is a better choice, if selection is to be made between the two types of biometric systems. This is because behavioral biometrics does not require complex and specialized hardware and can be used for monitoring the behavior of a person without his pieces of knowledge [8]. In keystroke biometrics, the typing behavior of the user is used to establish identification and authentication. KD are emerging as a promising security option. The combination of KD with emerging nanotechnology and sensor technologies can replace the existing security system. The aim of this paper was to review ML and sensor technologies in the context of KD, identify loopholes and suggest possible future directions. The rest of the paper was organized as follows: In section 2 the background dynamics were discussed. Research works related to the use of ML techniques in KD were discussed and compared in section 3. In section 4 sensor enhanced KD approaches were mentioned. Conclusion and recommendations for future research were presented in section5.

Background

The process of user's legitimate right before providing him access to secure resources authentication [9]. Authentication methods can be broadly categorized into 4 classes [10], these are object-based authentication, authentication methods include knowledge-based, password-based, and biometric [11]. The above-cited techniques were discussed briefly in Table 1 [12]. Authentication in valves cross-checking unique information provided by an individual. This peculiar data can be a token for biometrics or a piece of unique knowledge. The most used passwords are knowledge-based. The most common forms of knowledge-based passwords are text a graphics-based password, code or pattern, a personal identification number [13]. To this date, password-based authentication systems are standard or benchmark techniques for user authentication. Reasons for the immense popularity of password-based authentication system is the cost-effectiveness and easy implementation [14]. Over the years the security provided by passwords is being challenged by an increased number of intrusion attacks and wrongful use. There are many programs of nanotechnology in cyber security and to be able to handiest grow as time goes on.

The second category is token-based passwords [15]. This type of authentication system requires physical possession of an object is which is used for authentication. Token-based authentication systems can be deployed at a large scale; however, this approach is vulnerable to theft for loss. This means that even if the legitimate token is provided at the authentication stage, it cannot be ensured that the person possessing that token is genuine or authorized. Multiple stage authentication systems can resolve the above-mentioned token-based authentication systems. In multiple-stage authentication, the token is coupled with a knowledge-based method. This method can provide better security if the secrecy of knowledge is maintained.

The word biometric refers to the unique traits of an individual, with me be physical or behavioral. Biometrics is a profoundly unmistakable technique and can be utilized for differentiating different people [16]. Physiological or physical biometrics uses unique physical characteristics of a person's fingerprint, face, and iris scan. Physiological biometric demonstrate robust performance and high recognition accuracy.

Keystroke Dynamics

As was discussed in the preceding section, KD [17] analyses the user's typing style. Figure 1 displays the block diagram of a Keystroke Dynamics Authentication (KDA) system. The user is firstly required to enroll or register in the system. The significance of this phase is to generate a user profile and store it in a dataset. A user profile is generated by analyzing the input and extracting the relevant features. The classification of KD was shown in Figure 2. In static KDA user is required to enter a fixed text during all the login sessions, which is the same as entered in the registration phase. On the other hand, in Dynamic KDA, a user has the liberty to change the input. Dynamic KDA can be further classified as periodic KDA and Continuous KDA. In Periodic KDA the

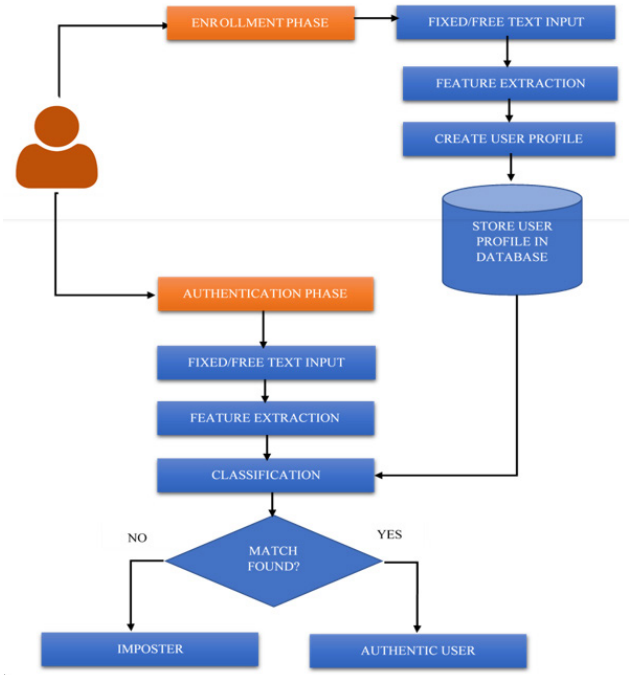

Figure 1: Block diagram of an authentication system using KD.

Table 1: Overview of different authentication approaches.

Biometric characteristics		
Physiological	**Fingerprint**	One of the oldest methods of biometric authentication is fingerprint recognition. The fingerprints changes with time and are hard to detect in case of injuries or accidents.
	Face recognition	Face recognition techniques uses image processing to anchor the feature of the face such as distance between eyebrows, face structure, etc.
	IRIS scan	The intrusive biometrics associated with the eye shape is the iris scan. An intimate user reader contact is not required in this technique and a simple camera is sufficient. This technique shows the highest efficiency.
	DNA	The most prominent way of establishing a person's identity physically is DNA matching. Many DNA profiling techniques can be used for this purpose such as Short Tandem Repeats analysis. This technique is used in situation where exact and precise matches required.
	Hand geometry	The security technique which works on the acquired physical features of hand and fingers of the users is called hand geometry. This technique is simple to use and provides satisfactory performance.
Behavioral	**Voice pitch**	Invoice identification technology a combination of physiological and cognitive variables is used to create a voice spectrograph. The voice is captured by a voice processing device. The different features for user identification by voice are rhythm, nestle tone, and basic frequency in flexion.
	Typing rhythm	The biometric technique which identifies the user based on his way of typing on keyboard is called identification by typing rhythm. The typing rhythm for the typing speed of each person is unique and forms the basis of this security domain. The processing of the extracted features from the typing rhythm are done in keystroke dynamics. The concept behind the security technique is that different users are different in typing speed and style.
	Signature	Signature recognition is also related to biometric identification as different crucial parameters such as stress level velocity and stroke can be incurred bisining physical activity. Signature recognition can be either dynamic or static.

authentication takes place at a predefined time period mostly during login, whereas in Continuous KDA the user is verified continuously in the entire session. Though Dynamic KDA is an enhancement over periodic KDA it increases architectural complicity and introduces computational overhead. Once the input is provided, feature extraction is performed. The extracted features may be conventional such as timing-based features or enhanced such as pressure and acceleration-based.

Timing-based features determine the pattern of key press and release events.

In the next step, user's profile is created using a combination of the above-mentioned features and it is stored in a database. Dwell time and flight time are the features that are most frequently extracted.

During testing, the features are once more dynamically extracted and contrasted with those already existent in the database. Classification is the most crucial step in the KD system. Both training database and classification algorithm determine the overall performance of KD based authentication system. Numerous techniques, including Statistical, Manhattan, Support Vector Machine (SVM), Genetic Algorithm, Hidden Markov Model (HMM) [18], Gaussian Mixture Model (GMM) [19], and Firefly algorithm [20], are used in the literature to test KD. It can be observed that most of the researchers have applied the ML algorithm in the classification phase. The publicly available datasets for KD are the CMU-2 dataset, Bio Chaves, Pressure Sensitive, GREYC, and web GREYC [21].

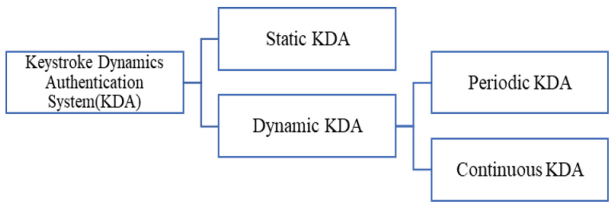

Figure 2: Topology of KD family.

The accuracy of KD is less when compared to other biometric techniques. The reason for this is a dependence of typing rhythm on the emotional state of a user, which makes user uniqueness and consistency a difficult task. The accuracy of KDA can be improved either by improving the quality of data and classification or by using some additional information like artificial cues and data from different sensors.

Traditional benchmarks or matrices for keystroke dynamics

The classifiers for KD are validated based on security matrices, namely False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER).

The FAR is a measure of the chances of accepting a malicious user. The FRR is a measure of the chances of rejecting an authorized user. FAR and FRR can be calculated by respectively. FAR and FRR are inversely proportional to each other, and a robust security system should have a low and equal value of FAR and FRR. This is called ERR. There are two categories of KD namely dynamic or free text and static or structured text. In static KD, the behavior of an individual is examined at fixed checkpoints and specific instances such as a login session. On the other hand, continuous monitoring takes place in dynamic KD.

An example of dynamic KD is analyzing user's typing behavior during browsing the internet along with a list of most frequently visited websites. The downside of Dynamic KDA is its intrusive nature, which may lead to security and privacy issues.

Feature extraction and classification are two important processes in KD [22]. Feature extraction is the process of extracting useful attributes of the user from his typing behavior. These features are used to create a user profile and characterize users. In the classification stage, these extracted features are categorized using different algorithms such as neural networks and machine learning and are matched to determine if the extracted features resemble the reference user. Based on this result the access rights are processed.

Feature extraction in keystroke dynamics

Typing rhythm is extracted while typing on a keyboard by an interface of computer and user. If proper data analysis and sampling techniques are applied to typing rhythm it can act as a crucial parameter for establishing a person's identity. In KD, certain features are extracted that usually depend upon the time which the keys are held down and between latency of different keys. Typical features extracted in keystroke biometrics were shown in Figure 3. Flight time is defined as the time elapsed between releasing one key and pressing another key. On the other hand, dwell time is defined as the time interval for which a particular key is pressed. Another feature that can be used in keystroke authentication is typing speed. Typing speed denotes the rate of typing characters or in other words, it defines a total number of characters typed in a unit time. Typing speed is not used while developing user authentication by KD due to its inaccuracy and insufficiency in defining the entire behavior of the user while typing.

Therefore, most of the research use flight time and dwell time as the prominent feature while designing user authentication by KD. Other advanced features such as digraph and trigraph, a virtual key force can also be used but requires higher computational power and specialized algorithms and in some cases hardware too. However, user authentication by KD shows less precision as compared to other biometric techniques. One possible reason for this is the variability in typing patterns even if not created intentionally.

Evaluation

Actual User Authentication is the act of conforming user's authenticity through active human to machine transfer of credentials. Actual imposters are the intruders that launch user-level attacks to take over rights from the user either during the start or in the middle of a session. There are 4 rates of evaluating accuracy:

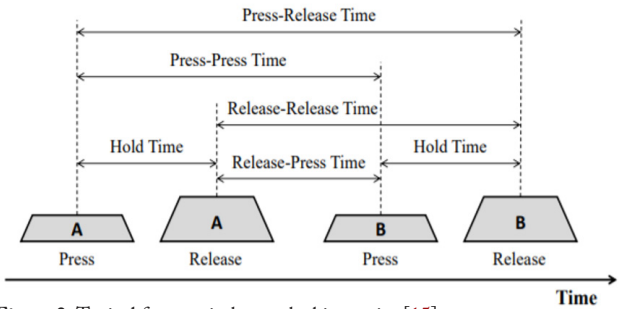

Figure 3: Typical features in keystroke biometrics [15].

True positive

True positive rate refers to the number of cases in which the actual user was an authentic user and the biometric security system also predicted authentic user.

False negative

False Negative is the rate at which the actual user was an authentic user, but the biometric system predicted it as an imposter.

False positive

False Positive is the rate at which the user was an imposter, but the biometric system classified it as an authentic user.

True negative

True Negative is the rate at which the person was an imposter and the biometric system also classified it as an imposter.

As mentioned in the previous section, the typing pattern of the user is analyzed in KD. The block diagram of a KDA system was shown in Figure 3. The user is firstly required to enroll or register in the system.

The significance of this phase is to generate a user profile and store it in a dataset. A user profile is generated by analyzing the input and extracting the relevant features. Based on the type of input KD can be static or dynamic [21]. In static KDA user is required to enter a fixed text during all the login sessions, which is the same as entered in the registration phase. On the other hand, in Dynamic KDA, a user has the liberty to change the input. As shown in Figure 2, Dynamic KDA can be further classified as Periodic KDA and Continuous KDA [23].

The subsequent step is to create a user profile by using any combination of the extracted features and store it in the database. Dwell time and flight time are most used for this purpose [21]. The extracted features are stored in the database in form of a user profile. In the testing phase, the extracted features are compared against the user profiles present in the database. Therefore 'classification' is the most important step. The classification algorithm and training database have a profound impact on the overall performance of the authentication system. Due to this KDA is tested by using different classification algorithms for instance Statistical [24], Manhattan [25], SVM [26], Genetic Algorithm [27], HMM [28], GMM [29], and firefly algorithm [30]. ML algorithms are mostly used in classification. Publicly available datasets such as GREYC. web GREYC, Pressure Sensitive, Bio Chaves, and CMU-2 dataset can be used for validation purposes [31]. When compared with other biometric techniques, KD show relatively less accuracy. This is because typing rhythm is extremely variable and depends upon a person's concentration level, emotional state as well. The accuracy of KDA can be increased by many improving the data classification using ML techniques or by obtaining additional information such as pressure and typing force using different sensors.

Benefits and limitations of keystroke dynamics

The benefits of KD were as summarized below [32, 33].

KD can show a high percentage of user adoption and user convenience as it is not an intricate process. Most people use a computer in their daily life and are often habitual with it. KD can be easily integrated into the present consumer devices. KD can not only be used for security purposes but also for container surveillance.

The KD has some disadvantages as well, which were summarized below [34-37]

1. Uniqueness and user consistency are hard to achieve.
2. The KD uses typing rhythm or typing path pattern for user authentication which often varies with emotional state and stress level.
3. The system is susceptible to a high level of vulnerability even if not intentionally created.

Machine Learning Techniques in Keystroke Dynamics

The past decade has witnessed enormous development in ML and classification techniques. The paradigm of ML is to identify the patterns in data and draw plausible conclusions from it. ML techniques are used for developing efficient cryptographic algorithms. Artificial Neural Network based efficient hashing algorithm was demonstrated [17]. These are extensively used in KDA systems. The classification in KDA can be performed using numerical metrices such as Euclidean distance and Manhattan distance but ML techniques are preferred due to better efficiency. KDA is developed using both classical and advanced ML techniques. Some examples of these techniques are NN, SVM, K-Nearest Neighbors (KNN), and HMM.

The interconnection between noise and features in data is obtained by using HMM. HMM is a system of hidden variables that have a conditional or generative dependency. This makes HMM suitable for KDA. The use of HMM in KDA was demonstrated [38]. The accuracy of ML based techniques directly depends on the size and quality of the training dataset. Nevertheless, handling a large dataset is a strenuous task. Unsupervised ML techniques such as KNN can be used while working with a dataset of a small sample size. KNN was used in the development of a KDA [39, 40].

SVM was used as a classification algorithm in KD analysis [41-43]. In recent times NN are also being used to solve classification problems in keystroke dynamics. NN can find inherent patterns even in a complex and noisy system. NN was used for predicting missing digraphs [44]. The experimental results were FAR equal to 0.0152% and FRR equal to 4.82%. NN cannot be used as a substitute algorithm for traditional methods like statistical regression as these methods require high training data, processing resources, and time. The limitations of NN lead to the development of hybrid technologies. For example, fuzzy logic and NN were used in conjunction with each other in KDA [44-49]. The system was able to achieve significant accuracy as fuzzy logic helps in generalizing the data and NN helps in exploring the missing dataset.

Time Based Technology

Statistical methods and typing patterns were used to develop a stronger authentication system as compared to the password authentication system picture [50]. Flight time and dwell time were extracted from the typing rhythm and a user profile was created using meantime or average time.

The habitual rhythm and password were used for designing an authentication system [51]. The data was collected from 15 users while typing three common passwords 6 times. The stage was used in this research and the extracted features were flight time and dwell time.

Bayesian regularized feed-forward neural network (BRNN) was implemented in KD based authentication systems and [52]. The data collected from 20 users who provided 50 samples in four sessions. The input layer of the BRNN consisted of 23 neurons and the output layer consisted of 20 neurons.

An innovative approach for improving the efficiency of a KD based authentication system was presented [53]. In this research work, the user was instructed to set the password in his preferred language instead of the benchmark language.

Alsuhibany et al. have reviewed the progress in the field of keystroke dynamics in the time of 2008-2013 [21]. The prominent research works were compared based on database, experiment, results, and performance. The appropriateness and nature of typing rhythm as an authentication system were presented in [54]. A review of the KD method was presented in [55] and the authors concluded that adding KD with the existing security systems can enhance security and privacy. In [56] the authors tested the performance of keystroke-based authentication systems in a situation of synthetic attached. The research work proposes a novel keystroke data representation model using potential functions and a decision tree algorithm of ML. The results revealed that the proposed system can be used in a real-life authentication system.

Artificial Cues

In [57] the authors and emphasized the importance of user consistency and uniqueness in a keystroke biometric system. Uniqueness refers to the difference in the user's patterns from an imposter as well as from other users. Consistency refers to the similarity in the user's pattern when he uses the system multiple times. Artificial cues are used with Easter biometrics to improve user consistency and recognition. In this research work, fixed text was used with artificial cues in the registration phase. However, it was not specified which fuels were most significant for the user.

The authors in [58] demonstrate that the increase in uniqueness and consistency of user translates into a new and improved authentication system and better recognition accuracy. Artificial rhythms and tempo cues when added explicitly in the password during the registration phase led to more distinct feature extraction and classification.

The capacity of time and sound information for authentication and identification of users was investigated [59]. The research work has compared timing based and audio-based KD for this purpose 50 test subjects were instructed to type a password a hundred times in 4 sections. The accuracy of the sound-based authentication system is an investigator [60]. This paper compares both timing based and audio-based keystroke dynamics systems in authentication as well as identification stage. The hypothesis that artificial cubes improve consistency, uniqueness, and discriminability was tested and validated [61]. The Mouse signatures were used as secondary factor for improving the recognition efficiency keystroke biometric system [62].

Rhythm key based encryption scheme for ubiquitous devices (Ubi-RKE) was presented in [63]. Key memo ability and secure encryption based on the user's typing rhythm were provided by this algorithm on ubiquitous devices. The proposed research work was a benchmark technique and was more efficient than other existing schemes as it provides a strong cipher. The research work related to artificial cues was summarized. Accuracy of 90.6% was achieved and EER of less than 2 percent was achieved [64]. It can be concluded that artificial cues and rhythm improves the efficiency of KD.

Keystroke Dynamics with Sensor Data and Nanotechnology

The advancement in Micro Electromechanical Systems, Very Large Integration technologies has led to the availability of different sensors for instance pressure, temperature, gyroscope, accelerometers, and many others. An approach for sensor enhanced KD using a pressure sensor was depicted [65]. In sensor enhanced KDA the data was acquired in real-time from different sensors. Then this data was fused with timing data to decrease EER. An EER of 0.08% was obtained using a pressure sensor [66]. The authors in [67] have used KD timing parameters with pressure parameters of the keyboard and an EER of 0.6% was achieved. The proposed device was applied with the biometric sensor, which identifies the fingerprint pattern, as soon as the voter places his left-hand index finger [68]. Classifier fusion technique was used along with pressure sensor keyboard to achieve EER of 1.41% [69]. A two-factor authentication system using pressure-enhanced keystroke dynamics was developed. SVM was used as a classifier; the experimental result was 99.67% accuracy. In this experience the identification of self-meeting.

Processes in dwelling systems and their self-prepared dynamical states with the information about their sensitivity and selectivity have paved the manner for developing new strategies for controlling the dynamic of self-assembled systems in nanoscale [70]. Accelerometers were used to obtain motion data during typing and thus enhance accuracy [71]. This approach was used and EER obtained was 7.89. KDA system was also developed using acoustic signals [40]. Acoustic signals obtained during typing were analyzed with timing data [72]. However, using acoustic signals does not lead to considerable improvement in EER. The most significant results were found in [74]. In this research, EER was as low as 1.41%, on a sufficiently large sample size of 5000 samples by using pressure sensors. In other research work, the performance was not as good as with artificial cues. However, this domain is ever evolving as it is more practical and easier to commercials as compared to the former.

Soft Biometrics

Keystroke biometrics is also used in identifying soft biometric traits of a person such as age, gender, and left handedness or right handedness. Authors in [73] have used typing patterns of a computer keyboard to protect extra information about a user such as age group, gender (male/female), emotional state (excitation/anger), type of handling (using one hand or two) [74]. A novel approach for predicting soft biometrics by using KD was presented and referenced [75-77]. On the other hand, soft biometrics is used as secondary formation with a KD based authentication system to improve the recognition efficiency in reference.

Conclusion

KD is not a buzzword and was proposed in 1975. KD is non-intrusive biometric security and can be easily implemented without additional hardware or training. In this paper, the previous research works related to the development of authentication systems based on KD have been summarized. The authors have focused on the intersection of KD with ML and sensor technologies. From the survey, it was observed that a plethora of ML based KD system exists and extensive research was conducted on the same. However, the research was not generalized, and different authors have used different ML algorithms on different datasets or numbers of users. Research can be conducted, which provides a comparative analysis of all prominent ML algorithms with a similar dataset, or on different publicly available datasets. Research can also be conducted for degerming the most suitable ML technique depending on the number of users and type of features. Another research gap is that most studies were based on conventional features i.e. timing-based features and usability of non-conventional features should be further explored. Research in sensor enhanced KD is still at an initial stage and requires dedicated efforts. It can be observed that the efficiency of KDA can be enhanced by using different sensors. Best results are obtained when pressure sensors are used, a possible reason behind this may be that data acquired from pressure sensors indirectly represents the typing force, which is unique for an individual. Research can be conducted to determine the effect of placement and number of pressure sensors on the EER. A comparative study can be performed which provides insight about the effect on EER by using pressure sensors with different ML techniques explored.

References

1. Pew Research Center [www.pewresearch.org] Accessed on November 18, 2022.
2. Yang L, Li C, You R. Tu B, Li L. TKCA: a timely keystroke-based continuous user authentication with short keystroke sequence in uncontrolled settings. *Cybersecur* 4: 13. https://doi.org/10.1186/s42400-021-00075-9

3. Bhatt DP, Raja L, Sharma S, 2020. Light-weighted cryptographic algorithms for energy efficient applications. *Journal of Discrete Mathematical Sciences and Cryptography* 23(2): 643-650. https://doi.org/10.1080/09720529.2020.1729510
4. Aloul F, Zahidi S, El-Hajj W. 2009. Two factor authentication using mobile phones. IEEE/ACS International Conference on Computer Systems and Applications, pp 641-644. https://doi.org/10.1109/AICCSA.2009.5069395
5. More SB, Ubale AB, Jondhale KC. 2008. Biometric Security. First International Conference on Emerging Trends in Engineering and Technology, pp 701-704. https://doi.org/10.1109/ICETET.2008.71
6. Eliashberg J, Chatterjee R. 1985. Analytical models of competition with implications for marketing: issues, findings, and outlook. *J Mark Res* 22(3): 237-261. https://doi.org/10.1177/002224378502200302
7. Lanchester FW. 1916. Aircraft in warfare: the dawn of the fourth arm. London, Constable and Company Limited, UK.
8. Kiyani AT, Lasebae A, Ali K, Rehman MU, Haq B. 2020. Continuous user authentication featuring keystroke dynamics based on robust recurrent confidence model and ensemble learning approach. *IEEE Access* 8: 156177-156189. https://doi.org/10.1109/ACCESS.2020.3019467
9. Theh PS, Zhang N, Teoh ABJ, Chen K. 2015. Recognizing your touch: towards strengthening mobile device authentication via touch dynamics integration. Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia, pp 108-116. https://doi.org/10.1145/2837126.2837127
10. Sadikan SFN, Ramli AA, Kasim S, Mahdin H, Salamat MA, et al. 2019. An initial framework of fuzzy neural network approach for online learner verification process. *International Journal of Advanced Trends in Computer Science and Engineering* 8: 185-189. https://doi.org/10.30534/ijatcse/2019/3781.32019
11. Maharjan P, Kumar S, Bhatta T, Cho H, Park C, Salauddin Md. 2021. Keystroke dynamics based hybrid nanogenerators for biometric authentication and identification using artificial intelligence. *Adv Sci* 8(15): 2100711. https://doi.org/10.1002/advs.202100711
12. Teh PS, Jin AB, Yue S. 2013. A survey of keystroke dynamics biometrics. *The Scientific World Journal* 2013: 408280. https://doi.org/10.1155/2013/408280
13. Shepherd SJ. 1995. Continuous authentication by analysis of keyboard typing characteristics. Proceedings of the 1995 European Convention on Security and Detection, pp 111–114.
14. Karnan M, Akila M, 2009. Identity authentication based on keystroke dynamics using genetic algorithm and particle swarm optimization. Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT '09), pp 203–207.
15. Harilal A, Toffalini F, Homoliak I, Castellanos J, Guarnizo J, et al. 2018. The Wolf of SUTD (TWOS): a dataset of malicious insider threat behavior based on a gamified competition. *J Wirel Mob Netw Ubiquitous Comput Dependable Appl* 9(1): 54-85. https://doi.org/10.22667/JOWUA.2018.03.31.054
16. Ngugi B, Kahn BK, Tremaine M. 2011. Typing biometrics: impact of human learning on performance quality. *Journal of Data and Information Quality* 2(2): 1-21. https://doi.org/10.1145/1891879.1891884
17. Shekhawat K, Bhatt DP. 2019. Recent advances and applications of keystroke dynamics. International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 680-683. https://doi.org/10.1109/ICCIKE47802.2019.9004312
18. Mankiw NG. 2014. Principles of microeconomics. Cengage Learning, Harvard University, USA.
19. Spiegel M, Tookes H. 2007. Dynamic competition, innovation and strategic financing. Yale School of Management. pp 1-63.
20. Pisani PH, Lorena AC. 2015. Emphasizing typing signature in keystroke dynamics using immune algorithms. *Appl Soft Comput* 34: 178-193. https://doi.org/10.1016/j.asoc.2015.05.008
21. Alsuhibany SA, Almuqbil AS, Wang D. 2021. Analyzing the effectiveness of touch keystroke dynamic authentication for the arabic language. *Wireless Communications and Mobile Computing* 2021: 9963129. https://doi.org/10.1155/2021/9963129
22. Trojahn M, Arndt F, Ortmeier F. 2013. Authentication with keystroke dynamics on touch screen keypads-effect of different N-graph combinations. MOBILITY 2013: The Third International Conference on Mobile Services, Resources, and Users, pp 114-119.
23. Alshehri A, Coenen F, Bollegala D. 2018. Iterative keystroke continuous authentication: a time series based approach. *Künstl Intell* 32: 231-243. https://doi.org/10.1007/s13218-018-0526-z
24. Chang T, Tsai C, Lin J. 2012. A graphical- based password keystroke dynamic authentication system for touch screen handheld mobile devices. *Journal of system and software* 85(5): 1157-1165. https://doi.org/10.1016/j.jss.2011.12.044
25. Killourhy K, Maxion R. Why did my detector do that? In: Jha S, Sommer R, Kreibich C (eds) Recent advances in intrusion detection. Springer, Berlin, Heidelberg, Germany, pp 256-276. https://doi.org/10.1007/978-3-642-15512-3_14
26. Giot R, El-Abed M, Rosenberger C. 2009. Keystroke dynamics with low constraints SVM based passphrase enrollment. IEEE International conference on biometrics: theory, applications and systems, pp 1-6. https://doi.org/10.1109/BTAS.2009.5339028
27. Dwivedi C, Kalra D, Naidu D, Aggarwal S. 2018. Keystroke dynamics based biometric authentication: a hybrid classifier approach. IEEE Symposium series on computational intelligence (SSCI), pp 266-273. https://doi.org/10.1109/SSCI.2018.8628852
28. Rodrigues R, Yared G. 2006. Biometric access control through numerical keyboards based on keystroke dynamics. In: Zhang D, Jain A (eds) Advances in biometrics. Springer, Berlin, Heidelberg, Germany, pp 640-646. https://doi.org/10.1007/11608288_85
29. Hosseinzadeh D, Krishnan S. 2008. Gaussian mixture modeling of keystroke patterns for biometric applications. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 38(6): 816-826. https://doi.org/10.1109/TSMCC.2008.2001696
30. Muthuramalingam A, Gnanamanickam J, Muhammad R. Optimum feature selection using firefly algorithm for keystroke dynamics. In: Abraham A, Muhuri P, Muda A, Gandhi N (eds) Advances in intelligent systems and computing. Springer, Cham, pp 399-406. https://doi.org/10.1007/978-3-319-76348-4_39
31. Giota R, B. Dorizzib and C. Rosenberger. 2015. A review on the public benchmark databases for static keystroke dynamics. *Comput Secur* 55: 46-61. https://doi.org/10.1016/j.cose.2015.06.008
32. Senk C, Dotzler F. 2011. Biometric authentication as a service for enterprise identity management deployment: a data protection perspective. Sixth International Conference on Availability, Reliability and Security, pp 43-50. https://doi.org/10.1109/ARES.2011.14
33. de Ru WG, Eloff JHP. 1997. Enhanced password authentication through fuzzy logic. IEEE Expert, 12(6): 38-45. https://doi.org/10.1109/64.642960
34. Maisuria LK, Soon OC, Kin LW. 1999. Comparison of artificial neural networks and cluster analysis for typing biometrics authentication. IJCNN'99. International Joint Conference on Neural Networks, 5: 3295-3299. https://doi.org/10.1109/IJCNN.1999.836188
35. Kang P, Hwang SS, Cho S. 2007. Continual retraining of keystroke dynamics based authenticator. Lee SW, Li SZ (eds) Advances in biometrics. Springer, Berlin, Germany, 4642: 1203-1211. https://doi.org/10.1007/978-3-540-74549-5_125
36. Teh PS, Teoh ABJ, Tee C, Ong TS. 2010. Keystroke dynamics in password authentication enhancement. *Expert Syst Appl* 37(12): 8618-8627. https://doi.org/10.1016/j.eswa.2010.06.097
37. Giot R, Dorizzi B, Rosenberger C. 2011. Analysis of template update strategies for keystroke dynamics. IEEE Workshop on Computational Intelligence in Biometrics and Identity Management (CIBIM), pp 21-28. https://doi.org/10.1109/CIBIM.2011.5949216

38. Monaco JV, Tappert CC. 2018. The partially observable hidden Markov model and its application to keystroke dynamics. *Pattern Recognition* 76: 449-462. https://doi.org/10.1016/j.patcog.2017.11.021
39. Wesoowskiet TE, Porwik P. 2015. User verification based on the analysis of keystrokes while using various software. *Journal of Medical Informatics & Technologies* 24: 13-22.
40. Mhenni A, Cherrier E, Rosenberger C, Amara NEB. 2018. Towards a secured authentication based on an online double serial adaptive mechanism of users' keystroke dynamics. International Conference on Digital Society and eGovernments (ICDS), pp 1-9.
41. Alsultan A, Warwick K, Wei H. 2017. Non-conventional keystroke dynamics for user authentication. *Pattern Recognit Lett* 89: 53-59. https://doi.org/10.1016/j.patrec.2017.02.010
42. Kim J, Kim J, Kang P. 2018. Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection. *Appl Soft Comput* 62: 1077-1087. https://doi.org/10.1016/j.asoc.2017.09.045
43. Alsultan A, Warwick K, Wei H. 2018. Improving the performance of free-text keystroke dynamics authentication by fusion. *Appl Soft Comput* 70: 1024-1033. https://doi.org/10.1016/j.asoc.2017.11.018
44. Ahmed AA, Traore I. 2013. Biometric recognition based on free-text keystroke dynamics. IEEE Transactions on Cybernetics, 44(4): 458–472. https://doi.org/10.1109/TCYB.2013.2257745
45. Sridhar M, Abraham T, Rebello J, D'souza W, D'Souza A. 2013. Intrusion detection using keystroke dynamics. In: Das V. (ed) Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing. Springer, New York, USA, pp 137-144. https://doi.org/10.1007/978-1-4614-3363-7_16
46. Deng Y, Zhong Y. 2013. Keystroke dynamics user authentication based on Gaussian mixture model and deep belief nets. *Int Sch Res Notices* 2013: 565183. https://doi.org/10.1155/2013/565183
47. Balagani KS, Phoha VV, Ray A, Phoha S. 2011. On the discriminability of keystroke feature vectors used in fixed text keystroke authentication. *Pattern Recognit Lett* 32(7): 1070-1080. https://doi.org/10.1016/j.patrec.2011.02.014
48. Purgason B, Hibler D. 2012. Security through behavioural biometrics and artificial intelligence. *Procedia Comput Sci* 12: 398-403. https://doi.org/10.1016/j.procs.2012.09.093
49. Chang TY. 2012. Dynamically generate a long-lived private key based on password keystroke features and neural network. *Information Science* 211: 36-47. https://doi.org/10.1016/j.ins.2012.04.009
50. Zhao G, Yang J, Jun C, Zhu G, Jiang Z, et al. 2018. Keystroke dynamics identification based on triboelectric nanogenerator for intelligent keyboard using deep learning method. *Adv Mater Technol* 4(1): 1800167. https://doi.org/10.1002/admt.201800167
51. Roy S, Roy U, Sinha DD. 2014. Enhanced knowledge-based user authentication technique via keystroke dynamics. *International Journal of Engineering Science Invention* 3(9): 41-48.
52. Zareen FJ, Matta C, Arora A, Singh S, Jabin S. 2018. An authentication system using keystroke dynamics. *Int J Biom* 10(1): 65. https://doi.org/10.1504/IJBM.2018.10011201
53. Bours P, Brahmanpally S. 2017. Language dependent challenge-based keystroke dynamics. International Carnahan Conference on Security Technology (ICCST), pp. 1-6. https://doi.org/10.1109/CCST.2017.8167838
54. Marriott P. 2004. Authentication by typing rhythm. [https://www.giac.org/paper/gsec/4118/authentication-typing-rhythm/106548]
55. Sawant MM, 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.
56. Serwadda A, Phoha V. 2013. Examining a large keystroke biometrics dataset for statistical-attack openings. *ACM Transactions on Information and System Security* 16(2):1-30. https://doi.org/10.1145/2516960
57. Cho S, Hwang S. 2005. Artificial rhythms and cues for keystroke dynamics based authentication. In: Zhang D, Jain AK (eds) Advances in biometrics. Springer, Berlin, Heidelberg, Germany, pp 626-632. https://doi.org/10.1007/11608288_83
58. Hwang SS, Lee HJ, Cho S. 2009. Improving authentication accuracy using artificial rhythms and cues for keystroke dynamics-based authentication. *Expert Systems with Applications* 36(7): 10649-10656. https://doi.org/10.1016/j.eswa.2009.02.075
59. Pleva M, Bours P, Ondáš S, Juhár J. 2017. Improving static audio keystroke analysis by score fusion of acoustic and timing data. *Multimed Tools Appl* 76: 25749-25766. https://doi.org/10.1007/s11042-017-4571-7
60. Bours P, Kiktov E, Pleva M. 2015. Static audio keystroke dynamics. In: Dziech A, Leszczuk M, Baran R (eds) Multimedia communications, services and security. Springer, Cham, pp 159-169. https://doi.org/10.1007/978-3-319-26404-2_13
61. Kang P, Park S, Cho S, Hwang SS, Lee HJ. 2006. The effectiveness of artificial rhythms and cues in keystroke dynamics based user authentication. In: Chen H, Wang FY, Yang CC, Zeng D, Chau M, et al. (eds) Intelligence and security informatics. pp 161-162. https://doi.org/10.1007/11734628_22
62. Chang T, Yang Y, Peng C. 2010. A personalized rhythm click-based authentication system. *Information Management & Computer Security* 18(2): 72-85. https://doi.org/10.1108/09685221011048328
63. Lee JD, Im HJ, Kang WM, Park JH. 2014. A rhythm key based encryption scheme for ubiquitous devices. *Mathematical Problems in Engineering* 2014: 683982. https://doi.org/10.1155/2014/683982
64. Hori T, Kita Y. Empirical evaluation of rhythm-based authentication method for mobile devices. In: Barolli L, Enokido T, Takizawa M (eds) Advances in network-based information systems. Springer, Cham, pp 529–538. https://doi.org/10.1007/978-3-319-65521-5_46
65. Loh SXC, Ow-Yong HY, Lim HY, Lai WK, Lim LL. 2017. Fuzzy inference for user identification of pressure-based keystroke biometrics. 2017 IEEE 15th Student Conference on Research And Development (SCOReD), pp 77-82. https://doi.org/10.1109/SCORED.2017.8305417
66. Suraj, Sarma P, Yadav AK, Barma S. 2018. Keystroke rhythm analysis based on dynamics of fingertips. In: Tanveer M, Pachori R (eds) Machine intelligence and signal analysis. Springer, Singapore, pp 555–567. https://doi.org/10.1007/978-981-13-0923-6_48
67. Trojahn M, Arndt F, Ortmeier F. Authentication with time features for keystroke dynamics on touchscreens. In: De Decker B, Dittmann J, Kraetzer C, Vielhauer C (eds) Communications and multimedia security. Springer, Berlin, Heidelberg, Germany, pp 197–199. https://doi.org/10.1007/978-3-642-40779-6_17
68. Thamizharasan N, Geetha A. 2017. Integration of biometric sensor with Aadhaar for voting process. *J Environ Nanotechnol* 6(1): 19-22. https://doi.org/10.13074/jent.2017.03.171237
69. Trojahn M, Ortmeier F. 2013. Toward mobile authentication with keystroke dynamics on mobile phones and tablets. 27th International Conference on Advanced Information Networking and Applications Workshops, pp 697-702. https://doi.org/10.1109/WAINA.2013.36
70. Gholpayeghani M, Raiesdana S, Nasrabadi A. 2007. Biometric nanotechnology and nonlinear dynamics. First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07), pp 8. https://doi.org/10.1109/ICQNM.2007.4
71. Antal M, Nemes L. 2016. The MOBIKEY keystroke dynamics password database: benchmark results. In: Silhavy R, Senkerik R, Oplatkova Z, Silhavy P, Prokopova Z (eds) Software engineering perspectives and application in intelligent systems, pp 35-46. https://doi.org/10.1007/978-3-319-33622-0_4
72. Nonaka H, Kurihara M. 2004. Sensing pressure for authentication system using keystroke dynamics. International Conference on Computational Intelligence, pp 17-19.

73. Lv H, Wang WY. 2006. Biologic verification based on pressure sensor keyboards and classifier fusion techniques. IEEE Transactions on Consumer Electronics, 52(3): 1057-1063. https://doi.org/10.1109/TCE.2006.1706507

74. Roy S, Roy U, Sinha DD. 2019. Feasibility of predicting soft biometric traits based on key stroke dynamics characteristics. *International Journal of Computer Sciences and Engineering* 7(1): 150-157.

75. Srividya B. 2016. Nanotechnology in forensics and its application in forensic investigation. *Research and Reviews: Journal of Pharmaceutics and Nanotechnology* 4(2): 1-7.

76. Kołakowska A. 2017. Usefulness of keystroke dynamics features in user authentication and emotion recognition. In: Hippe Z, Kulikowski J, Mroczek T (eds) Human-computer systems interaction. Springer, Cham, pp 42-52. https://doi.org/10.1007/978-3-319-62120-3_4

77. Soni V, Bhatt DP, Yadav NS. 2020. An efficient approach of Neuro-Hash and its comparision with Cryptograhic Hash. 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp 1241-1245. https://doi.org/10.1109/ICRITO48877.2020.9197915