User Authentication Based on Keystroke Dynamics

Sourav Mandal[1], Anwesa Nandy, and Rounak Saha

Department of Computer Science & Engineering, Institute of Engineering and Management (IEM), University of Engineering and Management Kolkata,
[1]souravmandal8737@gmail.com

Abstract. Keystroke dynamics is a new security enhancement approach. It relies on identifying users with respect to their distinct typing patterns. However, while many are still familiar with those traditional password-based systems, they are becoming more vulnerable to different types of attacks, pointing out how these systems are getting out of date. Behavioral biometrics used by keystroke dynamics includes dwell time, flight time, typing speed and some other factors. The reliability of keystroke dynamics for user authentication is evaluated in this study through the use of machine learning algorithms. Using Random Forest algorithm, we achieved excellent accuracy of differentiating users based on their typing behavior, which may be useful for practical applications. Keystroke dynamics presents a low cost, user friendly and innovative option to improve security of accounts. This can bring about a true paradigm shift in authentication systems by spanning multiple devices while enhancing security and additionally resisting attacks.

Keywords: Keystroke Dynamics, User Authentication, Typing Patterns, Machine Learning, Random Forest, Behavioural Biometrics

1 Introduction

Nowadays, user accounts protection is one of the most important challenges to face in the digital environment. A popular technique to use is the passwords, but it is not very efficient when it comes to security. You can begin with phishing, brute force, or even shoulder surfing could be exploited to hack them [1]. That is why, there are spirits that researchers are to improve the ways of user data protection and one of such methods is behavioural biometrics[2] [3]. Keystroke dynamics is the most promising technique among the mentioned techniques. It operates on aspects to do with typing, for example the amount of time a typist spends on a key (dwell time), the amount of time between key presses which is known as flight time and the enter-key press time[4] .From such patterns, one can be able to verify users by their normal typing patterns.The purpose of this research is to analyse to which extent keystroke dynamics can be effective for user authentication[5]. Then, it divides the concepts on which it is based, describing the characteristics that can be extracted from typing behaviour and

the methods applied to examine them[6]. The aim is therefore to identify the advantages and disadvantages of this method. Thus, knowing what does and does not work, we are on the right path to creating more reliable, less complex means of authentication which are vastly superior to conventional passwords[7].

2 Literature Review

User authentication on the basis of keystroke dynamics has attracted much research interest in the recent past because of the claims that it provides a low intrusiveness,low cost and high accuracy way of identifying users[7]. Keystroke dynamics deal with other parameters involving typing including the dwell time, flight time, typing rate and tempo[3]. These patterns are always private to the user and do not change and therefore they are good for user identification[5]. A work presented a review of keystroke dynamics and considered it a promising technique for the identification of biometric systems[7][8], and put forward some problems also, such as the differences of using keystroke dynamics because of the mood, health, and environmental condition of the user. The study also underlined that algorithms for detecting such accounts in the environment should contain high-performance characteristics and be suitable for recognising real users and impostors depending on various parameters[9][10].
The process of keystroke dynamics authentication involves three critical stages: gathering of data, pre-processing and finally figuring out which bin the new data fits into[8]. In data acquisition, typing data is mostly recorded, preferably from a keyboard or another device. Feature selection is aimed at selecting those features, which can be discriminative. We have to select features like dwell time, flight time and errors and other essential patterns[4][7]. Last is the classification where further analysis of features extracted is conducted in an aim of identifying legitimate users from the impostors[10]. Later, it performed a comparative assessment of several anomaly-detection algorithms for keystroke dynamics and pointed to the two main difficulties associated with imbalanced data that might result in biased operation[11]. Realizing this pre-pandemic was crucial in showing that even with the best of intentions, identification callers require solid metric and benchmark structures in order to become properly insured that they are being fairly and accurately authenticated in their place of work[8][11].
Advancement in keystroke dynamics research has dramatically shifted in the past few years majorly due to the contribution of machine learning[12]. Kinds of classifiers that have been used to boost classification accuracy are the Support Vector Machines (SVMs), Decision Trees, Neural Networks (NNs), Deep Learning models[12]. For example, Revett presented a statistical approach for keystroke dynamics based on bioinformatics techniques[13]. Later, experiment with deep learning approaches to show that most sophisticated models could learn minor differences in typing style, enhancing the effectiveness of the authentication system[14]. These findings make it necessary that one chooses appropriate machine learning models based on keystroke data characteristics [13].
Keystroke dynamics can be practiced in two basic modes, namely static and

continuous authentication[9]. Static authentication authenticates the users occasionally like at login while continuous authentication observes typists constantly in a session to ensure they are genuine [15] [2]. Static authentication mechanisms and their threat were studied by Monrose and Rubin who underlined the need to include keystroke dynamics into multi-factor applications [16]. The other is continuous authentication that provides a higher level of security since the user's identity is constantly being verified[17]. A paper provided evidence of such a technique in practice showing that continuous monitoring is useful in identifying session hijacking and any other unauthorized access session [18].
Nevertheless, keystroke dynamics has several problems. Typing, behaviour, and nervousness affect typing naturally; for example, one's emotions, health, or equipment used affect system results. To overcome this problem, showed how normalization can reduce the impact of variability. One drawback is the threat that relates to spoofing attacks when an attacker tries to emulate the typing pattern of a legitimate user. To this they suggest integrating keystroke dynamics with other biometric modalities including voices or fingerprints to act as backup in case the other fails to identify the user appropriately[19].
Keystroke dynamics as a technique of user authentication is also in demand beyond traditional computing contexts. For example, where the use of the keypad for example in smartphones and tablets poses some interesting possibilities and problems for keystroke dynamics[20]. Since typing behaviour is done on small touchscreens, it may not be as efficient as typing on a full keyboard hence requiring new methods of acquiring data and features [21]. An author examined some limitations of using keystroke dynamics on mobile devices, such as; the screen size and the position of the user while typing, as well as the usage of touch screen or soft keyboards. The study also pointed out that there is a need to focus on such characteristics for purposes of designing algorithms that will be able to handle such disparities with high degree of efficiency [21]. Further, studies have been made to define a fusion of keystroke dynamics with other forms of behaviour and physical characteristics, for instance mouse dynamics or touch screen gestures for enhancing the reliability of the authentication systems. Such a multi-modal approach seems to propose certain advantages over keystroke dynamics, for instance, it is vulnerable to the so-called spoofing attacks or variable typing behaviour [22].

3 Methodology

This research uses a methodology that would effectively capture and analyze keystroke dynamics for user authentication. We define it as feature extractor, data preparation and application to machine learning models.

3.1 Key Terminologies and Feature Extraction

Feature extraction of typing behavior reveals individual characteristics of typing behaviours, which is unique. Key features include [23]:

- Hold Time: It measures functionalities of calibration duration while a key is pressed. It mirrors an experience: Younger typists, or those with fewer levels of typing speed, or a combination of the two, have longer hold times than more experienced ones, so that they do not have the same rhythm.
- Keydown-Keydown Time: It does its magic by calculating the next interval between two key presses and showing you how fast you are typing and how all warm. Typists who have longer intervals between inputs and those with shorter ones between inputs are slower typists and faster typists respectively.
- Keyup-Keydown Time: Cycles the number of milliseconds from the release of the 1st key until key down another. Hand-eye coordination though, it's actually deliberation, which is to say typing complex passwords.
- Typing Speed: It runs the time for typing sequences and aggregates it, by counting hold time and keydown-keydown time onto each of them, and how efficient the typing is.
- Error Rate and Corrections: Two aspects of error frequency and correction behavior are analyzed to examine their impacts on user confidence and content familiarity.
- Flight Time: Both variance in finger movement and keyboard familiarity gives time between release of one key and press of the next.
- Pressure Applied: Although this didn't collect these measurements, the modern keyboards can also measure key pressure, providing us with more tells about physiological differences.

3.2 Machine Learning Models

Various supervised learning algorithms were used in this study to classify users based on keystroke dynamics, with a focus on scalability and non linear pattern handling [12].

- Logistic Regression[39]: A linear model with a sigmoid function to predict probabilities is used. It is fast and interpretable, but it lags behind in non-linear data which prevents its use in keystroke dynamics.
- Random Forest [37]: An Ensemble method which is multiple decision trees combining predictions in order to have robust performance. It's got nonlinear interactions, it keeps you from overfitting, and it's got some nice feature importance metrics, so yeah, that's your go to.
- Support Vector Machines (SVM) [35]: SVM provides an effective solution in high dimensional spaces and found non linear decision boundaries using kernel functions. However, it can capture complex patterns well, but it is computationally intensive with a good deal of parameter tuning.
- K-Nearest Neighbors (KNN)[38]: A simple proximity based classifier. It's easy to understand, but computationally expensive for large datasets, and dependent on choices of neighbors and distance metrics.
- Naive Bayes [36]: An assumption of feature independence in a probabilistic model. This simplification enables computationally efficient application for high dimensional data while it worked well for uncorrelated features.

– Gradient Boosting [40]: It is effective for those datasets that have low ratio, or noises, considering weak learners progressively and combining them to minimize errors. But it is computationally intensive and sensitive to parameter tuning.

4 Dataset Preparation

4.1 Data Collection

A custom desktop application used to intercept keystrokes, recording parameters such as keypress rate and duration, was then used to collect the data. Participants typed stereotype phrases to reflect real behavior in genuine samples, while imposter samples included participating actors typing to reflect attack scenarios to increase data realism [24].

4.2 Data Cleaning and Augmentation

– Data Cleaning: The missing values, noise and outliers are removed. To effectively maintain dataset integrity, users with abnormally high errors or patterns were excluded.
– Data Augmentation: To increase dataset diversity and facilitate models to deal with varying and natural typing like fatigue or distraction, we perturb features like keydown, keydown time, and hold time [25].

4.3 Integration and Merging

Different sources of participants and sessions were joined together, shuffled, randomized to avoid temporal bias. To ensure representative training and testing sets, this step was taken .

4.4 Format conversion and Normalization

Min-Max scaling was used to normalize features to normalize all variables onto a common scale, improving model convergence [26]. To fit into machine learning tools, the dataset was converted to CSV format.

4.5 Public Datasets

To supplement in house data, public datasets, such as MEU-Mobile KSD 2016, were incorporated to add in demographic diversity [27].Compared across studies, this approach improved model generalizability and enabled validation.

5 Performance Analysis

5.1 Feature Correlation Analysis

Features with high positive correlations strongly influence the target, while negatively correlated features have an inverse relationship(Fig 1).

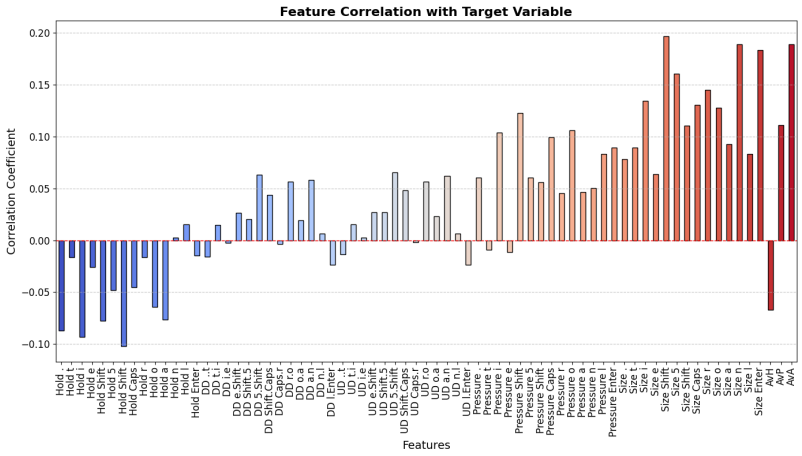

Fig. 1: Correlation of features with the target variable

Features with near-zero correlations have minimal impact and can potentially be excluded, aiding in efficient feature selection for model development.

5.2 Key Observations

Performance analysis evaluates the effectiveness of the chosen machine learning models. The models were tested on multiple metrics: accuracy, precision, recall, and F1 score. The results are summarized in the table below:

Algorithm	Accuracy	Precision	Recall	F1 Score
Random Forest	92.48%	93.29%	92.48%	92.49%
KNN	63.81%	71.22%	63.81%	64.15%
Naive Bayes	69.06%	74.14%	69.06%	69.67%
Gradient Boosting	80.94%	83.96%	80.94%	81.18%

Table 1: Performance metrics of different machine learning algorithms

The key observations are:

1. Using its ensemble approach to model such complex, nonlinear relationships in high dimensional data such as keystroke dynamics [28], Random Forest developed an accuracy of 92.48%. Averaged results reduce overfitting and provide robust to robust and generalized results.
2. Feature engineering was critical to the realization of this solution since metrics such as Hold Time and Keydown Time were very effective in distinguishing the users based on representation of unique, non replicable behavioural traits [29].
3. Model Comparisons:
   - Logistic Regression: It struggled with the nonlinear data.
   - SVM: The nonlinear boundaries were managed at a high computational cost.
   - KNN: It is not so good with a high dimension of data and less sensitive to feature scaling and parameter tuning.
   - Naive Bayes: Poor performance was obtained on interdependent features as in typing rhythm, due to independence assumptions simplification.
   - Gradient Boosting: However, it iteratively reduced classification errors, but was not as robust to noisy data.
4. The data was split into ten folds to train and test, and 10 fold cross validation ensured robust performance. The use of this approach avoided overfitting risk, promoted consistent parameter tuning, and evaluated model generalization for practical use [30].
5. Random Forest's nature of an ensemble, feature importance, scalability and work with high dimensional datasets makes it a good fit for deployment in secure applications such as banking and government services [31]. It has performance and adaptability ensuring that it supports continuous authentication systems.

6 Discussion

This paper shows that keystroke dynamics are feasible, yet fraught, for enabling user authentication, and discusses the performance metrics, feature importance, and practicality for supporting such an application.
User's key unique behaviors including motor skills, typing speed, and hand-eye coordination can be effectively captured by key Hold Time, keydown-keydown Time, and keyup-keydown Time features in order to differentiate users accurately. Behavioral diversity metrics such as Typing Speed and Error Rate add further, however they demand more advanced feature engineering.

- Model Performance: The accuracies achieved by Random Forest (92.48%) were due to the fact that it is capable of handling nonlinear data while reducing overfitting. SVM worked well with nonlinear kernels but took a long time to compute, KNN and Logistic Regression worked poorly. As with Gradient Boosting, we also saw that it was able to perform well, although less robustly to noise [32].

- Limitations: Generalizability is limited by a small dataset size and diversity. Datasets must be expanded to deal with varying demographics, keyboards and multiple languages. It remains challenging to simulate realistic impostor behavior and require advanced techniques. Typing behavior was not addressed for external factors such as device type, environment, and user fatigue.
- Ethical Considerations: Keystroke dynamics are non intrusive and cheap, but they pose privacy concerns as they may accordingly tell on user information. Adding techniques such as homomorphic encryption and differential privacy can mitigate risk [33]. As a way to augment security and usability, keystroke dynamics is added to other biometrics combined in multi factor authentication systems.

7 Conclusion and Future Scope

Despite these challenges, keystroke dynamics holds significant promise as a user authentication method. Its non-intrusive nature, ease of implementation, and potential for continuous user verification make it an attractive option for various applications, including access control, online banking, and mobile device security [33]. Future studies should build enhanced keystroke authentication formats that shield from multiple security threats. The Internet of Things and cloud computing offer many chances for research on keystroke dynamics technology. Building systems that use keystroke dynamics authentication requires careful study of ethical issues and privacy concerns to maintain proper functionality [34].

References

1. Bendovschi, A.: Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance. 28, 24–31 (2015). https://doi.org/10.1016/S2212-5671(15)01077-1
2. Yampolskiy, R.V., Govindaraju, V.: Behavioural biometrics: a survey and classification. International Journal of Biometrics. 1, 81 (2008). https://doi.org/10.1504/ijbm.2008.018665
3. Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafic, T., Camtepe, A., Lohlein, B., Heister, U., Moller, S., Rokach, L., Elovici, Y.: Identity theft, computers and behavioral biometrics. In: 2009 IEEE International Conference on Intelligence and Security Informatics. IEEE (2009).
4. Yilin Li, Baochang Zhang, Yao Cao, Sanqiang Zhao, Yongsheng Gao, Jianzhuang Liu: Study on the BeiHang Keystroke Dynamics Database. In: 2011 International Joint Conference on Biometrics (IJCB). pp. 1–5. IEEE (2011).
5. Zhong, Y., Deng, Y.: Keystroke dynamics for user authentication. Computer Vision and Pattern Recognition Workshops (CVPRW), 2012 IEEE Computer Society Conference on. (2012). https://doi.org/10.1109/CVPRW.2012.6239225
6. Peacock, A., Xian Ke, Wilkerson, M.: Typing patterns: a key to user identification. IEEE Security & Privacy Magazine. 2, 40–47 (2004). https://doi.org/10.1109/msp.2004.89

7. A. Patil, R., L. Renke, A.: Keystroke Dynamics for User Authentication and Identification by using Typing Rhythm. International Journal of Computer Applications. 144, (2016). https://doi.org/10.5120/ijca2016910432
8. admin: Biometrics Solutions. https://www.biometric-solutions.com/, last accessed 2025/01/21.
9. Banerjee, S.P., Woodard, D.: Biometric Authentication and Identification Using Keystroke Dynamics: A Survey. Journal of Pattern Recognition Research. (2012). https://doi.org/10.13176/11.427
10. Teh, P.S., Teoh, A.B.J., Yue, S.: A survey of keystroke dynamics biometrics. TheScientificWorldJournal. 2013, 408280 (2013). https://doi.org/10.1155/2013/408280
11. Killourhy, K.S., Maxion, R.A.: Comparing anomaly-detection algorithms for keystroke dynamics. In: 2009 IEEE/IFIP International Conference on Dependable Systems & Networks. pp. 125–134. IEEE (2009).
12. Sarker, I.H.: Machine Learning: Algorithms, Real-World Applications and Research Directions. SN Computer Science. 2, (2021). https://doi.org/10.1007/s42979-021-00592-x
13. Revett, K.: A Bioinformatics Based Approach to User Authentication via Keystroke Dynamics. International Journal of Control, Automation, and Systems. 7, 7–15 (2009). https://doi.org/10.1007/s12555-009-0102-2
14. Sarker, I.H.: Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions. SN Computer Science. 2, (2021). https://doi.org/10.1007/s42979-021-00815-1
15. Douhou, S., Magnus, J.R.: The reliability of user authentication through keystroke dynamics. Statistica Neerlandica. 63, 432–449 (2009). https://doi.org/10.1111/j.1467-9574.2009.00434.x
16. Monrose, F., d. Rubin, A.: Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems. 16, 351–359 (2000). https://doi.org/10.1016/S0167-739X(99)00059-X
17. Mondal, S., Bours, P.: Continuous Authentication using Behavioural Biometrics. Continuous Authentication using Behavioural Biometrics. (2013). https://doi.org/10.1109/ISBA.2015.7126342
18. Kumar Baitha, A., Smitha Vinod, Prof.: Session Hijacking and Prevention Technique. International Journal of Engineering & Technology. 7, 193 (2018). https://doi.org/10.14419/ijet.v7i2.6.10566
19. Kołakowska, A., Landowska, A.: Keystroke Dynamics Patterns While Writing Positive and Negative Opinions. Sensors. 21, 5963 (2021). https://doi.org/10.3390/s21175963
20. Wang, X., Shi, Y., Zheng, K., Zhang, Y., Hong, W., Cao, S.: User Authentication Method Based on Keystroke Dynamics and Mouse Dynamics with Scene-Irrelated Features in Hybrid Scenes. Sensors. 22, 6627 (2022). https://doi.org/10.3390/s22176627
21. Choi, M., Lee, S., Jo, M., Shin, J.S.: Keystroke Dynamics-Based Authentication Using Unique Keypad. Sensors. 21, 2242 (2021). https://doi.org/10.3390/s21062242
22. Maiorana, E., Kalita, H., Campisi, P.: Mobile keystroke dynamics for biometric recognition: An overview. IET Biometrics. 10, 1–23 (2020). https://doi.org/10.1049/bme2.12003
23. Yaacob, M.N., Idrus, S.Z.S., Ali, W.N.A.W., Mustafa, W.A., Jamlos, M.A., Wahab, M.H.A.: A Review on Feature Extraction in Keystroke Dynamics. Journal of Physics: Conference Series. 1529, 022088 (2020). https://doi.org/10.1088/1742-6596/1529/2/022088

24. Fiske, S.T., Cuddy, A.J.C., Glick, P., Xu, J.: A model of (often mixed) stereotype content: Competence and warmth respectively follow from perceived status and competition. Journal of Personality and Social Psychology. 82, 878–902 (2002). https://doi.org/10.1037//0022-3514.82.6.878
25. Shmuel, A., Glickman, O., Lazebnik, T.: Data Augmentation for Deep Learning Regression Tasks by Machine Learning Models. https://arxiv.org/abs/2501.03654
26. UCI Machine Learning Repository. https://archive.ics.uci.edu/dataset/399
27. Kim, Y.-S., Kim, M.K., Fu, N., Liu, J., Wang, J., Srebric, J.: Investigating the impact of data normalization methods on predicting electricity consumption in a building using different artificial neural network models. Sustainable Cities and Society. 118, 105570 (2025). https://doi.org/10.1016/j.scs.2024.105570
28. Mohammed, A., Kora, R.: A comprehensive review on ensemble deep learning: Opportunities and challenges. Journal of King Saud University - Computer and Information Sciences. 35, 757–774 (2023). https://doi.org/10.1016/j.jksuci.2023.01.014
29. Feature Engineering (FE) Tools and Techniques for Better Classification Performance. International Journal of Innovations in Engineering and Technology. 8, (2017). https://doi.org/10.21172/ijiet.82.024
30. Berrar, D.: Cross-Validation. In: Encyclopedia of Bioinformatics and Computational Biology. pp. 542–545. Elsevier (2019).
31. Wang, H.: Research on the Application of Random Forest-based Feature Selection Algorithm in Data Mining Experiments. International Journal of Advanced Computer Science and Applications. 14, (2023). https://doi.org/10.14569/ijacsa.2023.0141054
32. Thanh Noi, P., Kappas, M.: Comparison of Random Forest, k-Nearest Neighbor, and Support Vector Machine Classifiers for Land Cover Classification Using Sentinel-2 Imagery. Sensors. 18, 18 (2017). https://doi.org/10.3390/s18010018
33. Shadman, R., Wahab, A.A., Manno, M., Lukaszewski, M., Hou, D., Hussain, F.: Keystroke Dynamics: Concepts, Techniques, and Applications. https://arxiv.org/abs/2303.04605
34. Sadikan, S.F.N., Ramli, A.A., Fudzee, M.F.Md.: A survey paper on keystroke dynamics authentication for current applications. In: AIP Conference Proceedings. p. 020010. AIP Publishing (2019).
35. Evgeniou, T., Pontil, M.: Support Vector Machines: Theory and Applications. In: Lecture Notes in Computer Science. pp. 249–257. Springer Berlin Heidelberg, Berlin, Heidelberg (2001).
36. Peretz, O., Koren, M., Koren, O.: Naive Bayes classifier – An ensemble procedure for recall and precision enrichment. Engineering Applications of Artificial Intelligence. 136, 108972 (2024). https://doi.org/10.1016/j.engappai.2024.108972
37. Louppe, G.: Understanding Random Forests: From Theory to Practice. https://arxiv.org/abs/1407.7502
38. Rithesh, R.N.: SVM-KNN: A Novel Approach to Classification Based on SVM and KNN. International Research Journal of Computer Science. 4, (2017). https://doi.org/10.26562/irjcs.2017.aucs10088
39. An Introduction to Logistic Regression Diagnostics. In: Applied Logistic Regression Analysis. pp. 68–91. SAGE Publications, Inc., 2455 Teller Road, Thousand Oaks California 91320 United States of America (2002).
40. Ayyadevara, V.K.: Gradient Boosting Machine. In: Pro Machine Learning Algorithms. pp. 117–134. Apress, Berkeley, CA (2018).