International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

TWO MODEL BIOMETRICS AUTHENTICATION FOR LOCKER SYSTEM

Dr K. Deepa Thilak[1], E. Poonguzhali [2], V. Gowri[3], M. Nivedha[4]

[1]*Associate Professor, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry*
[2]*Assistant Professor, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry*
[3,4]*Student, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry*

Abstract - *Due to the increasing vulnerabilities in cyberspace, password or pin alone is not enough to prevent a breach, it is mandatory to prevent the attacks or to identify the attackers. The covert nature of keystroke dynamics has a high potential for use in cyber intelligence since it cannot be copied by attackers. In the existing system, the keystroke dynamics are used for identification of the authorized users which provides security to avoid breaches. But this will not provide the expected efficiency because the behavior biometrics will be changed due to some external circumstances. In this project, the usefulness of keystroke dynamics establishes person's identity. Since it gives the unique identification of the individual in various external circumstances. To overcome this issue, we use a facial recognition system in this project. We also examined the performance of the identification system when a user, unlike his normal behavior, types with only one hand, and we show that performance then is not optimal, as was to be expected.*

Key Words: **Authentication, Behavior Biometrics, Keystroke Dynamics, Convolutional Neural Network, Biometric Authentication.**

1. INTRODUCTION

Keystroke dynamics, keystroke biometrics, typing dynamics and of late typing biometrics, is that the elaborated temporal arrangement data that describes specifically once every key was ironed and once it absolutely was free as an individual is written at a input device. The behavioral biometric of Keystroke Dynamics uses the way and rhythm within which a private varieties characters on a keyboard or input device. The keystroke rhythms of a user are measured to develop a singular biometric guide of the user's writing pattern for future authentication. Vibration data is also accustomed produce a pattern for future use in each identification and authentication tasks. Normally, all that's preserved once work a writing session is that the sequence of characters akin to the order within which keys were ironed and temporal arrangement data is discarded. For example, "I saw three zebras!"

- The user used the left shift key, or the caps-lock key to form the "i" develops into a capitalized letter "I".
- The letters were all typewritten at constant pace, or if there was a protracted pause before any characters whereas trying to find that key.
- The user typewritten any letters wrong at the start and so went back and corrected them, or if they got them right the primary time.

2. LITERATURE SURVEY

The key grouping [13] has been employed for the obfuscate password. Latency is considered for four conditions like the press to release, press to press, release to release and release to press. The press and releases of the users have been recorded and stored in the database while typing the password in the keypad. They are stored as keys in the hash table by generating hash values. They mainly focus on credential theft in particular. The main aim is to divide the di-graphs into groups for each user separately by applying the clustering algorithm. In this way, the authors obtained almost the same accuracy as if they would use the original di-graphs, but now in a much more efficient way. But this algorithm doesn't work for several users and clustering di-graphs have the possibility of exposing to the attackers.

Keystroke dynamics [14] has been used for finding fraudulent messages in instant messages. In this proposed system, each user generally needs only 20 minutes of training US English keystroke dynamics. This system mainly has two phases, the Enrollment phase, and the Authentication phase. For training keystroke dynamics data has been gathered from each user in the enrollment phase. Approximately 200 words have been trained by each user to generate a unique Predicted Keystroke Dynamics (PKD). After that, some basic information like gender, age, computer-use habits and typically used IM software has been gathered. The proposed Keystroke Dynamics Authentication system will obtain press-release time and release- press time while typing the alphabets. The means and standard deviation of the RPs are available in 26 * 26 matrices. The proposed system has two methodologies like symmetric prediction and cross prediction. The main advantage of this system is that shorter training time, fewer false alarms and recognition accuracy are higher. No data will be recorded when the user enters the non-letter keys like numeric keys or symbol keys.

The double serial adaptation strategy [15] that considers a single capture-based enrollment process has been employed. The typing manners of the users differ by the characteristics of timing pattern and pressure pattern. But these characteristics may change over time due to the acquired

habit of typing the password, the state of mind and activeness of users and the keyboard dissimilarity. In this proposed system, there are four phases, Preprocessing phase, Enrollment phase, Verification phase and Adaptation phase. In preprocessing phase, the temporal information like PP (press-to-press), RR (release-to-release), PR (press-to-release) and RP (release-to-press) are observed and noted. In enrolment phase, single sample has been extracted for reference. In the verification phase, several distance metrics like statistical, Hamming, Euclidean and Manhattan distances are considered and measured. The adaptation phase updates both decision and adaption thresholds. The performance metrics like False Non-Match Rate (FNMR), False Match Rate (FMR), Equal Error Rate (EER), Area under Curve (AUC) and Accuracy are evaluated for the proposed system.

The Behavioral biometrics information [16] like keystroke dynamics and Swipe dynamics are used to provide security in mobile devices. The typing pattern and swiping pattern have been observed from various persons and the system has been trained with those datasets. The spatial features, swipe features, and temporal features have been extracted and classification has been made based upon these features. The various machine learning techniques probabilistic modeling, cluster analysis, Decision tree, Support vector machine, neural network, distance measure and statistical analysis has been analyzed and compared. The accuracies and F1 score comparison has been made based upon the Temporal, spatial and swipe features. In these various algorithms like Naïve Bayes, kNN, CART, SVM, MLP, Logistic regression, and LDA has been used for comparison. Among this LDA provides the best accuracy when compared with other algorithms. This method provides better accuracies with Temporal, Spatial and swipes features.

Eye writer's eye-tracking technology [17] is used because each movement of an individual's eye is unique. The movement of the pupil can be tracked with precise accuracy. They have recorded where the person is looking or how the person's eyes are moving exactly. In order to use eye-tracking to authenticate a person by using the Eye writer, the user must create a rudimentary shape by only using their eyes. The user must glance at the starting point of the shape and then blink to indicate that the point on the screen that is being glanced at, is the starting point that the user wants to select. From this point, the user must draw the shape on the screen within a predefined grid. The moment the shape is complete; the user will blink once again in order to indicate that the process is complete. This approach allows a user to provide authentication. The biometrically recorded data has been checked with some aspects like dwell time, the line starting point. Line deviation, line endpoint , acceleration, and deceleration. But this system was not successful at finding a user if the identity is not in the reference database.

Three uni-modal biometric authentication systems [18] like fingerprint, face and voice signal are compared and analysis has been recorded. These uni-model systems have been separately processed and results are compared. The input for fingerprint has been provided by Thumbprint. Similarly for face webcam is used and a mike recorder is used for voice signals. The performance metrics like FTC, FTE, FAR, GAR, FRR, and EER are measured and compared. Individually, each system processes the given input data and provides authentication. On comparing, the performance of the fingerprint biometric system provides better security and authentication than face and voice biometric system.

The multi-model authentication system [19] is combined with Keystroke Dynamics. The typing rhythm of the individual has been used for analyzing. This XGBoost algorithm is providing higher performance than other compared algorithms. The data set has been collected from users 30 times during 2 sessions with a software keyboard. Various supplementary technologies like Numpy, Scipy, and Pandas have been used for reading and preprocessing the data. Confusion Matrix (CM) and Receiver Operating Characteristic (ROC) curve have been derived using Matplotlib for visualizing the training the curves. In contrast, the change in the behavior of a person may lead to impaired performance.

A framework [20] dedicated to speaker verification to recognize unlock pattern based on the behavior of the user has been adopted. Extra biometric information like the speed of drawing and the pressure of the figure on the touch screen is used for authentication. Statistical models such as Gaussian mixture models with universal background modeling are used in the speaker system. The EM algorithm has been applied to maximize the log-likelihood. The EER performance is analyzed and compared. Since there is no large dataset for unlocking patterns, the experiment is performed with a limited number of users.

The Keystroke Dynamics [22] can be applied in banking sector. The storage and retrieval of user's data has been studied for authentication.

Title & Year	Advantages	Disadvantages
Behavioral Biometrics scheme with keystroke and swipe dynamics for user authentication on mobile platform(2019)	The results obtained by the combinational use of all three features (Temporal features, spatial features, Swipe Features) outperformed those obtained by single set of features.	The overall accuracy and F1 score for the evaluated classifiers are from 78.57% to 89.67% and 75.61% to 88.61%.
Continuous authentication by free-text keystroke based on CNN Plus RNN(2019)	The error rate of this model reaches the lowest level when three keystroke features H+RP+PP (Hold time of the key +Interval between release of the first	When the sequence length is low, the model leads to high error rate and poor recognition and the sequence length increases the noise data in

	key and tap of the second key + Interval between Press of the first key and second key).	the sequence will increase as well as FAR , FRR and EER.
Keyword – based approach for recognizing fraudulent messages by keystroke dynamics (2019)	The VBS classifier is used to predict the PR (Press-Release) and RP(Release-Press) which is efficient than the Statistical Classifier.	In enrolment phase, the legitimate users will be requested to input an article of approximately 200 words thrice as training samples.
Analysis of Authentication system based on Keystroke Dynamics (2019)	The KSD has been chosen to be integrated with other authentication systems because it does not require any additional hardware, needs less effort for an implementation, provides transparent.	The fact that a person may change the behavior over time may lead to an impaired performance by creating a significant challenge in the area.
Recognition of Biometric Unlock Pattern by GMM-UBM(2018)	An average of 14% EER is obtained while relatively higher EER values are due to small number of mixtures unable to sufficiently represent the data.	Since there is no large available common dataset for unlock pattern studies, the experiment is performed with a limited number of users, like almost all the existing studies.

3. DISADVANTAGES

• The biggest disadvantage is the existing system still heavily depends upon the username and password because of the primary passphrase. If this mixture were to be hacked, the individual then ought to bear the complete Enrollment method yet again, with a unique username and secret.

• Password methodology doesn't offer a sturdy identity check. Security is entirely supported by confidentiality and therefore the strength of the password.

• Using the fingerprint scanner doesn't take into thought once someone physically changes in fingerprint authentication.

• Iris scanning life science systems usually need close proximity to the camera, which may cause discomfort for a few.

• The value of element and code programs is expensive.

• Although the potential uses of Keystroke Recognition stay sturdy, it's still not widely deployed in several security applications.

4. DISCUSSION

Conventionally, express authentication strategies like the password is used. However, the system would be broken if the secret is purloined. Therefore, there's a continuous look for ways to strengthen authentication for the locker system. Behavioral biometric data like keystroke dynamics is used for enhancing security. Keystroke dynamics could be a science of learning regarding keystrokes that differentiate every user-supported typewriting speed, latency between keystrokes, and pressure applied on keys, etc. Keystroke dynamics fall into non-static bio-metrics which can vary with time. Non-static bio-metrics depends on many environmental, physical, and biological factors. Authentication is receiving increasing attention. This paper presents summaries of the authentication theme that employs a mixture of secret and keystroke dynamics for locker. Options extracted from the typewriting pattern were evaluated. Accuracy of the system is increased by exploitation combined behavioral life science options, as compared with exploitation solely one set of options.

5. CONCLUSION

The Data breaches as become very challenging due to development in technology. Security measures like password or pin, fingerprint, Iris, etc. have been developed to restrict these breaches yet these measures have some disadvantages in it. From this survey, we have observed that these papers has many advantage, the performance of the system is comparatively low. Behavioral biometrics is the best approach to authenticate the user which cannot be copied by the intruder.

REFERENCES

[1] S. Krishnamoorthy, L. Rueda, S. Saad, & H. Elmiligi, "Identification of User Behavioral Biometrics for Authentication Using Keystroke Dynamics and Machine Learning," ICBEA, pp. 50-57, 2018.

[2] A. Salem and M. S. Obaidat. (2019). "A novel security scheme for behavioral authentication systems based on keystroke dynamics," in Security and Privacy. e64. 10.1002/spy2.64.

[3] Roh, J. H., Lee, S. H., and Kim, S. (2016). Keystroke dynamics for authentication in smartphone. In 2016 International Conference on Information and Communication Technology Convergence (ICTC), pages 1155–1159.

[4] Roy, U., Sinha, D., and Roy, S. (2017). User authentication: Keystroke dynamics with soft biometric features. In Internet of Things (IoT), pages 123–142. CRC Press.

[5] ShenTeh, P. and NingZhang (2016). A survey on touch dynamics authentication in mobile devices. ScienceDirect, 59(2):210–235.

[6] Zaidan, D., Salem, A., Swidan, A., and Saifan, R. (2017). Factors affecting keystroke dynamics for verification data collecting and analysis. In 2017 8th International Conference on Information Technology (ICIT), pages 392–398.

[7] Stock Sawasdee, Personal Identification through Keystroke Dynamics, Standford University, December 2017.

[8] H. Crawford, E. Ahmadzadeh, S. Clara, H. Crawford, R. Ohanian, Authentication on the go: assessing the effect of movement on mobile device keystroke dynamics, in Thirteenth Symposium on Usable Privacy and Security (2017), pp. 163–173

[9] B.S. Saini, N. Kaur, K.S. Bhatia, Keystroke dynamics based user authentication using numeric keypad, in 7th International Conference on Cloud Computing, Data Science and Engineering (IEEE, 2017), pp. 25–29

[10]R. Young, S. Randall, L. Jeffrey and P. Isaac, "Keystroke Dynamics: Establishing Keyprints to Verify Users in Online Courses." Computers in the Schools, vol. 20, no. 1, pp. 48-68, (2019)

[11] Ali, Md Liakat, Monaco, John V., Tappert, Charles C., and Qiu, Meikang. "Keystroke Biometric Systems for User Authentication". In: Journal of Signal Processing Systems (2016), pp. 1–16.

[12] LEE, H. S., LAU, T. S., LAI, W. K., KING, Y. C., and LIM, L. L. (2017). User identification of numerical keypad typing patterns with subtractive clustering fuzzy inference. 2017 IEEE 15th Student Conference on Research and Development, pages 83–88.

[13] Itay Hazan , Oded Margalit , Lior Rokach (2020). Keystroke dynamics obfuscation using key grouping in ELSEVIER.

[14] Cheng-Jung Tsai , Po-Hao Huang (2019). Keyword-based approach for recognizing fraudulent messages by keystroke dynamics in ELSEVIER.

[15] Abir Mhenni , Estelle Cherrier , Christophe Rosenberger , Najoua Essoukri Ben Amara (2019). Double serial adaptation mechanism for keystroke dynamics authentication based on a single password in ELSEVIER.

[16] Ka-Wing Tse, Kevin Hung(2019) Behavioral Biometrics Scheme with Keystroke and Swipe Dynamics for User Authentication on Mobile Platform in IEEE.

[17] Bobby L. Tait(2019) Behavioural biometrics authentication tested using EyeWriter technology in IEEE.

[18] Balaka Ramesh Naidu, K.V.L Bhavani, Ch Someswara Rao and P.V.G.D Prasad Reddy. Comparative Analysis of Three Single Trait Biometric Authentication Models in International Conference on Communication and Signal Processing, April 4-6, 2019.

[19] Amanzhol Daribay, Mohammad S. Obaidat, Fellow of IEEE, and P. Venkata Krishna(2019) Analysis of Authentication System Based on Keystroke Dynamics in IEEE.

[20] M. Erdal zbek, Mohamed Amine Haytom, Estelle Cherrier Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France(2018) Recognition of Biometric Unlock Pattern by GMM-UBM in IEEE.

[21] Tsimperidis I, Arampatzis A, Karakos A, Keystroke dynamics features for gender recognition, *Digital Investigation* (2018), doi: 10.1016/j.diin.2018.01.018.

[22] Poonguzhali. E, Sasikala.P, Suganya.S, Vishnupriya.S, Visual Role Mining for Banking Sector (2013)