ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

A Survey on Authority Identification Using Keystroke

Shreenand Sadanand Tamhankar[1] , Sanket Gulabrao Jambhulkar[1], Aniket Nuria Rathod[1] , Prajakta Anant Shelar [1], Aniket Gautam Gaikwad[2]

Department of Computer, Zeal College of Engineering and Research, Pune, Maharashtra, India

ABSTRACT: This paper worked of choosing a correct input for performing keystroke Dynamics authentication.The pulse dynamics is the study to identify / authenticate a person based on their typing rhythms, which are inferred from key press events such as key press and key release. A great amount of research work has been done in this field where researchers have used only alphabetic or alphanumeric or only numerical entries. In this document we address the question. In this system we will work on alphabetic character with entering sentences that are generated by system and get the speed by keystroke dynamics.If user is performing typing speed according to his stored speed that he will access the system or his account.Proposed system will work for user authentication for his data.

KEYWORDS: Featureextraction,keystroke dynamic, Random Number.

I.INTRODUCTION

Keystroke authentication can be classified as either static or continuous. The first refers to keystroke analysis performed only at specific times, for example during a loginprocess, while the analysis of the typing rhythm is performed continuously during a whole session when the latter is applied, thus providing a tool to also detect user substitutionafter a successful login. The effectiveness of keystroke dynamics as an authentication characteristic for traditional computer keyboards has been deeply investigated. In modern times all the information is stored and shared using computers or mobile devices. With increased use of mobile devices the risk of theft of sensitive data has also increased. To protect data we use password but these passwords can be easily cracked by the hackers. For better security, measures like finger scan, retina scan etc. are used which are a form of physical biometric. But these measures are very costly to implement. Keystroke dynamics is a behavioral biometric method which identifies the user on the basis of his/her typing pattern . This system works by extracting features from the collected data. Then a classifier is used to build up the user profile. The same process is repeated while testing and if the profile matches the one in the databaseThe user is authenticated otherwise not. The deployment of keystroke dynamics for authentication does not include any extra cost as you just require a keyboard for typing which is an integral part of computer system. There are two types of authentication in keystroke dynamics: fixed text and free text. In fixed text the input text is predefined and the user has totype the same text during enrolment and authentication time. In free text the user is free to type any text according to his liking during enrolment and authentication time, thus eliminating the need to remember passwords.

II.EXISTING SYSTEM

The vast majority of currently available mobile devices still uses weak authentication mechanisms based on passwords or PINs, which do not ensure an appropriate security level for the access to the stored information and to the available services. It is worth pointing out that the need of guaranteeing secure data access represents an issue of paramount importance especially when dealing with mobile devices, which may be easily lost or stolen because of their small sizes, and which are often lent to other people, being thus exposed to possible surreptitious uses .In order to improve the security of mobile devices, the use of biometrics [2] has been recently proposed as automatic recognition

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

strategy. A biometric based recognition system relies on the use of attributes derived from physiological (fingerprint, face, iris, etc.) or behavioral (voice, signature, etc.) characteristics of the user himself to perform recognition. Therefore such data are much more difficult to be forgotten, lost, stolen, copied or forged than traditional identifiers likePINs or tokens.

III. REVIEW OF LITERATURE

[1]This paper introduces a novel approach for free-text keystroke dynamics authentication which incorporates the use of the keyboard's key-layout. The method extracts timing features from specific key-pairs. The Euclidean distance is then utilized to find the level of similarity between a user's profile data and his/her test data. The results obtained from this method are reasonable for free-text authentication while maintaining the maximum level of user relaxation. Moreover, it has been proven in this study that flight time yields better authentication results when compared with dwell time[1].

[2] This paper provide a basic background of the psychological basis behind the use of keystroke dynamics. We also discuss the data acquisition methods, approaches and the performance of the methods used by researchers on standard computer keyboards also find use and acceptance of this biometric could be increased by development of standardized databases, assignment of nomenclature for features, development of common data interchange formats, establishment of protocols for evaluating methods, and resolution of privacy issues[2].

[3] This works on 28 users typed the same 10-digit number, using only the right-hand index finger. Employing statistical machine-learning techniques (random forest), we achieved an un weighted correct-detection rate of 99.97% with a corresponding false-alarm rate of 1.51%, using practiced 2- of-3 encore typing with outlier handling. This level of accuracy approaches sufficiency for two-factor authentication for passwords or PIN numbers[3].

[4] This papre presents the study to develop and evaluate techniques to authenticate valid users, using the keystroke dynamics of a user's PIN number entry on a numerical keypad, with force sensing resistors. Added with two conventional parameter lists of elements, i.e. digraph latency times and key hold times, keying force was chosen as a third element. Two experiments were conducted. The first experiment was to evaluate whether the three types of elements derived from keystrokes have a significant effect for subjects and to examine how trials and session effects generated the variation of the three elements. The second experiment was to demonstrate the system performance by calculating the False Rejection Rate (FRR) and the False Acceptance Rate (FAR) of the system[4].

[5] The ability of third generation telephones to store sensitive information, such as financial records, digital certificates and company records, makes them desirable targets for impostors. This paper details the feasibility of a non-intrusive subscriber authentication technique – the use of keystroke dynamics. This feasibility study comprises a number of investigations into the ability of neural networks to authenticate users successfully based on their interactions with a mobile phone keypad[5].

[6] Now days mobile handsets have found an important place in modern society, with hundreds of millions currently in use. The majority of these devices use inherently weak authentication mechanisms, based upon passwords and PINs. This paper presents a feasibility study into a biometric-based technique, known as keystroke analysis – which authenticates the user based upon their typing characteristic. In particular, this paper identifies two typical handset interactions, entering telephone numbers and typing text messages, and seeks to authenticate the user during their normal handset interaction[6].

[7]propose several ways to improve the quality. But, first we define the quality of patterns in terms of two factors: uniqueness and consistency. Finally, the results of a preliminary experiment are presented that support the utility of the proposed methods[7].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

IV. SYSTEM ARCHITECTURE

PROPOSED SYSTEM ARCHITECTURE-

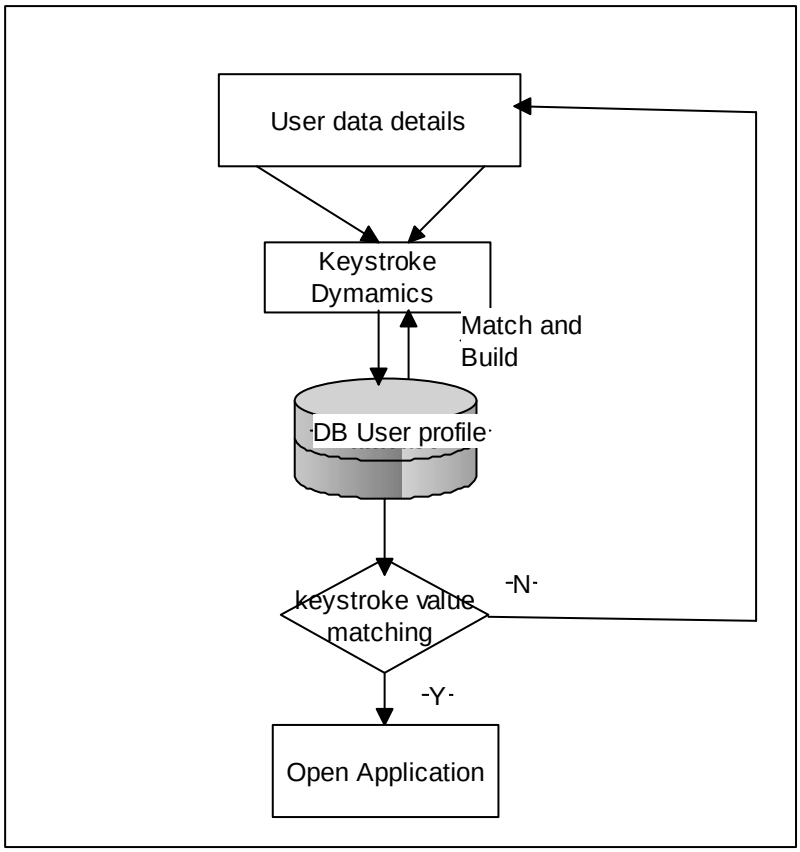

Fig.1: System architecture

V. SYSTEM OVERVIEW

Propose the system with the text input method. The proposed system will generate group of sentence at least four or five times and user have to type this at the time of registration. The system will extract feature and perform keystroke dynamic and save keystroke value .Then while at the time of login ,user will also get three sentences and the system will calculate keystroke value accordingly by keystroke dynamic if that keystroke value is matched with user already stored keystroke value then he will successfully login to system and gets access to handle his account. Here This system works by extracting features from the collected data. Then a classifier is used to build up the user profile. The same process is repeated while testing and if the profile matches the one in the database The user is authenticated otherwise not.

VI. CONCLUSION

In this paper, System worked on choosing a correct input for performing keystroke Dynamics authentication. The system will work on randomly generated sentences that are easy to calculate user's keystroke value. This system

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

works by extracting features from the collected data. The combination of hold time and latency gave the best results.On data collection feature extractionwas performed. Proposed system increase security of user's data

REFERENCES

[1] A. Alsultan and K. Warwick, "User-Friendly Free-Text Keystroke Dynamics Authentication for Practical Applications," in 2013 IEEE International Conference on Systems, Man, and Cybernetics, 2013, pp. 4658–4663.
[2] S. P. Banerjee and D. Woodard, "Biometric Authentication and Identification Using Keystroke Dynamics: A Survey," *Journal of PatternRecognition Research*, vol. 7, no. 1, pp. 116–139, 2012.
[3] R. A. Maxion and K. S. Killourhy, "Keystroke Biometrics with Number- Pad Input," in IEEE/IFIP International Conference on Dependable Systems & Networks(DSN), 2010, pp. 201–210.
[4] K. Kotani and K. Horii, "Evaluation on a keystroke authentication system by keying force incorporated with temporal characteristics ofkeystroke dynamics," *Behaviour and Information Technology*, vol. 24, no. 4, pp. 289–302, 2005.
[5] N. L. Clarke, S. M. F. B. M. Lines, and P. L. Reynolds, "Keystroke Dynamics on a Mobile Handset : A Feasibility Study," *InformationManagement and Computer Security*, vol. 11, no. 4, pp. 161–166, 2003.
[6] N. L. Clarke and S. M. Furnell, "Authenticating mobile phone users using keystroke analysis," International Journal of Information Security, vol. 6, no. 1, pp. 1–14, 2007.
[7]Sungzoon Cho, Seongseob Hwang Artificial Rhythms and Cues for Keystroke Dynamics based Authentication.january 2006
[8] M. Trojahn, F. Arndt, and F. Ortmeier, "Authentication with Keystroke
Dynamics on Touchscreen Keypads-Effect of different N-Graph Combinations,"
MOBILITY 2013 : The Third International Conference on Mobile Services, Resources, and Users Authentication, pp. 114–119,2013.
[9] A. Buchoux and N. L. Clarke, "Deployment of keystroke analysis on a Smartphone," in *Proceedings of 6th Australian Information Security Management Conference*, 2008, pp. 29–39.
[10] K. S. Balagani, V. V. Phoha, A. Ray, and S. Phoha, "On the discriminability
of keystroke feature vectors used in fixed text keystroke authentication," *Pattern Recognition Letters*, vol. 32, no. 7, pp. 1070–1080, 2011.