Person Identification Using Keystroke Dynamics

Parth Sagar, Sneha Patil, Yogesh Dangat,Pooja Athalye, Shubham beldare
[1,2,3,4]Computer Department, RMD Engineering college, warje Pune, Country - India - 411058.

Abstract :Many authentication systems are being used. Authentication systems like password, pattern, biometric etc. are used. But this system has some drawbacks. Password can be easy to guess if it is small or user has written somewhere. Pattern can be guessed using shoulder surfing. Biometric system is more secured than password and pattern. But it is more threating to user physically as in some cases like which happened in Bangkok where a user's thumb was chopped off for getting his fingerprint for unlocking his car. Because of this we are going to use a known biometric system which is least used i.e. keystroke dynamics. In this the users keystroke are used for authentication. In this paper we are going to use the keystroke dynamics for person identification. We are going to use the three schemes for identifying the person who is typing. For this we are going to use the various machine learning algorithm with pairwise user coupling technique. We are going to show the performance separately as well as together. We are going to prove that user coupling technique in bottom up tree structure shows the best performance in terms of accuracy and time complexity. We are going to validate the technique using keystroke data

Keyword: Key stock Pattern information, Identification Keystroke, Person Identification.

Introduction:

Many authentication systems are being used. Authentication systems like password, pattern, biometric etc. are used. But this system has some drawbacks. Password can be easy to guess if it is small or user has written somewhere. Pattern can be guessed using shoulder surfing. Biometric system is more secured than password and pattern. But it is more threating to user physically as in some cases like which happened in Bangkok where a user's thumb was chopped off for getting his fingerprint for unlocking his car. Because of this we are going to use

a known biometric system which is least used i.e. keystroke dynamics. In this the users keystroke are used for authentication. In this paper we are going to use the keystroke dynamics for person identification. We are going to use the method for identifying the person who is typing. For this we are going to use the various machine learning algorithm with pairwise user coupling technique. We are going to show the performance separately as well as together. We are going to prove that user coupling technique in bottom up tree structure shows the best performance in terms of accuracy and time complexity. We are going to validate the technique using keystroke data.

Problem definition

The Existing system to find the Person identification by using key stock pattern. User enter User name and password first its fetch the key stock and store into dataset. User enter the password system can identified the pattern of the Keystroke but sometime pattern identification problems To create to the system. We have also investigated the optimized feature set for person identification by using keystroke dynamics. And is need to improve the pattern identification for the keystroke dynamics.

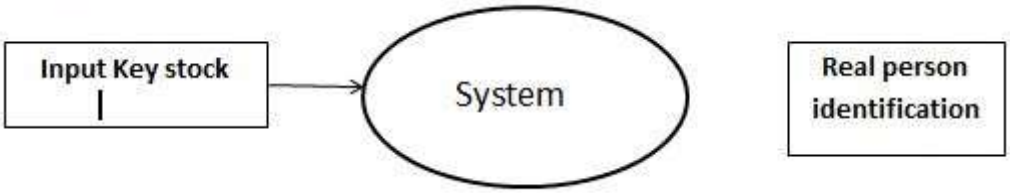
Objectives

To develop a web application providing secure person identification by using keystroke dynamics:

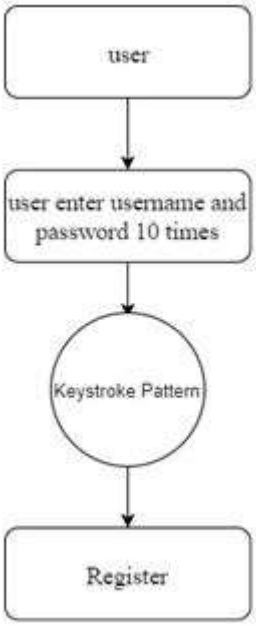
- To providing secure personal identification
- user enter the password system fetch the key stock and create one pattern.
- User match that pattern the enter the system.
- Its secure and valid person assess the system

System design:

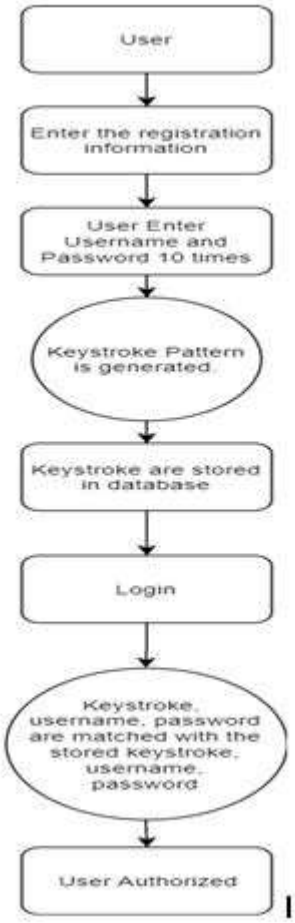
DFD 0



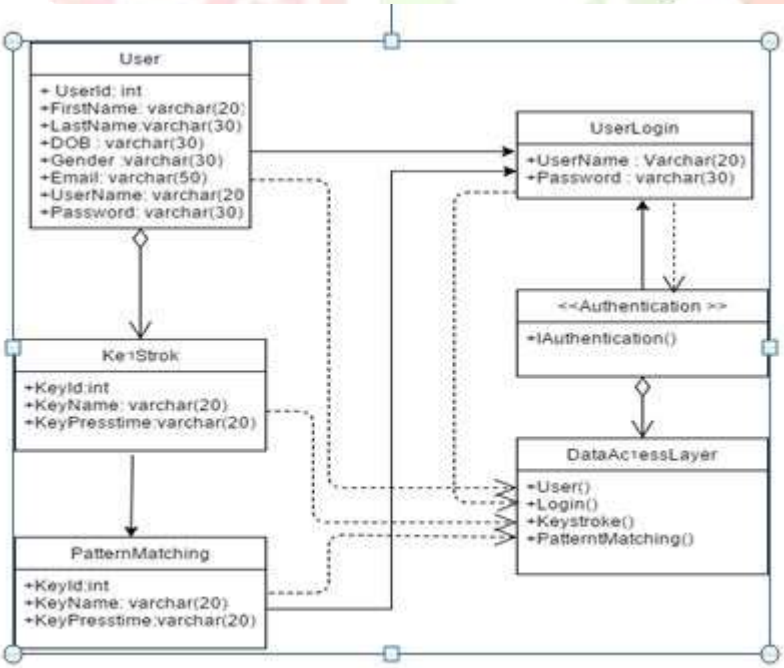
DFD 1



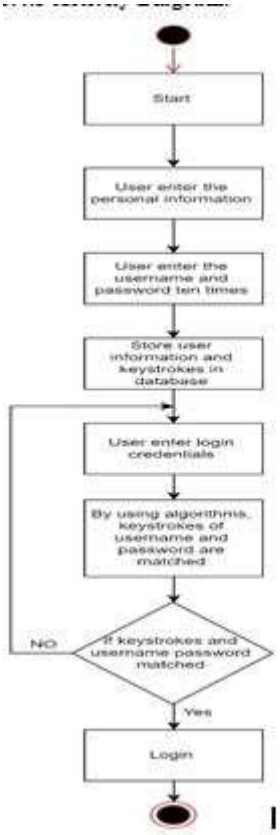
DFD 2



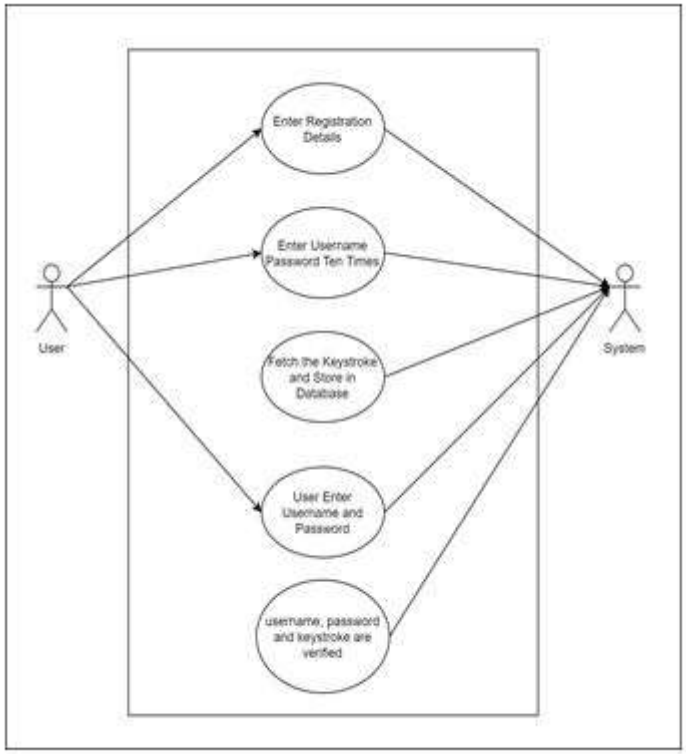
Class digram



Activity Diagram



Use case diagram



Architecture diagram

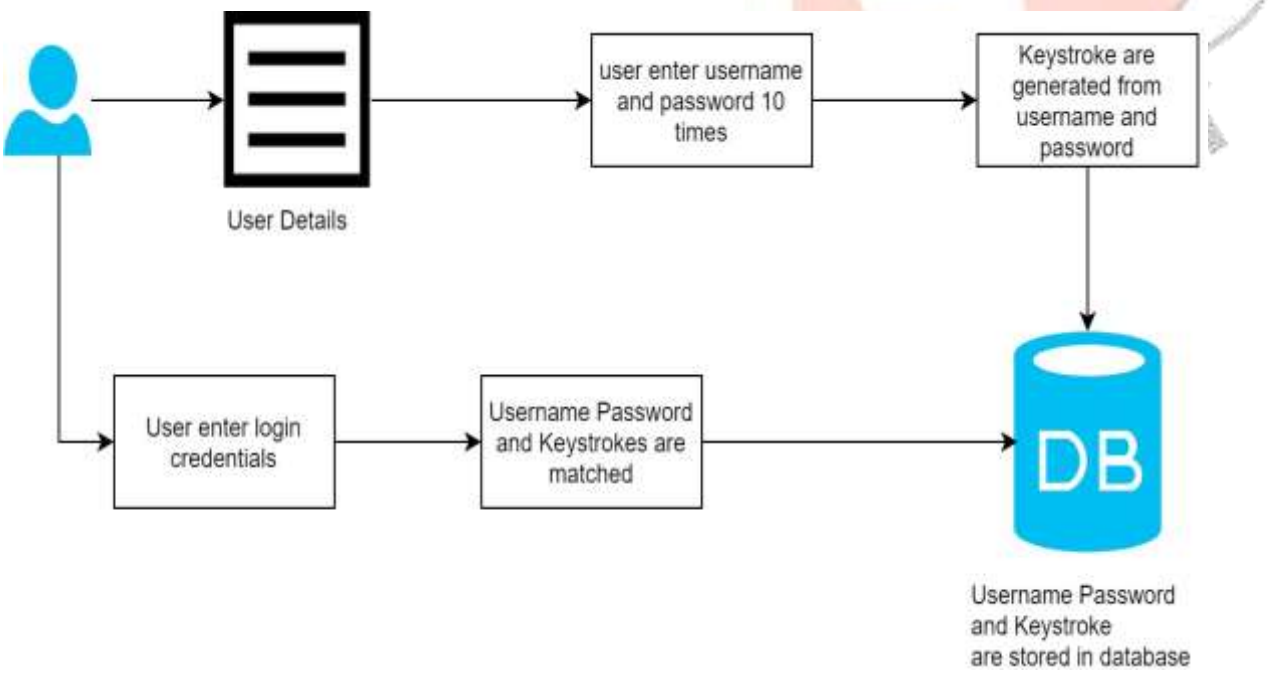


Fig- System Architecture

In this architecture diagram first user has to register with their authenticated mail id and correct information and has to enter the password in 5 step, after this the system will store the info of user and password to the database. And the user will be successfully registered. When the user will login the user has enter the email and password, if the user keystroke password matches then only the user will be successfully login otherwise failed login.

Related work

1. John V. Monaco, Ned Bakelman, Sung-Hyuk Cha, and Charles C. Tappert an application of this work is intruder detection, by which we mean the discovery that somebody other than the authentic user is using the computer. Keystroke biometric systems measure typing characteristics believed to be unique to an individual and difficult to duplicate Continual authentication is ongoing verification but with possibleinterruptions. This is in contrast to continuous authentication which would mean without interruption. We define burst authentication as verification on a short period of computer input after a pause.

2. Mohammad Nauman and Tamleek Ali Traditional approaches to authenticationinvolving 'strong passwords' have several limitations in the context of mobile phones. Miniature keyboards (and in latest devices – on-screen touch keyboards) tend to motivate users to choose simpler, and thus weaker, passwords. A solution to this problem, proposed and implemented on desktop computers since more than two decades back, is keystroke-dynamics analysis [1,2] that usesmore sophisticated parameters, such as duration between each keystroke pressed,alongside password matching to strengthen authentication.

3. KrisztianBuza Although the dynamics of typing, e.g. the time series of the duration ofkeystrokes, is characteristic to users, it is obvious that even the same user cannot always type with the exactly same dynamics. if we consider a large setof users, such as millions of students participating in online education, it may bedifficult and time-consuming for human experts to identify patterns that are ableto reliably distinguishing users from each other. Therefore,

approaches based onmachine learning is required for user identification based on typing patterns

HYPOTHESES

1- In this, we are developing a system to find the Person identification by using key stock pattern. User enter User name and password first its fetch the key stock and store into dataset. User enter the password system can identified the pattern of the Keystroke but sometime pattern identification problems

2- To create to the system. We have also investigated the optimized feature set for person identification by using keystroke dynamics. And is need to improve the pattern identification for the keystroke dynamics.

DELIMITATION OF THE STUDY

1- In this paper we find out the keystroke of password enter by the user and system will find out the authenticated user by their keystroke when they will login to the system.

2- To overcome the problem of security we have developed this concept which will identify the user by analyzing their keystroke.

DESIGN OF THE STUDY

1]**Identification of system:** this paper is developed for the purpose of security, in this identification of the users will be analysing by their keystroke, if keystroke matches then also user will able to login to the system.

Input: User details and password;

Output: identify the user by keystroke.

F1=Naïves bayes (This function helps to predict the users keystroke.),

F2=keystroke capture (it will capture the entered password keystroke)

SAMPLE OF THE STUDY

In this, we are developing a system that helps a user to provide the security to the web application by using concept of keystroke in which the system will analyze the keystroke for the person identification.

TOOLS UDED

S/W System Configuration: -

- Operating System : windows 8 and above..
- Application Server : Tomcat5.0/6.X
- Language : Java
- Front End : HTML, JSP
- Database : MySQL
-

H/W System Configuration: -

- Processor - Pentium –III
- RAM - 2GB (min)

Hard Disk - 20 GB

STATISTICAL TECHNIQUE USED

We have developed Registration page in the system in which user has to enter the details and password. In this user has to enter the password in 5 step in each user‘s password are captured and stored in database and also its information is stored in database. We have used database as MySQL. after 5 step of password system will provide a OTP which is generated automatically and send to registered User’s mail, and that OTP should be enter by the user to the system then only User will be Successfully Register otherwise Registration will be failed. When user will login with their email and password, the system will analyse the keystroke of your password, if it match then the system will identify the person and successfully login.

ALGORITHM

Naïve bayes:

We have used naïve Bayes algorithm for the prediction of keystroke and analysing the user by their keystroke.

Comparative result:

1. **Keystroke dynamics as a biometric for authentication**: This paper address the practical importance of using keystroke dynamics as a biometric for authenticating access to workstations. Keystroke dynamics is the process of analysing the way users type by monitoring keyboard inputs and authenticating them based on habitual patterns in their typing rhythm. And also the inherent limitations that arise with the use of keystroke dynamics as an authentication mechanism are attributed to the nature of the reference "signature" and its relationship to the user — recognizing users based on habitual rhythm in their typing pattern uses dynamic performance features that depend upon an act — the rhythm is a function of the user and the environment.

2. **Biometric Authentication and Identification using Keystroke Dynamics**: A **Survey**:: In this survey, they presented an extensive survey of research conducted in the field of keystroke dynamics over the past three decades. However, there are a few challenges and open areas of research that should be addressed in order to make this an effective biometric. Keystroke dynamics has a strong psychological basis which should be explored to gain deeper understanding of the motor behavior during typing. Using these concepts, models could be built to better understand the processes involved in typing.

3. **Keystroke Biometric Identification and Authentication on Long-Text Input**: The results indicate that the keystroke biometric can be useful for identification and authentication applications if sufficient enrollment samples are available and if the same type of keyboard is used to produce both the enrollment and the questioned samples. The keystroke biometric was significantly weaker for the identification application (but not the authentication application) when enrollment and testing use different input modes (copy or free-text), different keyboard types (desktop or laptop), or both different input modes and different keyboard types. Additional findings include the degree of performance degradation as the number of subjects increases and as the time interval between enrollment and testing increases.

4. **Data Classification for achieving Security in cloud computing:** In this Many classification techniques are have used that classifies the data in social network or other application area. They have identified a set of parameters for data classification in cloud. It is for providing security levels based on type of content and accessibility. We are providing the level of security in cloud storage as per the required confidentiality and access restrictions for the data specified. We have analyzed few data elements and classified

them based on the proposed parameters. All the elements that are stored in cloud storage can be classified first based on the content and access control parameters.

Comparison of existing paper with previous paper:

From previous literature, it recognize that certain features tend to provide more useful than others system. some paper have also work on security like biometric authentication in which there were some limitation that arise such as typists break text in small predictable groups, or due to the limitations on memory buffer size, a static typing biometrics in user authentication. The inputs are the key down and up times and the key ASCII codes captured while the user is typing a string. Some System uses more sophisticated classification techniques such as Support Vector Machines (SVM) might be explored. Also, although it is likely difficult to mimic another person's keystroke pattern. Or some previous paper uses the classier that does not give the accurate result to the system, therefore we try to increase the accuracy of identify the keystroke by using naïve Bayes classier which will give the best output to the system and also provide the OTP function so that only authenticate user will be registered and also check whether the email address that provide does really exist or not.

Experiment Result:

Results demonstrate that the user register is successfully only when user enters the correct information and 5 step password process in which the user's keystroke are stored and an otp code is send to authenticated user, if the user enter the correct OTP then only the user will be successful register and users details are been successful stored in the database. And while login user has to enter the correct email and password keystroke, our system analyses the keystroke and identify the user and successfully the user will able to access the account .

Future scope:

The experiment results show how our system will help to provide the security to the system, it will help the authenticate user to access their access, so that no one can access their account and also it provide the security of OTP which will help the system that the user's email is exist or not.

Conclusion

In this paper, we have used keystroke dynamics for person identification. Our method is more accurate than the other system when it comes to person identification. We have used identification method with pairwise user coupling which show best performance. This system is still secure even when password is compromised. And it will analyse the person by their keystroke and only authenticate user will able to access the account.

Acknowledgment:

It gives us great pleasure in presenting the preliminary project report on '**Person Identification Using Keystroke Dynamics** '.

I would like to take this opportunity to thank my internal guide Prof. Parth Sagar, giving me all the help and guidance I needed I am really grateful to them for their kind support. Their valuable suggestions were very helpful.

I am also grateful to Prof. Vina Lomte, Head of Computer Engineering Department, RMD engineering college for his indispensable support and suggestions.

In the end our special thanks to Prof Parth Sagar, for providing various resources such as laboratory with all needed software platforms,

Sneha Patil

Yogesh Dangat

Pooja Athalye

Shubham Beldare

(B.E. Computer Engineering).

Reference:

1. S. P. Banerjee and D. L. Woodard, "Biometric authentication and identification using keystroke dynamics: A survey," Journal of Pattern Recognition Research, vol. 7, pp. 116–139, 2012.

https://pdfs.semanticscholar.org/f797/1a4341f968263a1d7d6ea219f3266bc7fcf9.pdf

2. S. Bhatt and T. Santhanam, "Keystroke dynamics for biometric authentication- a survey," in Int. Conf. on Pattern Recognition, Informatics and Mobile Engineering (PRIME'13), 2013, pp. 17–23.
http://www.jprr.org/index.php/jprr/article/view/427

3. M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," Applied Soft Computing, vol. 11, no. 2, pp. 1565 – 1573, 2011
https://www.sciencedirect.com/science/article/pii/S156849461000205X

4. L. Araujo, J. Sucupira, L.H.R., M. Lizarraga, L. Ling, and J. B. T. Yabu-Uti, "User authentication through typing biometrics features," IEEE Trans. on Signal Processing, vol. 53, no. 2, pp. 851–855, 2005.https://link.springer.com/chapter/10.1007/978-3-540-25948-0_94

5. F. Bergadano, D. Gunetti, and C. Picardi, "Identity verification through dynamic keystroke analysis," Intelligent Data Analysis, vol. 7, no. 5, pp. 469–496, 2003.
https://www.sciencedirect.com/science/article/pii/S0020737305801658

6. K. S. Killourhy, "A scientific understanding of keystroke dynamics," Ph.D. dissertation, Carnegie Mellon University, January 2012
https://dl.acm.org/citation.cfm?id=2520254

7. C. C. Tappert, M. Villani, and S.-H. Cha, "Keystroke biometric identification and authentication on long-text input," Behavioral Biometrics for Human Identification: Intelligent Applications, pp. 342–367, 2010.
http://csis.pace.edu/ctappert/it691-08fall/projects/keystroke-bookchap.pdf

8. J. Monaco, G. Perez, C. Tappert, P. Bours, S. Mondal, S. Rajkumar, A. Morales, J. Fierrez, and J. Ortega-Garcia, "One-handed keystroke biometric identification competition," in Int. Conf. on Biometrics (ICB'15), 2015, pp. 58–64.
http://ieeexplore.ieee.org/document/7139076/

9. S. Mondal, "Continuous user authentication and identification: Combination of security & forensics," Ph.D. dissertation, Norwegian University of Science and Technology (NTNU), February 2016.
https://www.sciencedirect.com/science/article/pii/S2214212617304659