IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 7, Issue 5, May 2018

# Keystroke Dynamic Authentication Using Graphical Password

**Prof P. D. Thakare[1], Samiksha Thakur[2]**

Professor, Dept. of Computer Engineering, JCOET, Yavatmal Maharashtra, India[1]

Student, Dept. of Computer Engineering, JCOET, Yavatmal Maharashtra, India[2]

**Abstract**: User authentication is one of the important issues for illegal access, especially to computer systems. Alphanumeric passwords can easily be hijacked later by some malicious user. A possible remedy against such a scenario is to use Keystroke Dynamics. Keystroke Dynamics is biometric used to measure the typing rhythm of the user for user authentication. Normally key logger proposed to record every keystroke made on the machine and offers the attacker the ability to steal large amounts of sensitive information without the permission of the owner of the message.

The main objective of this project is to provide 3 level securities for the operation in banking applications. initially, we are authenticating login id and password. Following user authentication, he will be shown with a graphical password screen which provides the additional security.

**Keywords**: Keystroke Dynamic-based Authentication, Graphical passwords, Cued Click- Points (CCP), checkpoint.

## I. INTRODUCTION

The system aims to develop an Authentication System. This system improves protection and confidentiality of the sensitive data. It observes the features based on permissions and analyses the features by using learning model. Security has been an issue from the inception of computer systems. Secured systems must be used to maintain proposed security. Password Authentication Systems have either been usable and insecure and not usable. Increasing either tends to complicate the other. Today, authentication is the principal method to guarantees information security and the most common and convenient method is password authentication. Traditional alphanumeric passwords are strings of letters and digits, which are easy for all users. Texts created passwords are nothing but the string of characters. For text passwords, peoples always create a password which is easy to remember but these passwords are easy for attackers to break. Due to the inadequacy of human retention, most users incline to choose short or simple passwords which are easy to remember. In main cases, these passwords are easy to guess and vulnerable to attack. Users have many passwords for personal computers, social networks, E-mail, and more. People often forget their passwords. If a password is not used frequently it will be even more susceptible to forgetting. If the password is hard to guess, it is hard to remember. Psychological theories have recognized decompose over time and interference with other information in long-term recollection as necessary reasons for forgetting. Another complex issue is that users have many passwords for computers, network, and e-mails. Detection a complex and long password is difficult. But Studies shows that human brain can better recall images than text. So here we give the graphical authentication method for better security.

## II. RELATED WORK

The approach of typing sample collection by monitoring users during their regular computing activities, without any particular constraints imposed on them. A user profile was determined[1] by calculating the mean and standard deviation of digraph latency and by considering only the digraphs occurring a minimum number of times across the collected typing samples. By collecting and analyzing data for five users.

The analysis of keystroke dynamics with fixed text [2](corresponding to keystroked passwords) examines database quality for keystroke dynamics authentication using two databases: the first KDS database remotely collected by the authors and the second Keystroke Dynamics Benchmark Data Set collected with specialized high precision keyboards.

Authentication methods based on biometrics techniques and efficient user authentication with keystroke dynamics using non-fixed text[5] of various size is explained. A small group of individuals, with data over the Internet using browser-based WWW application and on local machines using dedicated applications. The obtained results can be used for future keystrokes database creation.

The free text analysis of keystrokes that combines monograph and digraph analysis,[6] and uses a neural network to predict missing digraphs based on the relation between the monitored keystrokes is presented. Free text analysis systems, which are based on limited or fixed-text enrolment methods, the enrolment process of the proposed detection system is performed with a completely free text sample.

DOI 10.17148/IJARCCE.2018.7512

The graphical passwords scheme[7] to manage the difficulty level of guessing it along with the biometric authentication scheme by using a username with a graphical password using persuasive cued click points along with biometric authentication using fingernail plate. The scope of the scheme is limited to three fingers and it is used for high-security purpose where it is very important to keep tight security.

## III. PROPOSED SYSTEM

The primary objective of this project is to detect key stroke applications and prevent data loss and sensitive information leakage. At the time of registration user will keystroke dynamic authentication parameters in Database and select images(max 5) which he/she want as credentials at the time of user login and the user will also enter a number of splits. A number of splits will indicate the size of the matrix in which the image is going to divide. Then the user will give check- point for each image i.e. for example for a particular image split is 3 then that image will get divided into a 3x3 matrix and then check point can be a combination of row and column e.g. (1,2),(2,2)etc. Images and the respective checkpoint is get stored in the database. The KDA parameter can be measured by Down-Up (DU) time, Down-Down (DD) time, Up-Down (UD) time, Up-Up (UU) time, Down-Up2 (DU2) time.At the time of logon, the system will compare the keystroke's registered parameters and the log in time keystroke parameter if it matches the Open Graphical Password authentication window.

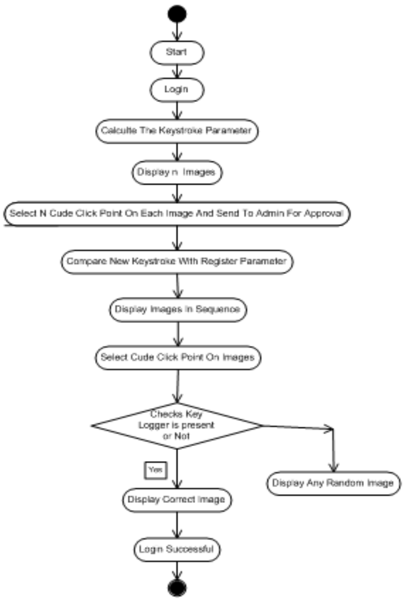

Start
Login
Calculte The Keystroke Parameter
Display n Images
Select N Cude Click Point On Each Image And Send To Admin For Approval
Compare New Keystroke With Register Parameter
Display Images In Sequence
Select Cude Click Point On Images
Checks Key Logger is present or Not
Yes
Display Correct Image
Display Any Random Image
Login Successful

Fig. Workflow of the Proposed System

The user will enter click point (which is given at the time of registration) then the system will check into the database using CCP, if checkpoint for each image matches with checkpoints stored in the database then user login is successful. the figure gives the overall workflow of the proposed system.

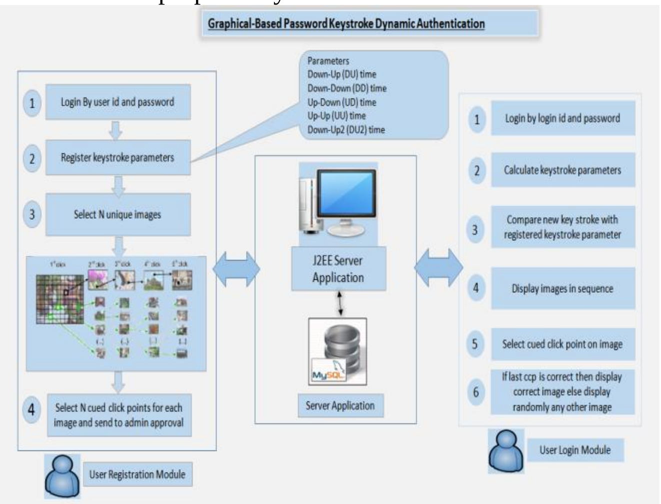

Graphical-Based Password Keystroke Dynamic Authentication
Parameters
Down-Up (DU) time
Down-Down (DD) time
Up-Down (UD) time
Up-Up (UU) time
Down-Up2 (DU2) time
1 Login By user id and password
2 Register keystroke parameters
3 Select N unique images
4 Select N cued click points for each image and send to admin approval
User Registration Module
J2EE Server Application
MySQL
Server Application
1 Login by login id and password
2 Calculate keystroke parameters
3 Compare new key stroke with registered keystroke parameter
4 Display images in sequence
5 Select cued click point on image
6 If last ccp is correct then display correct image else display randomly any other image
User Login Module

Fig. Architecture Diagram

DOI 10.17148/IJARCCE.2018.7512

## IV. PROPOSED ALGORITHM

### 1. Keystroke Dynamics Authentication (KDA):

The behavioural biometric of Keystroke Dynamics uses the way and beat in which an entity types characters on a keyboard or keypad. The keystroke beat of a user is precise to develop a unique biometric pattern of the user's typing pattern for future authentication. Raw sizes available from almost every keyboard can be recorded to find out Dwell time (the time a key pressed) and Flight time (the time between "key up" and the next "key down"). The recorded keystroke timing data is then processed from end to end a unique neural algorithm, which determines a primary pattern for future comparison. Similarly, vibration information may be used to create a pattern for future use in both recognition and verification tasks.

Data needed to analyse keystroke dynamics is obtained by keystroke logging. Normally, all that is retained when logging a typing session is the sequence of characters corresponding to the order in which keys were pressed and timing information is discarded. When reading email, the receiver cannot inform from reading the phrase "I saw 3 zebras!" whether: that was typed quickly or slowly the sender used the left shift key, the right shift key, or the caps-lock key to make the "i" turn into a capitalized letter "I" the letters were all typed at the same pace, or if there was a lengthy pause before the letter "z" or the number "3" while you were looking for that key the sender typed any letters wrong initially and then went back and corrected them, or if they got them right the first time. The help to keystroke dynamics (other behavioral biometrics) is that FRR/FAR can be used to by shifting the receiving threshold at the entity level. This allows for explicitly defined individual risk mitigation–something physical biometric technologies could never accomplish. A touch event includes the on touch down and up, producing five features DU, DD, UD, UU, DU2 defined as follows.

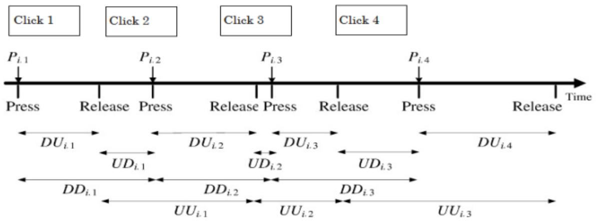


Fig. Time Interval between the Click

**Down-Up (DU) time:** DU time is the interval between the same click being pressed and being released
**Down-Down (DD) time:** DD time is the interval between the click being pressed and the next click being pressed.
**Up-Down (UD) time:** UD time is the interval between the click being released and the next click being pressed.
**Up-Up (UU) time:** UU time is the interval between the click being released and the next click being released.
**Down-Up2 (DU2) time:** DU2 time is the interval between the click being pressed and the next click being released.

### 2. Graphical Authentication Using CCP

Graphical passwords have been planned as alternatives to text passwords to advance both usability and security issues. Text passwords are the most accepted user authentication method, but have security and usability problems. Alternatives such as tokens and biometric systems have their own drawbacks. We propose and study the usability and security of the Cued Click Points (CCP), a recall graphical password method. Users click an image per point for image sequences. The next image is based on the previous click-point. Click-based graphical passwords: A Graphical password system is a knowledge-based authentication that attempts to use graphical password visual information for human memory is available elsewhere. There is a scope of exercise cued- recall Click-based Graphical Password. In such systems, users work as memory cues to help remind images of previously selected locations in one or more pictures and targets.

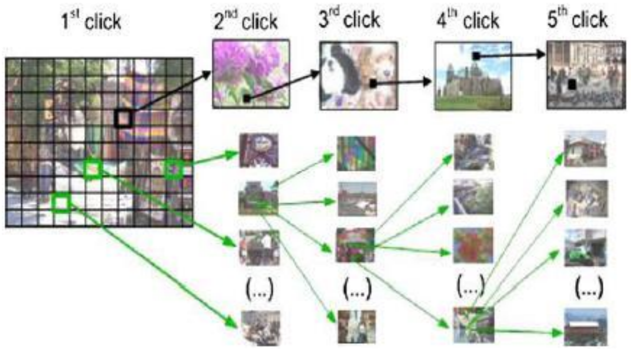


Fig. Cued Click Point

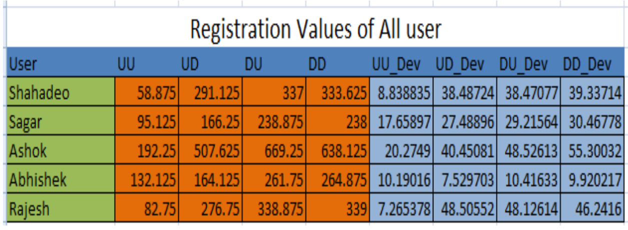
DOI 10.17148/IJARCCE.2018.7512

a) User Registration:
i. User allows selecting N unique images.
ii. Select cued click point on each image.
iii. Store cued click point in database.
b) User Login :
i. Display images in sequence.
ii. Select cued click point on each image.
iii. Check register ccp and new ccp are same or not , if ccp points are same then display next right
iv. image else display image from other images.

## V. EXPERIMENTAL RESULT

The system's GUI was designed using java JSP. The Core Technologies used were Java, JSP. The overall development was done in the Eclipse 3.3 Indigo and for DB we used MY SQL GUI browser. The database basically used for user storing user details like Username & Password. The tool used for db functionalities was MYSQL GUI Browser. At the time of registration, users will keystroke the dynamic authentication parameters in Database. The values are stored in the database with DD,DU, UD,UU,DU2 time. Table 1 gives the time interval between the click of the different users.

Table 1.Registration Values for Different Users



Registration Values of All user

| User | UU | UD | DU | DD | UU_Dev | UD_Dev | DU_Dev | DD_Dev |
|---|---|---|---|---|---|---|---|---|
| Shahadeo | 58.875 | 291.125 | 337 | 333.625 | 8.838835 | 38.48724 | 38.47077 | 39.33714 |
| Sagar | 95.125 | 166.25 | 238.875 | 238 | 17.65897 | 27.48896 | 29.21564 | 30.46778 |
| Ashok | 192.25 | 507.625 | 669.25 | 638.125 | 20.2749 | 40.45081 | 48.52613 | 55.30032 |
| Abhishek | 132.125 | 164.125 | 261.75 | 264.875 | 10.19016 | 7.529703 | 10.41633 | 9.920217 |
| Rajesh | 82.75 | 276.75 | 338.875 | 339 | 7.265378 | 48.50552 | 48.12614 | 46.2416 |

The interval between the clicks is different for each of the users. Graphical format is as shown in below figure.

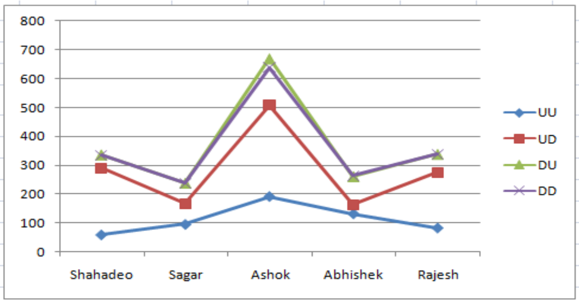
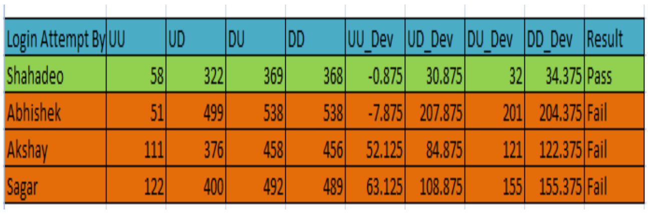


Fig: Plot of Registration Values of All user

If any other user attempted to login with Shahadeo account it failed due to different KDA parameter timing. The user's parameter is not matched with the shahadeo's parameters which are already stored. The different time intervals are shown in the table2.

Table 2. Shahadeo Account attempted by Different Users



| Login Attempt By | UU | UD | DU | DD | UU_Dev | UD_Dev | DU_Dev | DD_Dev | Result |
|---|---|---|---|---|---|---|---|---|---|
| Shahadeo | 58 | 322 | 369 | 368 | -0.875 | 30.875 | 32 | 34.375 | Pass |
| Abhishek | 51 | 499 | 538 | 538 | -7.875 | 207.875 | 201 | 204.375 | Fail |
| Akshay | 111 | 376 | 458 | 456 | 52.125 | 84.875 | 121 | 122.375 | Fail |
| Sagar | 122 | 400 | 492 | 489 | 63.125 | 108.875 | 155 | 155.375 | Fail |

All the user failed to login due to different parameter of KDA. Plots shows the same.

DOI 10.17148/IJARCCE.2018.7512

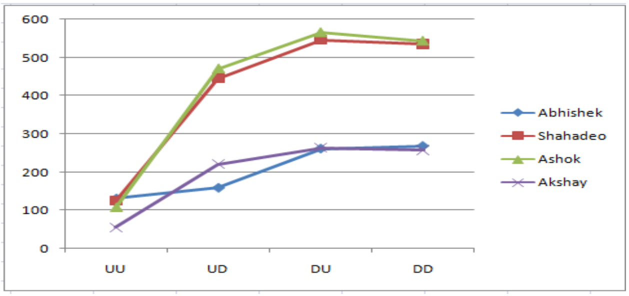
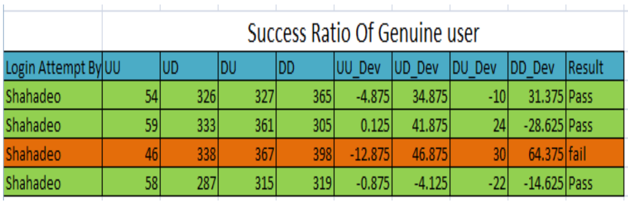


Fig: Login Values of Shahadeo by different user login Attempt

By trying all the attempt it finally gives that none of the other user can login the account without the account holder i.e. he will get the best security for his sensitive data and other important documents.

Table 3. Success Ratio



Success Ratio Of Genuine user

| Login Attempt By | UU | UD | DU | DD | UU_Dev | UD_Dev | DU_Dev | DD_Dev | Result |
|---|---|---|---|---|---|---|---|---|---|
| Shahadeo | 54 | 326 | 327 | 365 | -4.875 | 34.875 | -10 | 31.375 | Pass |
| Shahadeo | 59 | 333 | 361 | 305 | 0.125 | 41.875 | 24 | -28.625 | Pass |
| Shahadeo | 46 | 338 | 367 | 398 | -12.875 | 46.875 | 30 | 64.375 | fail |
| Shahadeo | 58 | 287 | 315 | 319 | -0.875 | -4.125 | -22 | -14.625 | Pass |

All the above discussion shows that the success ratio of proposed system is higher compared to any other technique. Below figure gives the success ration of the given scheme.

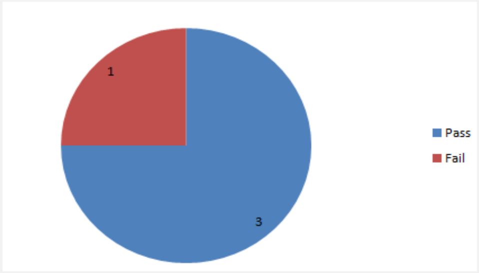


Fig: Success Ratio Of Genuine user

## CONCLUSION

The proposed system is used to provide 3 way securities for the sensitive information by using Keystroke Dynamics Authentication and Graphical Authentication Using CCP. The Graphical passwords have been designed for more secure and that to make passwords more memorable and easy to use by the people. This way we would improve security in banking applications.

## REFERENCES

[1] P. Dowland, S. Furnell, and M. Papadaki, “Keystroke analysis as a method of advanced user authentication and response,” inProc. IFIPTC11 17th Int. Conf. Inform. Security: Visions Persp., May 7–9, 2002,pp. 215–226.

[2] M. Rybnik, M. Tabedzki, and K. Saeed, A keystroke dynamics based system for user identification, Computer Information Systems and Industrial Management Applications CISIM 2008, pp. 225 - 230, 2008.

[3] M. Rybnik, P. Panasiuk, and K. Saeed,User Authentication with Keystroke Dynamics using Fixed Text , International Conference on Biometrics and Kansei Engineering – ICBAKE 2009, pp. 70 - 75, 2009.

[4] M. Rybnik, P. Panasiuk, and K. Saeed “Advances in the Keystroke Dynamics: the Practical Impact of Database Quality”, Lecture Notes in Computer Science (LNCS), Vol. 7564,Computer Information Systems and Industrial Management, Proceedings of 11th IFIP TC 8 International Conference, CISIM 2012, pp. 203-214, Venice, Italy, September 26-28,2012.

[5] Mariusz Rybnik,Marek Tabedzki, Marcin Adamski,Khalid Saeed,"An Exploration of Keystroke Dynamics Authentication using Non-fixed Text of Various Length",2013 International Conference on Biometrics and Kansei Engineering.

[6] Ahmed A. Ahmed and Issa Traore,"Biometric Recognition Based on Free-Text Keystroke Dynamics",IEEE TRANSACTIONS ON CYBERNETICS, VOL. 44, NO. 4, APRIL 2014.

[7] Ushir Kishori Narhar,Ram B. Joshi,"Highly Secure Authentication Scheme",2015 International Conference on Computing Communication Control and Automation.

[8] K. Killourhy and R.A. Maxion. (2009, June29).KeystrokeDynamics - Benchmark Data Set [Online]. Available:http://www.cs.cmu.edu/ keystroke/

[9] K.S. Killourhy and R.A. Maxion,The Effect of Clock Resolution on Keystroke Dynamics. In Proc. of the 11th InternationalSymposium on Recent Advances in Intrusion Detection,(RAID-08), Cambridge, MA, 2008.

DOI 10.17148/IJARCCE.2018.7512