Graphical-Based Password Keystroke Dynamic Authentication System for Android phone

[#1]Miss. Aarti Raman Sonawane, [#2]Prof. H. V. Kumbhar

[#1]ICT Teacher, Kendriya Vidyalay, Nasik, (Computer Engineering, PVPIT, Pune), India

[#2]Assistant Professor, Comp. Engineering , PVPIT, Pune, India

ABSTRACT

Most of the existing authentication system has certain drawbacks for that reason graphical passwords are most preferable authentication system where users click on images to authenticate themselves. An important usability goal of an authentication system is to support users for selecting the better password. User creates memorable password which is easy to guess by an attacker and strong system assigned passwords are difficult to memorize. So researchers of modern days gone through different alternative methods and conclude that graphical passwords are most preferable authentication system. The proposed system combines the existing cued click point technique with the persuasive feature to influence user choice, encouraging user to select more random click point which is difficult to guess.

ARTICLE INFO

Article History

Received: 8th June 2017

Received in revised form :

8th June 2017

Accepted: 10th June 2017

Published online :

17thJune 2017

Keywords - Reauthentication, usable security, Behavioural biometrics, graphical passwords, Smartphone.

I. INTRODUCTION

Keystroke Dynamics is behavioural biometric used to measure the typing rhythm of the user particularly for user authentication, when an individual types on the keyboard. It is assumed as a robust behavioural biometric. The functionality of this biometric is to measure the dwell time and flight time for changing keyboard actions.

The aim of this work is to provide 3 levels in terms of security for transaction in banking applications. First we are making use of encryption for sending user id and password on server from the user's mobile phone. Once the user is authenticated he will be shown with a graphical password screen. Secondly User is shown with sequence of images with 4x4 blocks; user has to select one block from each image. If user enters an incorrect click-point during login, the next image displayed will also be incorrect.

Legitimate users who see an unrecognized image know that they made an error with their previous click point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images. Third, We measure KDA (Keystroke Dynamic-based Authentication) for each images click. This project proposes a new graphical-based password KDA system for touch screen handheld mobile devices. The graphical password enlarges the password space size and promotes the KDA utility in touch screen handheld mobile devices. In addition, this paper explores a pressure feature, which is easy to use in touch screen handheld mobile devices, and applies it in the proposed system. This way we would improve security by using graphical authentication in mobile banking applications.

The most common approach to address this problem is the use of authentication mechanisms, e.g., PIN-based and pattern-based pass codes, which have been integrated into smartphone systems like Android and iOS. Unfortunately, most smartphone users tend to choose simple and weak pass codes for the sake of convenience and memorability, and some recent studies have shown how simple an attacker can derive the PIN pass codes from the oily residues left on the screen or the pattern pass codes from the shoulder surfing attack . An attacker could even infer the pass codes from the accelerometer and gyroscope readings. Therefore, it is highly desirable to enhance smartphone authentication with a passive and transparent authentication mechanism without active user involvement, to further detect whether the logged-in user is the true owner of a smartphone. An ongoing research project, the Active Authentication and Monitoring program initialized by DARPA (Defence Advanced Research Project Agency), aims to develop computational behavioural traits for validating the identity of the users in a meaningful and continual manner (without requiring the deployment of additional hardware sensors), through how users interact with the computing systems.

II. LITERATURE SURVEY

1] "Even or Odd: A Simple Graphical Authentication System" – 2015 – IEEE

Many portable devices need a simple authentication system to protect them from being used by an unauthenticated person such as a thief. The security of traditional methods such as pin codes or passwords is limited by shoulder

surfing where a casual or intentional observer observes an authentication session and derives all information necessary for authentication. Graphical authentication systems have been developed to forestall this attack. We present here an especially simple variant of a graphical authentication system based on the capacity of humans to recognize faces well. In our challenge-response scheme, a user is presented with a row of typically three faces and needs to decide whether the number of "friends" is even or odd. We present here an analysis of security and usability of this scheme.

2] "Highly Secure Authentication Scheme" – 2015

The increased level of effective security control and transaction fraud in the world of electronic and internet commerce, demands for highly secured identification and personal verification systems. The Knowledge based authentication system encourage to user in selecting password for high security. For high security application the proposed scheme presents an integrated evaluation of the graphical password scheme by using persuasive cued click points, including usability and security evaluations, and implementation considerations along with the biometric authentication using finger nail plate surface. It implements the graphical passwords scheme to improvise the difficulty level of guessing it along with the biometric authentication which is very convenient and efficient method by acquiring low resolution images of nail plate surface which is the outermost part of the nail unit.

3] An Anti-Shoulder Surfing Mechanism and its Memorability Test – IEEE-2012.

To improve security of mobile device graphical password towards shoulder surfing attack, an anti-shoulder surfing mechanism called Painting Album Mechanism is suggested. This mechanism is designed based on concept of painting album, and it is consists of three input schemes called Swipe Scheme, Color Scheme, and Scot Scheme. In this paper, use of this mechanism have been verifying with the memorability test. 30 respondents were authenticating with these three input schemes with multiple authentications. Results were showing Painting Album Mechanism is useful since respondents were succeeding in recalling theirs passwords in acceptable period of time.

III. MOTIVATION AND PROBLEM STATEMENT

Motivation

Internet security has become a serious issue for anyone connected to the Internet. To avoid unauthorized people accessing an information system, keystroke dynamics based authentication (KDA) systems combine password knowledge with typing characteristics to enhance the security of general password authentication systems.

Keystroke dynamics or typing dynamics is the process of analyzing the way a user types at a terminal by monitoring the keyboard inputs thousands of times per second, and attempts to identify them based on habitual rhythm patterns in the way they type.

The underlying principle of Biometric-based user authentication focuses on "who you are" which differs from conventional user authentication approach that mainly relies on "what you have" or "what you know." Thus, a biometric-based approach is based on the inherent and unique characteristics of a human user being authenticated. Biometric-based reauthentication approaches have been widely studied for PCs [3]–[14]. However, we can find only few such implementations on smartphones, which are either limited by coarse accuracy or restrict application scenarios or gestures. Therefore, in this section, we focus on the state of the art on smartphones. We first present some smartphone applications that perform the one-time identification and reauthentication. We then highlight some applications that tend to abuse the smartphone resources to observe the user's biometric characteristics, which can be used for various purposes including the attacks.

A. Attacks With User Behaviours on Smartphone: Existing smartphones are equipped with sensors such as GPS, microphone, accelerometer, magnetic field, gravity, temperature, and gyroscope.

B. Behavioral Biometrics-Based Authentication on Smartphone.
   1) One-Time Identification: This method enhances the security of sliding unlock pattern on smartphones by employing the intensity of pressure on touch screen.
   1) Reauthentication: Some other approaches have been proposed [7]–[11] to exploit users' gestures as features for user classification. These approaches cannot provide highly accurate classification and suffer from drawbacks.

IV. PROPOSED SYSTEM

This research work focus on providing better security system by analysing the typing behaviour of individuals using keystroke dynamics. Main emphasis of this is to recognize typing behaviour of the users using FFNN with MLP to achieve more secure system. Keystroke Dynamics is becoming popular in real time security systems. The methods developed so far are less efficient than proposed technique. This paper deals with typing behaviour of individuals using MLP and it also validates the features of users using cross validation in order to give more secure and efficient system than previous system.

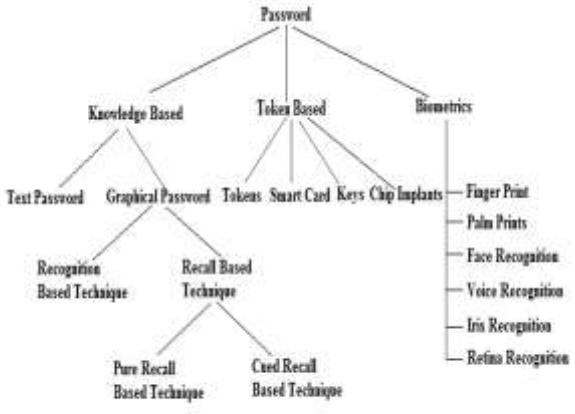


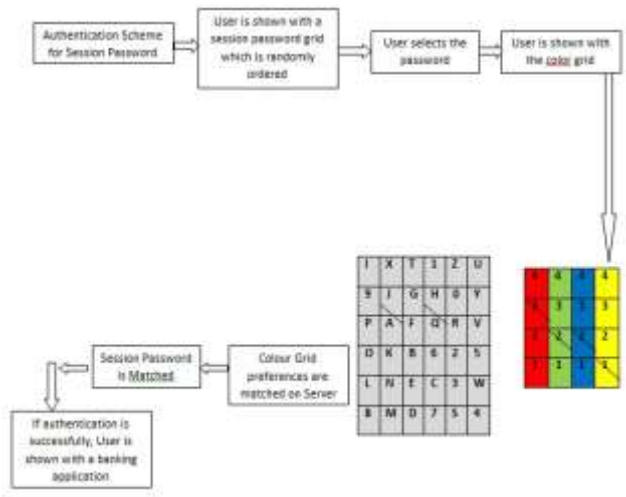
Fig: Classification of Password Authentication Methods

Product features are:

1. Encryption/decryption of data.
2. Graphical Authentication Using Cued Click- Points (CCP).
3. Measuring of KDA Parameters:
    1. Down-Up (DU) time: DU time is the interval between the same click being pressed and being released.
    2. Down-Down (DD) time: DD time is the interval between the click being pressed and the next click being pressed.
    3. Up-Down (UD) time: UD time is the interval between the click being released and the next click being pressed.
    4. Up-Up (UU) time: UU time is the interval between the click being released and the next click being released.
    5. Down-Up2 (DU2) time: DU2 time is the interval between the click being pressed and the next click being released.
4. Authenticating User based on KDA parameter.
5. Internet Banking application Login, fund transfer and balance enquiry.

V. SYSTEM ARCHITECTURE

Keystroke dynamics or typing dynamics is the process of analyzing the way a user types at a terminal by monitoring the keyboard inputs thousands of times per second, and attempts to identify them based on habitual rhythm patterns in the way they type. It is the detailed timing information when each key was pressed and when it was released as a person is typing at a computer keyboard. The behavioral biometric of Keystroke Dynamics is the manner and rhythm in which an individual types characters on a keyboard or keypad. The keystroke rhythms of a user are measured to develop a unique biometric template of the users typing pattern for future authentication. Raw measurements available from every keyboard can be recorded to determine Dwell time (the time a key pressed) and Flight time (the time between "key up" and the next "key down"). Key hold time or dwell time is defined as the time for which each keystroke was pressed. The keystroke latency is the combination of the hold and flight times. In other words, the system verifies how a person types. Keystroke verification techniques can be categorized as either static or continuous.



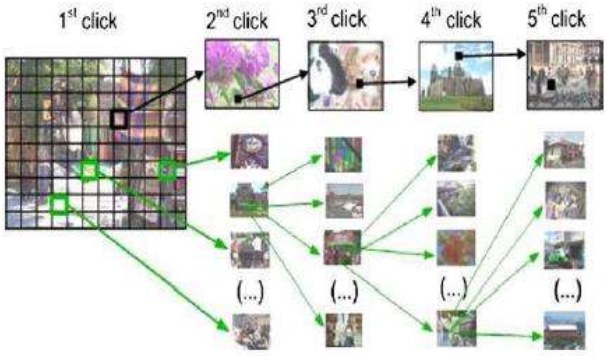


Fig: System Architecture

Static verification system approaches study keystroke characteristics at a specific time. Continuous verification, on the other hand, examines the user's typing behavior throughout the interaction time. Time-features can be extracted from keystroke data in many ways, such as studying keystroke latency, duration of key hold, pressure of keystroke, frequency of word errors, and typing rate. However, not all of these methods are widely used. Keystroke solutions are usually measured in three ways: dwell time – how long a key is pressed, flight time – how long it takes to move from one key to another, and key code. The recorded keystroke timing data is then processed through 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 identification and authentication tasks. Data needed to analyze keystroke dynamics is obtained by keystroke logging.

VI. MATHEMATICAL MODEL AND ALGORITHM

1. Keystroke analysis of clicks over images authentication :

step 1: KEY Stroke Dynamic

DU :- DOWN_UP
UD :- UP_DOWN
UU :- UP_UP
DD :- DOWN_DOWN

Step 2: Calculation for DD,DU,UD,DD
Get list of Values when Click

list a(D1,D2,...)
list b(U1,U2,...)

D1: 1446533079975
D2: 1446533080951
D3: 1446533081466
D4: 1446533082112

U1: 1446533080052
U2: 1446533081028
U3: 1446533081533
U4: 1446533082204

DU : (U1-D1)+(U2-D2)+...and so on / list.size()

UD : (D1-U2)+(D2-U3)+...and so on / (list.size()-1)

DD : (D2-D1)+(D3-D2)+...and so on / (list.size()-1)

UU : (U2-U1)+(U3-U2)+...and so on / (list.size()-1)

Step 2: Calculate Average of DD,DU,UD,DD

Step 3: Calculate Mean for all 4 images

Step 4: Calculate Standard Devition

Step 5: Check current click points

Step 6: subtract with average

Step 7: if result <= S.D
Login Successful
Else
Login Failed

2. AES Algorithm :

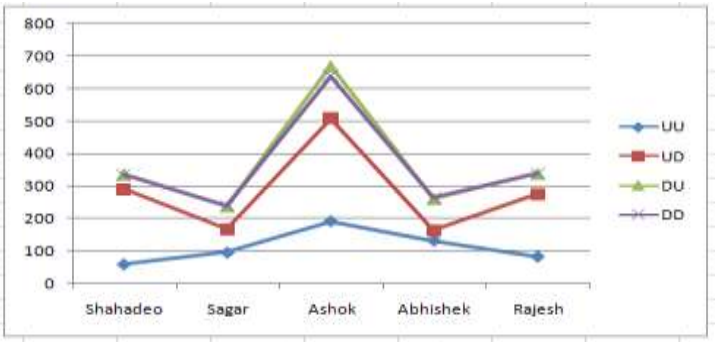
1. Key Expansions:- Round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial Round

Add Round Key:- Each byte of the state is combined with a block of the round key using bitwise xor.

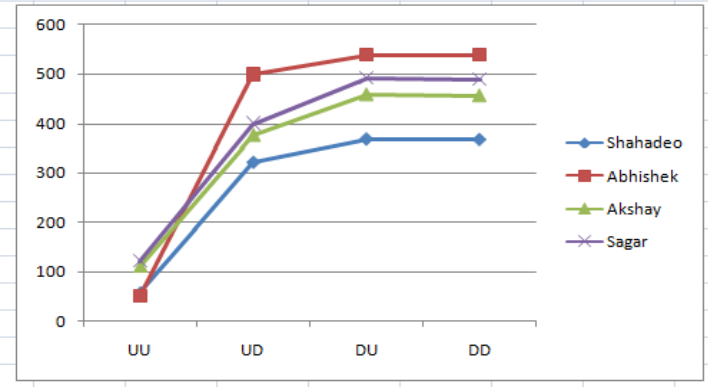
3. Rounds
   1. Sub Bytes: - A non-linear substitution step where each byte is replaced with another accords to a lookup table.
   2. Shift Rows: - A transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
   3. Mix Columns: - A mixing operation which operates on the columns of the state, combining the four bytes in each column.
   4. Add Round Key.
4. Final Round (no Mix Columns)
   1. Sub Bytes
   2. Shift Rows
   3. Add Round Key.

VII. PERFORMANCE RESULT AND ANALYSIS



Registration Values of All user

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



Login Values of Shahadeo by different user login Attempt

Login Values of Shahadeo by different user login Attempt										
User	Login Attempt By	UU	UD	DU	DD	UU_Dev	UD_Dev	DU_Dev	DD_Dev	Result
Shahadeo	Shahadeo	58	322	369	368	-0.875	30.875	32	34.375	Pass
Shahadeo	Abhishek	51	499	538	538	-7.875	207.875	201	204.375	Fail
Shahadeo	Akshay	111	376	458	456	52.125	84.875	121	122.375	Fail
Shahadeo	Sagar	122	480	492	489	63.125	188.875	155	155.375	Fail

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

VIII. CONTRIBUTION

We are using two level of security for authentication purpose which is:

1. Password Based Authentication
2. Keystroke analysis of clicks over images authentication
3. CCP (cued click point) Based authentication

Keystroke statistics of the user instead of password based or image based authentication which is difficult to predict.

Measuring of KDA (Keystroke dynamics attribute) Parameters:

1. Down-Up (DU) time:

   DU time is the interval between the same click being pressed and being free.
2. Down-Down (DD) time:

   DD time is the interval between the click being pressed and the next click being pressed.
3. Up-Down (UD) time:

   UD time is the interval between the click being released and the next click being pressed.
4. Up-Up (UU) time:

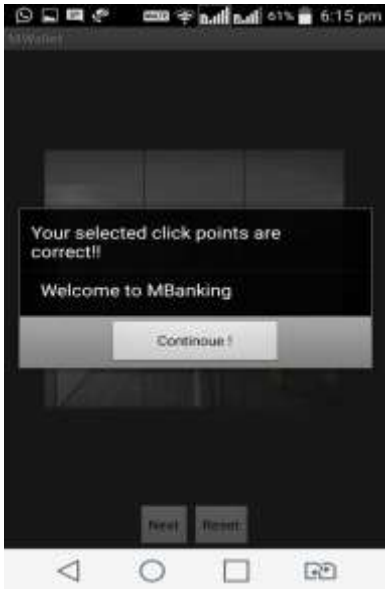
   UU time is the interval between the click being released and the next click being released.
5. Down-Up2 (DU2) time:

   DU2 time is the interval between the click being pressed and the next click being released.

4. Authentication using ccp:

We recommend that CCP be implemented and deployed in systems where offline attacks are not possible, and where any attack will be made against an online system that can limit the number of guesses made per account in a given time period.

IX. RESULTS FINDING



X. CONCLUSION AND FUTURE WORK

For Graphical passwords there is a rising interest is that they are better than the Text based passwords, while the important argument for graphical the proposed system removes the shoulder surfing attack. Also it removes the pattern formation and passwords are that people are better at memorizing graphical passwords than text-based passwords. Also hotspot attack since it provides the system suggestion.

ACKNOWLEDGEMENT

We take this golden opportunity to owe our deep sense of gratitude to our project guide Prof. H. V. Kumbhar, for her instinct help and valuable guidance with a lot of encouragement throughout this paper work, right from selection of topic work up to its completion. Our sincere thanks to Head of the Department of Computer Engineering Dr. B, K. Sarkar who continuously motivated and guided us for completion of this paper. I am also thankful to K. V. NO.1, Nasik staff members, for their valuable suggestions and valuable co-operation for partially completion of this work. We specially thank to those who helped us directly-indirectly in completion of this work successfully.

REFRENCES

[1] A. Tedeschi, B. Noble and F. Benedetto,A cloud-based tool for brand monitoring in social network, University of Roma TRE., Rome: IEEE International Conference on Future Internet of Things and Cloud, 2014.

[2] N. Bekmamedova and G. Shanks ,Social Media Analytics and Business Value : A Theoretical Framework and Case Study, 47th HawaiiInternational Conference on System Science., 2014.

[3] R. Feldman, Techniques and applications for Sentiment Analysis, Communications of the ACM:Vol 56, pp 4, 2013.

[4] K. Nigam, J. Lafferty and A. McCallum,Using Maximum Entropy for Text Classification, Carnegie Mellon University, Pitsburg.

[5] P. Goncalves, F. Benevenuto, M. Araujo and M. Cha, Comparing and combining Sentiment Analysis methods, UFMG, Brazil, COSN, 2013.

[6] J. Natkins, How to analyse Twitter data with Apache Hadoop.

