IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Shoulder Surfing with Honey word

[1]Pavan H. Patil, [2]Dr. Tripti Arjariya

[1]Student, [2]Professor

[1]Department of computer science and Engg.

[1]Bhabha Engineering Research Institute, Bhopal, MP- 4008887

Abstract: When customers add their passwords to a public room, they may risk stealing their password by attackers. By a direct observation or by capturing authentication, an intruder may catch the password. This is called shoulder-surfing and a hazard of specific concern is detected when it is authenticated in public areas. Until recently, the alertness on the user part was the only way to defend against shoulder-surfing. The surfing shoulder-resistant password authentication mechanism promises user-resistant shoulder-surfing authentication. This helps users to authenticate by graphically using their password at unknown places so users never have to click on password icons right away. The nice word function to identify an adversary who wants to log into the network using broken passwords can be described. The combination of existing user passwords known as slutty words is a new password. False password is basically nothing but the sweet words are designed for and username with sweet words, so that even the right password is an exacting feature, and certain people are sweet words. Then a warrant is activated to notify the manager about the password leakage when an opponent is attempting to enter in the system with a honey phrase. Nice term for hash password database attack. attack detection. The real password stored as a sweet word for any user account. For this analysis, the program should analyze the honey word extensively and make a statement on the use of weak points to focus. Reflect on realistic passwords, raising password storage costs, and swap new passwords from existing user passwords.

Index Terms **- Component, formatting, style, styling, insert.**

I. INTRODUCTION

The new graphical password scheme is mainly vulnerable to a proven threat from shoulder surfing, specifically when an attacker would catch a password from a direct view or a demo session. The shoulder-surfing becomes an exacerbated problem in graphic passwords, due to the illustration border. A graphical password is less difficult for most people to keep in mind than a text-based password. Suppose you have to use an 8-character password to access a laptop network. Robust, deviction-resistant, dictionary attack passwords can be created. Essential loggers, cyber engineering and shoulder surfing. There have been two problems to address in this regard: Initial passwords should be secured by proper encryption, and stored with their hash values determined using a salting process, or any other complicated mechanisms. Graphic passwords have been used for web, ATM, and E transaction authentication. It must therefore be difficult for an opponent to invert hashes to obtain passwords in plaintext. Secondly, a secure system must determine whether or not the discovery of a password file is an accident. The study focuses on the above issue and discusses fake passwords or accounts in an simple and cost-

effective way to identify password compromise. Once a user sends a login query, the login server determines the order between the clients and the order of the submitted password. The login server will give the user and his / her smooth word a message of the sort to a secure server called the "honey checker." The sweetheart determines whether the given terms are a password or a sweet word or not. When a honey word is sent, an alarm will rise or a previously chosen action will be taken. The sweet words cannot know anything about the password or the sweet words of the user. It has a single database that only includes the exact password order among the sweet words of the user.

II. PROBLEM STATEMENT

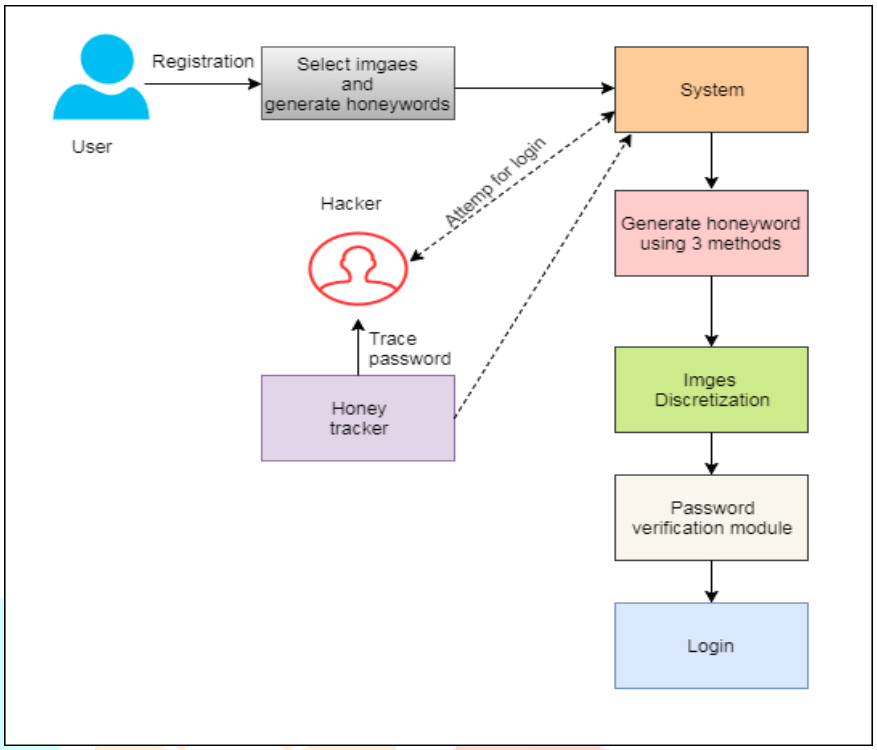
The proposed system presents in this project a safe graphical authentication framework called the Pass Matrix which protects users of windsurfing attacks and uses one-time login indicators to enter passwords in the open. For each photograph, a login indicator is generated randomly and after the session is completed is futile. The login indicator provides enhanced protection against surfing on the arm, as users use a dynamic pointer to display their passwords, instead of clicking directly on the password object. In order to detect password breach, we focus on security and deal with fake passwords or accounts as a simple and affordable way. Honey Pot is one manner in which password vulnerabilities can be detected. The manager actively creates misleading user accounts to draw opponents and senses the disclosure of a password, if any honey-pot passwords are used.

III. LITERATURE SURVEY

Sr. No	Paper Name	Year	Description	Advantages	Disadvantages
1	Multi-touch passwords for mobile device access	2012	Draw-a-Secret password schemes, like the Google Android Pattern Lock, entail stroking out a shape on a touch screen.	to increase password entropy	to utilize the novel functionalities provided
2	The doodb graphical password database: Data analysis and benchmark results	2013	We present DooDB, a doodle database containing data from 100 users captured with a touch screen-enabled mobile device under realistic conditions following a	high intra-user vari- ability in the production of doodles	the analysis of the impact of doodle complexity in the performance against skilled forgeries

			systematic protocol.		
3	Graphical Password-Based User Authentication With Free-Form Doodles	2015	User authentication using simple gestures is now common in portable devices. In this work, authentication with free-form sketches is studied.	High variability between capture sessions increases the error rates.	he GMM system has better performance against skilled forgerie
4	Covert attention shoulder surfing: Human adversaries are more powerful than expected	2013	When a user interacts with a computing system to enter a secret password, shoulder surfing attacks are of great concerne	human performance modeling tool for security analysis and improvement.	secure authentication method based on the abundant evidence
5	The doodb graphical password database: Data analysis and benchmark results	2013	We present DooDB, a doodle database containing data from 100 users captured with a touch screen-enabled mobile device under realistic conditions following a systematic protocol.	performance against forgeries is analyzed using state-of-the-art algorithms	to an improvement in their verification performance which would become closer to pseudo-signatures

IV. SYSTEM ARCHITECTURE

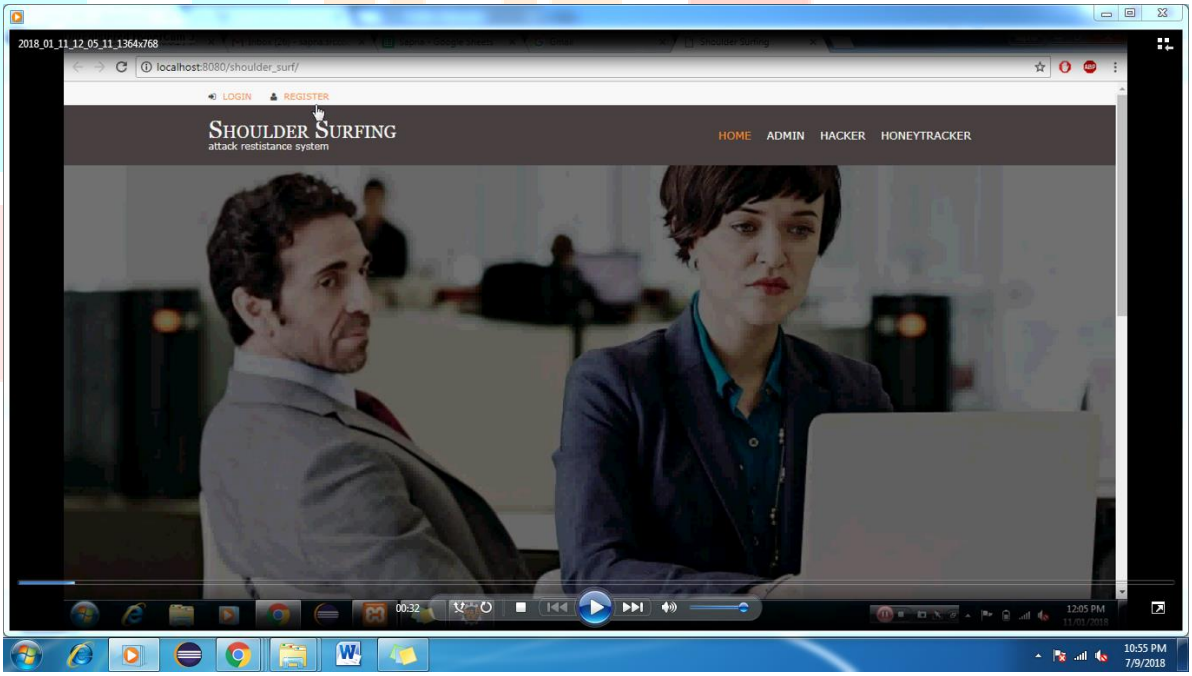


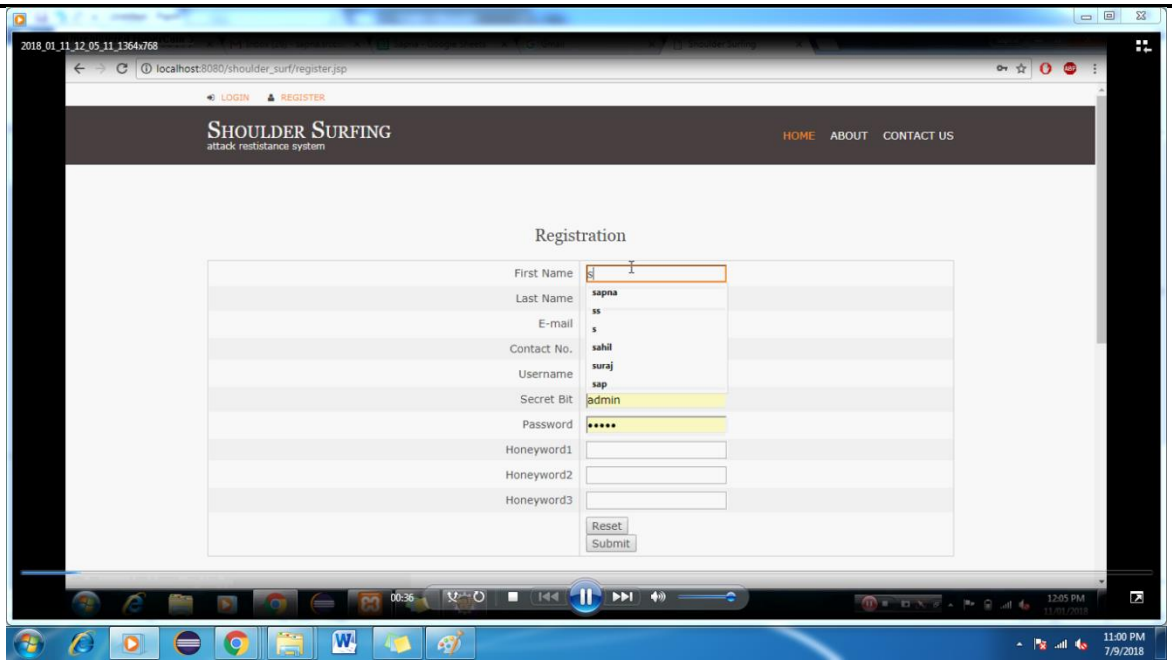
The block diagram is a simple and cost-effective approach to the security issue and the process of false passwords or accounts. Honey pot is one way of detecting an violation of a password register. Under this strategy, the programmer intentionally creates a deceitful user account to draw adversaries and detects a password leak if any of the passwords from a honey pot are used. In this paper , we proposed a new sweet word generation strategy to minimize overhead storage and to deal with the complexity of current methods for the development of sweet word. The model proposed is based on honey words for password cracking. The system based on graphic passwords called the Pass Matrix, we proposed was resistant to surfing. That image user can complete the position of their pass-square by means of a specific login indicator without explicitly clicking or pressing, which are acts that can be attacked by shoulder surfing. The design of the horizontal and vertical bars which surround the entire pass image does not give the attacker any indication to narrow the password break, even though it contains more than one record of the password. In Pass Matrix, only one password per passenger image for a sequence of images consists of a password. User-defined are the number of images (i.e., n). With Pass Matrix, users select 1 square per image, rather than as opposed to n squares, as in the Pass Points system, for a series of n images.

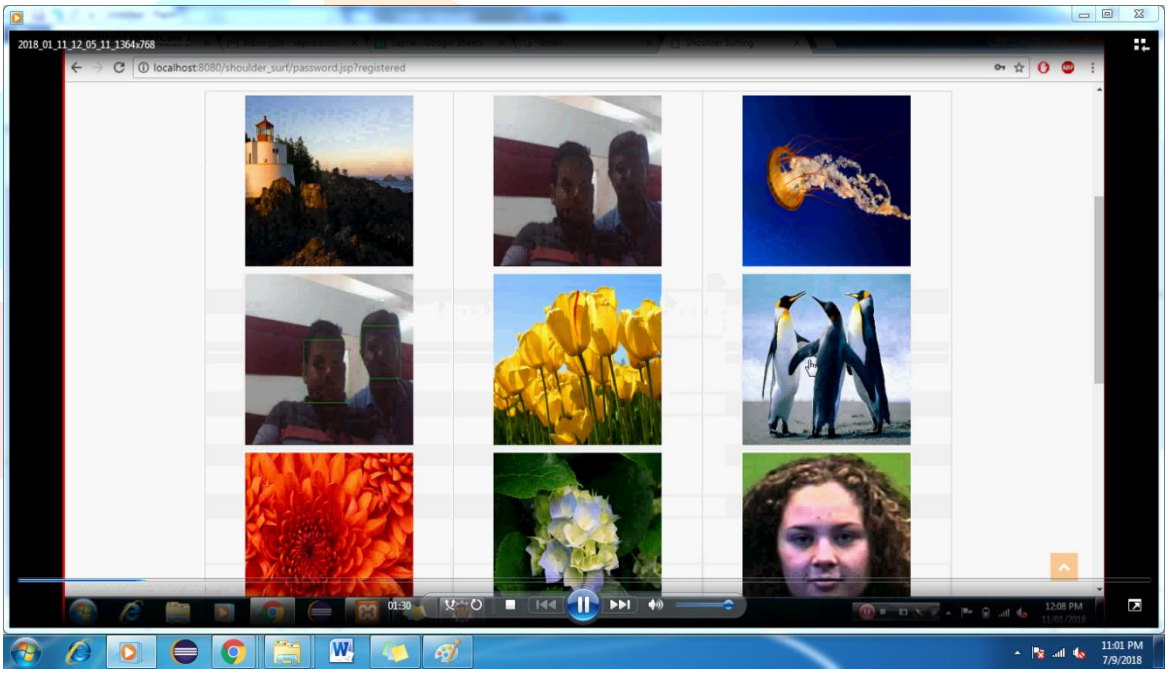
V. APPLICATION

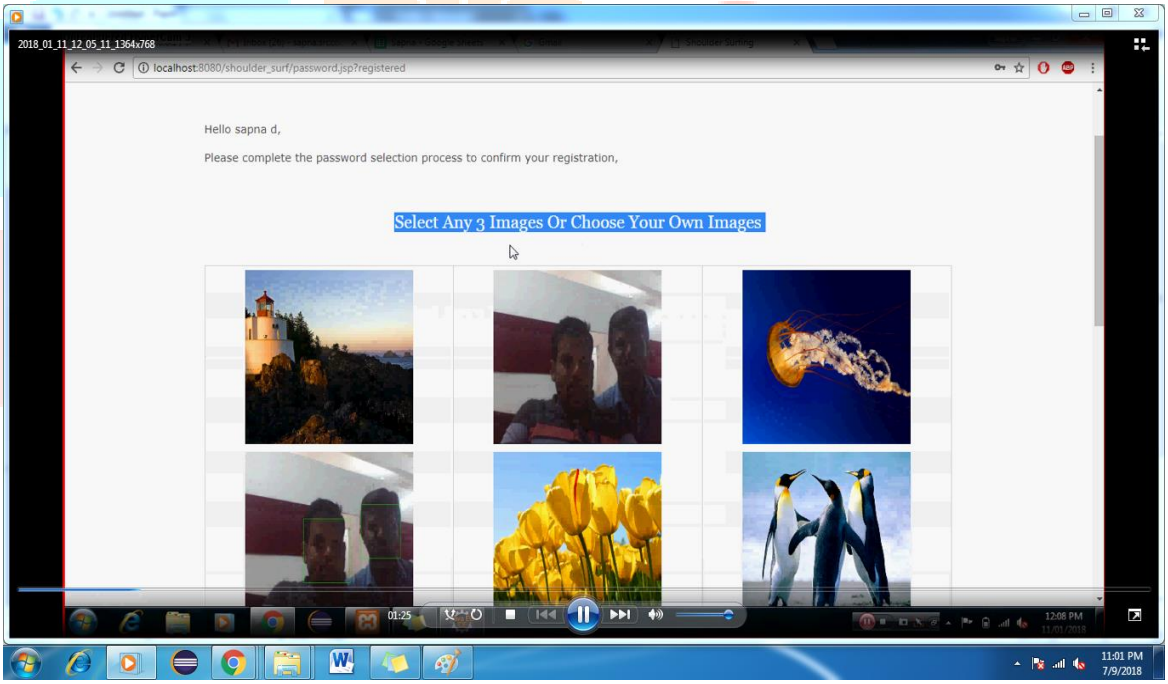
1. At online transaction.
2. To online social media.
3. System is useful to extract visually sensitive features that play an important role in the process of humans perceiving image content.
4. System can deal with Content authentication.
5. Feature extraction is a main step in all perceptual image hashing
6. schemes in which robust features will lead to better results in perceptual
7. Robustness.

VI. RESULT




2018_01_11_12_05_11_1364x768
localhost:8080/shoulder_surf/register.jsp
LOGIN
REGISTER
SHOULDER SURFING
attack restistance system
HOME
ABOUT
CONTACT US
Registration
First Name
Last Name
E-mail
Contact No.
Username
Secret Bit
Password
Honeyword1
Honeyword2
Honeyword3
sapna
ss
s
sahil
suraj
sap
admin
Reset
Submit
11:00 PM
7/9/2018


2018_01_11_12_05_11_1364x768
localhost:8080/shoulder_surf/password.jsp?registered
11:01 PM
7/9/2018



VII. CONCLUSION AND FUTURE SCOPE

They closely analyze the reliability of the honey-word framework and find many flaws that must be implemented before this technique is effectively understood. We pointed out that the strength of the honey word system essentially depends directly on the algorithm of generation; we have come up with a new strategy for generating a human-like algorithm by creating honest words that accidently use passwords that match other users from the computer system. We have a standard approach to ensuring the system's personal and business details. To order to decide whether a maliciously intruder inappropriately accesses information to a network program, we recommend tracking data access models through user actions of the profile. In addition to user real data, trapping documents stored on the device act as sensors for the detection of unauthorized entry. When inappropriately accessing or revealing information is suspected and after checked, we flood the malicious insider with false information for example in order to be able to dilute or confuse the user data.

REFERENCE

[1] D. Mirante and C. Justin, "Understanding password database compromises,"Dept. of Comput. Sci. Eng. Polytechnic Inst. of NYU, New York, NY, USA: Tech. Rep. TR-CSE-2013-02, 2013.

[2] A. Vance, "If your password is 123456, just make it hackme," New York Times, Jan. 2010.

[3] K. Brown, "The dangers of weak hashes," SANS Institute InfoSec Reading Room, Maryland US, pp. 1–22, Nov. 2013,[Online]. Available: http://www.sans.org/reading-room/whitepapers/authentication/dangers-weak-hashes-34412.

[4] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, "Password cracking using probabilistic context-free grammars," in Proc. 30thIEEE Symp. Security Privacy, 2009, pp. 391–405.

[5] F. Cohen, "The use of deception techniques: Honeypots and decoys," Handbook Inform. Security, vol. 3, pp. 646–655, 2006.

[6] M. H. Almeshekah, E. H. Spafford, and M. J. Atallah, "Improving security using deception," Center for Education and Research Information Assurance and Security, Purdue Univ., West Lafayette, IN, USA: Tech. Rep. CERIAS Tech. Rep. 2013-13, 2013.

[7] C. Herley and D. Florencio, "Protecting financial institutions from brute-force attacks," in Proc. 23rd Int. Inform. Security Conf., 2008, pp. 681–685.