A Smart Model To Enhance Cued Recall Of Textual Passwords

Jason Christopher.A[1], Jeevanandham.V[2], Joshua Pravin Raj .G[3],KalaiKovan.P[4], Thillaikarasi.R[5]
[1, 2, 3, 4] Dept of CSE
[5]Assistant Professor, Dept of CSE
[1, 2, 3, 4, 5] Saranathan College of Engineering,Trichy,Tamilnadu

Abstract- *Textual passwords remain the most commonly employed user authentication mechanism, and potentially will continue to be so for years to come. Despite the well-known security and usability issues concerning textual passwords, none of the numerous proposed authentication alternatives appear to have achieved a sufficient level of adoption to dominate in the foreseeable future. Password hints, consisting of a user generated text saved at the account setup stage, are employed in several authentication systems to help users to recall forgotten passwords. However, users are often unable to create hints that jog the memory without revealing too much information regarding the passwords themselves. We propose a rethink of password hints by introducing SYNTHIMA, a novel cued recall-based textual password method that reveals no information regarding the password, requires no modifications to authentication servers, and requires no additional setup or registration steps. SYNTHIMA makes use of users's contact lists, so that mapped password hints extracted from a user's contacts are automatically generated while the user is typing the password.*

I. INTRODUCTION

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. It has uses in the study of human–computer interaction. There are numerous keylogging methods, ranging from hardware and software-based approaches to acoustic analysis. These are computer programs designed to work on the target computer's software. Keyloggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Keyloggers can also be used by a family (or business) to monitor the network usage of people without their direct knowledge. Finally, malicious individuals may use keyloggers on public computers to steal passwords or credit card information. The keylogger can theoretically reside in a malware hypervisor running underneath the operating system, which remains untouched. It effectively becomes a virtual machine. Blue Pill is a conceptual example. A program on the machine 'gets root' and hides itself in the OS, and starts intercepting keystrokes (because they always go through the kernel). Such keyloggers reside at the kernel level and are thus difficult to detect, especially for user-mode applications who don't have root access. They are frequently implemented as rootkits that subvert the operating system kernel and gain unauthorized access to the hardware, making them very powerful. A keylogger using this method can act as a keyboard device driver for example, and thus gain access to any information typed on the keyboard as it goes to the operating system. The API based keyloggers hook keyboard APIs inside a running application. The keylogger registers for keystroke events, as if it was a normal piece of the application instead of malware. The grabbing-based keyloggers log web form submissions by recording the web browsing on submit events. These happen when the user finishes filling in the form and clicks on the "OK" or "Submit" or "Go" or anything that indicates that it is finished. This records form data before it is passed over the Internet. The Memory Injection (MitB)-based keyloggers alter memory tables associated with the browser and other system functions to perform their logging functions. This technique can be used by malware authors who are looking to bypass Windows UAC (User Account Control). The Zeus and Spy eye Trojans use this method exclusively. Non-Windows systems have analogous protection mechanisms that need to be thwarted somehow by the keylogger. This involves capturing network traffic associated with HTTP POST events to retrieve unencrypted passwords. This doesn't work if it is connected with HTTPS - in fact it was this kind of attack they were fighting when they invented HTTPS.

II. LITERATURE REVIEW

2.1. A Shoulder Surfing Resistant Graphical Authentication System [1] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh, Chia-Yun Cheng

Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as "the weakest link" in the authentication chain. Rather than arbitrary

alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. We also implemented a PassMatrix prototype on Android and carried out real user experiments to evaluate its memorability and usability. From the experimental result, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.

2.2. Secure and Usable PIN-Entry Method with Shoulder-Surfing Resistance[2]
Mun-Kyu Lee, Hyeonjin Nam

We propose a new PIN-entry method which prevents shoulder surfing attacks effectively. The proposed method uses a random mapping between PIN digits and alphabets given as challenges to the users. The user's task is to recognize this mapping and to enter the mapped alphabet sequence instead of directly entering the PIN digits. The intuitive nature and easy interface of the proposed scheme enables the users to learn it easily, and the experimental results in the pilot test show that the new method guarantees fast and reliable authentication. To be precise, the average authentication time was 5.8 to 6.8 seconds, and the average error rate was 3.3 to 6.7%.

2.3. Multi-touch authentication on tabletops [3] David Kim, Paul Dunphy,

The introduction of tabletop interfaces has given rise to the need for the development of secure and usable authentication techniques that are appropriate for the co-located collaborative settings for which they have been designed. Most commonly, user authentication is based on something known, but this is a particular problem for tabletop interfaces, as they are particularly vulnerable to shoulder surfing given their remit to foster co-located collaboration. In other words, tabletop users would typically authenticate in full view of a number of observers. In this paper, we introduce and evaluate a number of novel tabletop authentication schemes that exploit the features of multi-touch interaction in order to inhibit shoulder surfing. In our pilot work with users, and in our formal user-evaluation, one authentication scheme - Pressure-Grid - stood out, significantly enhancing shoulder surfing resistance when participants used it to enter both PINs and graphical.

2.4. On top of tabletop: A virtual touch panel display [4]
Li-Wei Chan, Ting-Ting Hu, Jin-Yao Lin, Yi-Ping Hung, Jane Hsu

In the real world, a physical tabletop provides public and private needs for people around the table. For competing scenarios such as playing a poker game or running a price negotiation around a tabletop system, privacy protection is obviously an indispensable requirement. In this work we developed a privacy-enhanced tabletop system composed of two kinds of displays, the tabletop surface and the virtual panel. All users share the large tabletop surface as a public display while every user is provided with a virtual panel emerging above the tabletop as a personal display for viewing private information. The virtual panel is an intangible, privacy-protected virtual screen created by a special optical mechanism which offers several promising characteristics, making it perfect to be integrated into a tabletop system. The contributions of the paper include: Firstly, we introduce a novel display technique, the virtual panel, into a tabletop system to build a privacy-enhanced tabletop system. Secondly, an analysis on display optics of the virtual panel is presented to explore other potentials of the display and to claim the feasibility of the proposed combination. Thirdly a computer vision-based interaction technique is proposed to provide direct-touch interaction for the virtual panel. Finally, we discuss a wide range of considerations on designing the user interface and interaction for the virtual panel.

2.5. Multiview User Interfaces with an Automultiscopic Display [5]
W. Matusik., C. Forlines, and H. Pfister.

Automultiscopic displays show 3D stereoscopic images that can be viewed from any viewpoint without special glasses. These displays are becoming widely available and affordable. In this paper, we describe how an automultiscopic display, built for viewing 3D images, can be repurposed to display 2D interfaces that appear differently from different points-of-view. For single-user applications, point-of-view becomes a means of input and a user is able to reveal different views of an application by simply moving their head left and right. For multi-user applications, a single-display application can show each member of the group a different variation of the interface. We outline three types of multi-view interfaces and illustrate each with example applications.

2.6. Enabling concurrent dual views on common LCD screens [6]

Seokhwan Kim, Xiang Cao, Haimo Zhang, Desney S. Tan

Researchers have explored a variety of technologies that enable a single display to simultaneously present different content when viewed from different angles or by different people. These displays provide new functionalities such as personalized views for multiple users, privacy protection, and stereoscopic 3D displays. However, current multi-view displays rely on special hardware, thus significantly limiting their availability to consumers and adoption in everyday scenarios. In this paper, we present a pure software solution (i.e. with no hardware modification) that allows us to present two independent views concurrently on the most widely used and affordable type of LCD screen, namely Twisted Nematic (TN). We achieve this by exploiting a technical limitation of the technology which causes these LCDs to show varying brightness and color depending on the viewing angle. We describe our technical solution as well as demonstrate example applications in everyday scenarios.

2.7. Use Your Illusion: secure authentication usable anywhere [7]

Eiji Hayashi, Rachna Dhamija, Nicolas Christin, Adrian Perrig

In this paper, we propose and evaluate Use Your Illusion, a novel mechanism for user authentication that is secure and usable regardless of the size of the device on which it is used. Our system relies on the human ability to recognize a degraded version of a previously seen image. We illustrate how distorted images can be used to maintain the usability of graphical password schemes while making them more resilient to social engineering or observation attacks. Because it is difficult to mentally "revert" a degraded image, without knowledge of the original image, our scheme provides a strong line of defense against impostor access, while preserving the desirable memorability properties of graphical password schemes. Using low-fidelity tests to aid in the design, we implement prototypes of Use Your Illusion as i) an Ajax-based web service and ii) on Nokia N70 cellular phones. We conduct a between-subjects usability study of the cellular phone prototype with a total of 99 participants in two experiments. We demonstrate that, regardless of their age or gender, users are very skilled at recognizing degraded versions of self-chosen images, even on small displays and after time periods of one month. Our results indicate that graphical passwords with distorted images can achieve equivalent error rates to those using traditional images, but only when the original image is known.

III. MODULE IMPLEMENTATION

3.1 USER REGISTRATION MODULE

Here the user registers his details. The user name should be unique. It is stored by an id in the database. Next a valid email id is procured. The user is redirected to the next screen. The generated unique identity is shown to the user for his login purposes. Then he is redirected to the next screen, where the user is shown the alphanumeric textual password.

3.1.1 TEXT GRID DEPLOYMENT

Here the user submits a textual password which should be having a minimum length of the 8 characters. This can be called as secret pass. The secret pass should contain even number of characters. This is validated and then stored in the user database. Next the user's id redirected to the next screen, where the user is shown the color screen.

3.1.2 SYNTHIMA HINT GENERATION

Given that a hint displayed by SYNTHIMA reveals no information regarding the password associated with it, knowing a password hint only would not be of value for the adversary. For an adversary who has access to the size and full content of the contact list, knowing the password hint will only help in reducing the search space of the dictionary on average to n1 of its original size. As SYNTHIMA displays more than one hint per password (e.g., for an 8-character password, a hint would be displayed after typing the 6th character, another hint after typing the 7th character and then another one after typing the 8th character), knowing the hint associated with any character of the password might contribute to reducing the search space further. That is, if the attacker managed to observe h number of hints associated with different characters of the password in question, the search space would be reduced.

3.2 EMAIL MODULE

The generated combination is sent to the users email id. The users then have to go to the corresponding mail id and find out the combination for the text and the appropriate code and enter it into the user's login.

3.3 VERIFICATION MODULE

During this phase the system verifies if the combination is right for the SYNTHIMA hint provider which has been supplied for this session. If the password is accurate then the user is allowed entry into the system otherwise the

login fails. As the interface changes every time, the session password changes. This technique is resistant to shoulder surfing. Due to dynamic passwords, dictionary attack is not applicable. The entered code is uploaded, matched and verified by the system.

IV.SOFTWARE REQUIREMENTS

USE CASES:

1. Registering user in Webserver

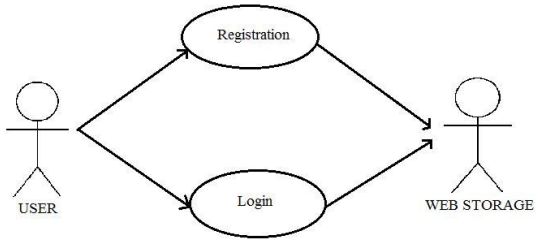


Fig 3.1 Registering user in webserver

DESCRIPTION

First the users register themselves in the system by providing their details which are stored in the data store. The users then login with the SYNTHIMA support.

2. Registering hints for password

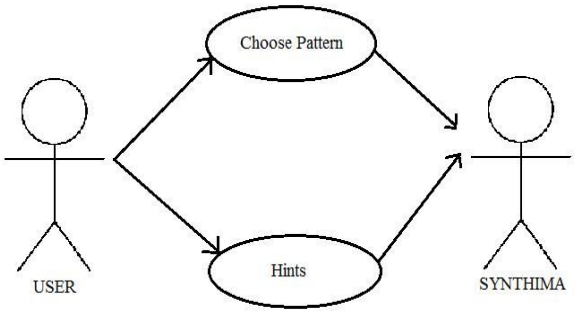


Fig 2 Registering Hints for Password

DESCRIPTION

The SYNTHIMA asks the users to choose a customized pattern model – like image, contact, email, color, place combo. Any customized combination may be used. Users are shown the hints generated based on the basis of selections made.

3. Generating hints

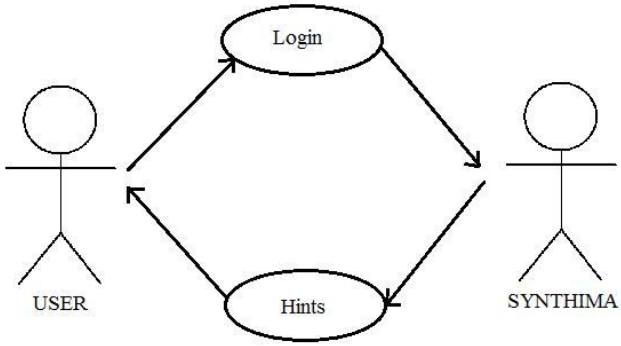


Fig 3 Generating hints

DESCRIPTION

The user's login the SYNTHIMA shows hints and allows them to login using the predefined patterns selected earlier.

4. Verification

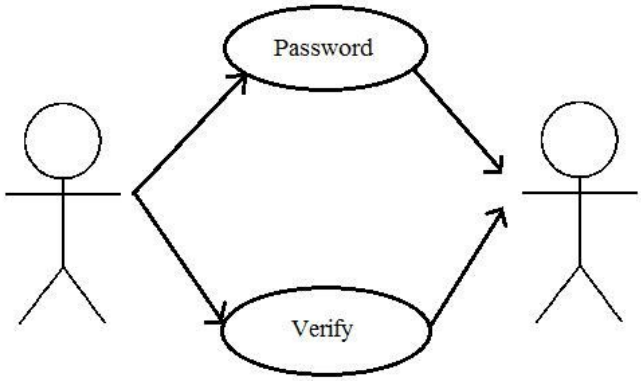


Fig 4 Verification

DESCRIPTION

The users passwords are verified and then granted access to the system if it is found to be correct.

3.4 FUNCTIONAL REQUIREMENTS:

1. Registering user In Webserver

Use case name	User Registration In Webserver
User	Details are registered
Register	Data are registered in the server
Login	The users login to the system.
Web Storage	Data are stored
Reference	Fig 1

2. Registering hints for password

Use case name	Registering hints for password
User	User can give information
Choose pattern	Having different patterns
Hints	Having many hints
Synthima	Algorithm
Reference	Fig 2

3. Generating hints

Use case name	Generating hints
Login	The user login to the system
Hints	Having different hints
Synthima	Algorithm
Reference	Fig 3

4. verification

Use case name	Verification
Password	Enter the password
Verify	It can validate user
Reference	Fig 4

V. DESIGN MODEL

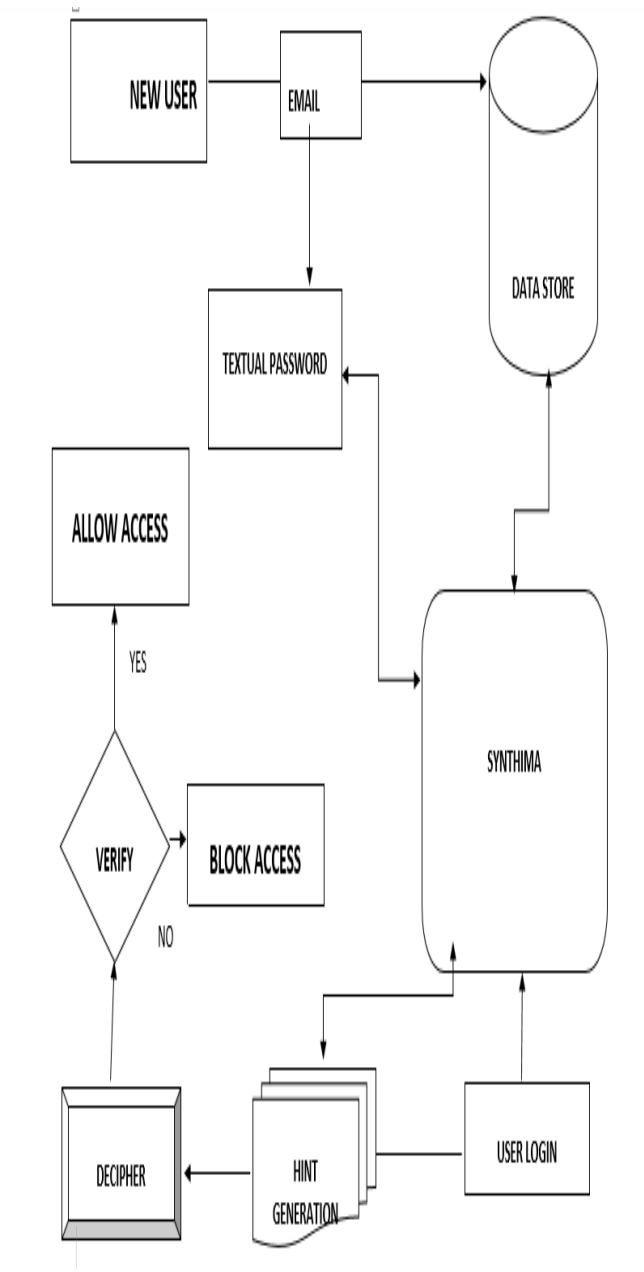


Fig 5.1 architecture

VI. TESTING

6.1 INTEGRATION TESTING:

Integration Testing means set of components interactionbetween the modules. In this system perform the integration testing on the one module to another module.

Test Report:

Sno	Input(s)	Expected Output	Obtained Output
1.	User registration	UserId Generated	User id Generated

6.2 Validation Testing:

Validation is the checking or testing of items, includes software, for conformance and consistency with an associated specification. Validation is the process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.

Module: User Login and User Menu

S.No	Input	Description	Expected output	Actual output
1.	password	Generating hints	Hints generated	Hints generated
2.	Userid and Password	verification	Login Sucess	Login Success

PROPOSED MODEL

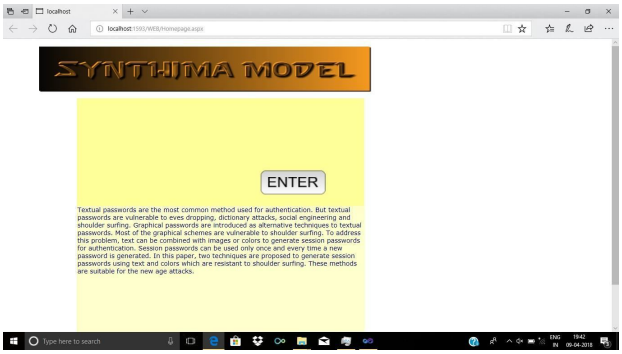
The SYNTHIMA mechanism functions by mapping each entered password to a name of a person that already exists in the user's contact list. It is further enhanced by using combination of pictures used for contacts, email ids, images, phone numbers etc. The SYNTHIMA model is pre-adjustable or customizable which allows the user to adjust the hints to displayed for a specified characters of a password. So as an example, based on this is where every odd character in a user's text password may be represented as an image hint. Every even character is represented as a contact's last name and every character after the sixth letter to be hinted as an email id or location place.

VIII. CONCLUSION

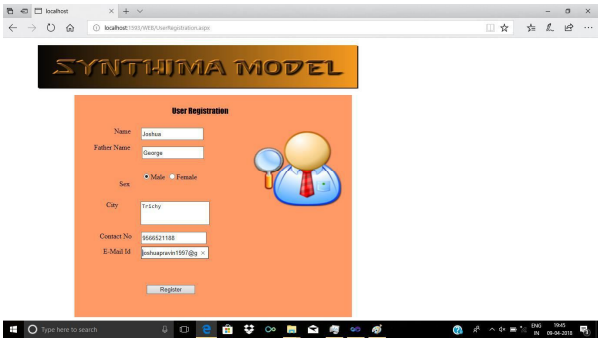
Thus the proposed SYNTHIMA algorithm model is a secure authentication mechanism functions by mapping each entered password to a name of a person that already exists in the user's contact list. It is further enhanced by using combination of pictures used for contacts, email ids, images, phone numbers etc. The SYNTHIMA model is pre-adjustable or customizable which allows the user to adjust the hints to displayed for a specified character of a password. On the basis of the associative-strength theory, this can be supported by the fact that encountering hints multiple times would strengthen the mental associative ties between passwords and hints, which would therefore allow users to utilize displayed hints more effectively

SCREENSHOTS OF MODULE:

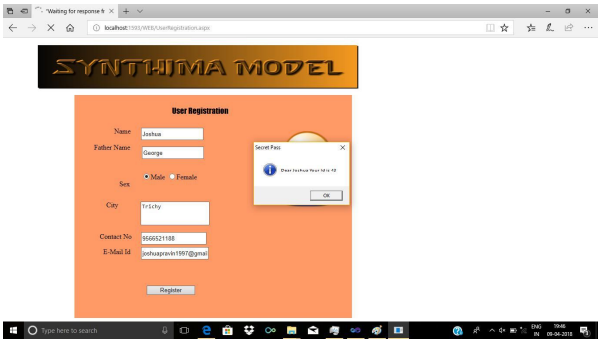
Home page



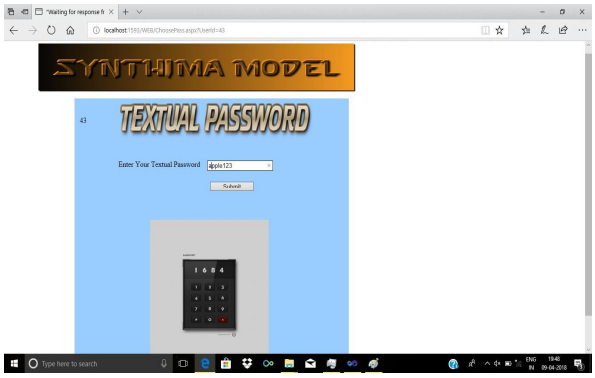
Registratin Successful



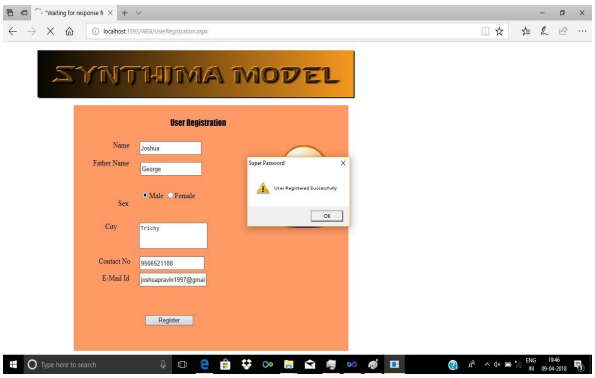
Login Page



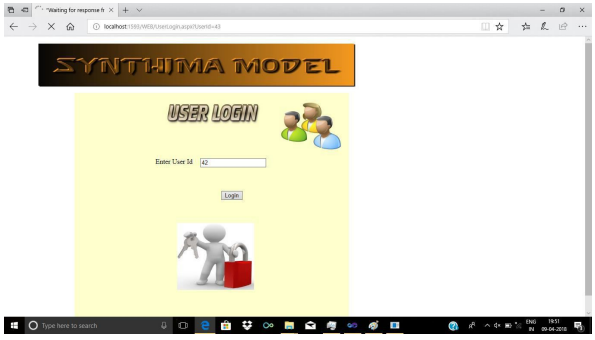
Choosing Password

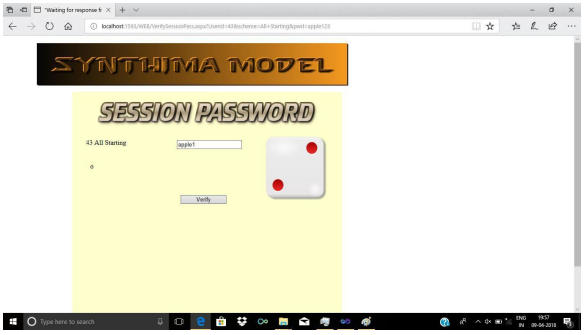


Hint Generation



Login Success





REFERENCES

[1] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh, Chia-Yun Cheng,
"A Shoulder Surfing Resistant Graphical Authentication System".

[2] Mun-Kyu Lee, Hyeonjin Nam, "Secure and Usable PIN-Entry
Method with Shoulder-Surfing Resistance".

[3] David Kim, Paul Dunphy, "Multi-touch authentication on tabletops".

[4] Li-Wei Chan, Ting-Ting Hu, Jin-Yao Lin, Yi-Ping Hung, Jane Hsu,
"On top of tabletop: A virtual touch panel display".

[5] W. Matusik., C. Forlines, and H. Pfister, "Multiview User Interfaces
with an Automultiscopic Display".

[6] Seokhwan Kim, Xiang Cao, Haimo Zhang, Desney S. Tan,
"Enabling concurrent dual views on common LCD screens".

[7] Eiji Hayashi, Rachna Dhamija, Nicolas Christin, Adrian Perrig, "Use Your Illusion: secure authentication usable anywhere".