IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Special Issue-14, May 2019 E-ISSN: 2347-2693

# Illusion Pin: Authentication Using Zero Knowledge Protocol

**Soubhagyalaxmi V Nerabenchi[1*], Sanjana B[2], Shaik ajith[3], Siddalinga Navadagi[4]**

School of Computing and Information Technology, REVA University, Bangalore, India

DOI: https://doi.org/10.26438/ijcse/v7si14.471473 | Available online at: www.ijcseonline.org

***Abstract***— we have used Illusion PIN(IPIN) to solve the problems regarding shoulder_surfing attacks on authentication schemes.PIN -based authentication are practically used on touch screen devices. PIN works on the principle technique of hybrid images.The hybrid images are been merged to keypads. These keypads are ordered to different digits.Thus,making the user to see the device and enter the password whereas the attacker would see another password as the attacker is not as close as the user.The keypads are been shuffled to avoid further attacks,if the attacker is able to remember the position of the keypads.To increase the reliability and security of illusion pin,we worked on algorithm based on human visual perception and calculatimg the minimum distance from attacker and the user.We evaluated our calculations with 84 simulated shoulder-surfing attacks that were obtained from 21 different people.All of the 84 attacks were unsuccessful and we evaluated the minimum distance that a camera cannot capture the necessary data from use’s keypad.. According to our analysis,surveillance camera were not able to capture the PIN of a touchscreen user when Illusion PIN is used.

***Keywords***—PIN, touch creen devices, Analysis surveillance

## I. Introduction

There are many ways to perform user authentication.In our project,we have used PIN authentication as it is simple and has maturity.PIN stands for Personal Authentication Number,this is a sequence of digits that verifies the identity of the user .PINs are simple as it consist of numeric characters(0-9) and has a short length of 4 or 6 digits.This PIN is more simpler than alpha-numeric passwords.As PINs are simple and short in length,it can be remembered without any faults.Thus,simplicity is converted into usability.PIN Authentication has been used for many years making it have maturity.It has been increased to a wide range of application like smartphones and net banking.The future enhancement of this project would depend on the hypothesis that PIN Authentication will avoid shoulder-surfing attacks without a significant overhead in its usability.This was enabled in the following ways:In touchscreen devices Illusion PIN(IPIN) was designed.The virtual keypad of have two different keypads as they have different ordering of digits.These two keypads are merged to a single hybrid image.The user would see one keypad as he is closer to the screen whereas the potential attacker would see another keypad as he is far away from the keypad.An algorithm was developed to calculated the visuality of the user’s keypad from a given viewing position.

## II. Modules Created

1. User Registration:

In user registration module,the user has to enter his personal details like User_id,User name,password,valid email_id along with these information user has to select an image.The user will be assigned to select three random images that are graphical password selected by coordinate squares of the images.These details are stored in the database.

2 .Hash code generation:

After setting the coordinating images,these details are stored in the database successfully.all the three images selected by the user is been concated and hash codes are generated.these hash codes are again stored in the database with respect to the user.

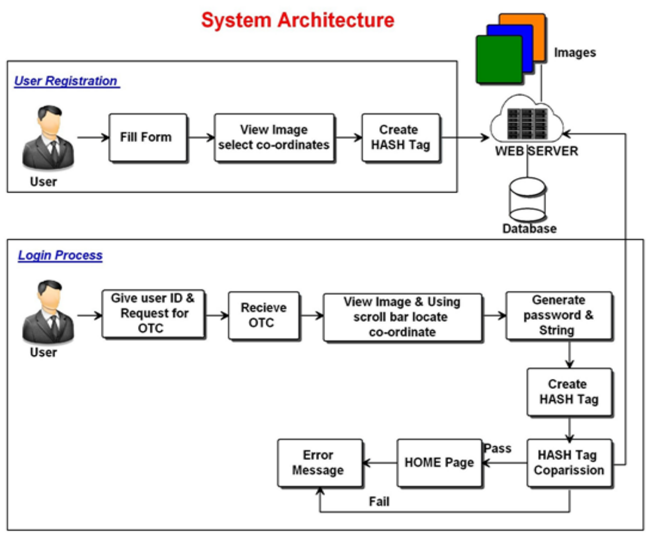
3. User Login Process:

The user can login by using the user_id and password which was entered during registration process.If the entered user_id and password is valid then the user will recieve One Time Password(OTP) to his/her registered email id.The OTP consist of random pair of vertical and horizontal sliders.User has to arrange the vertical and horizontal sliders for just three images.The OTP coordinate value must be same as that to coordinates selected by the user during registration OTP will generate hash codes that are concated.If the hash codes match then login is successful and enters into homepage else login is unsuccessful and login page will be displayed.

4. Admin:

Admin has to login to his account using authenticated user name and password.After successful registration of an user,Admin can view the user’s details.

## III. System architecture



## IV. SYSTEM DESIGN

Designing of Web apps focuses on technical and non-technical activities.The display and experience provided by the content is developed by graphical design.The user interface has aesthetic layout which is developed by interface design.The Web App's technical structure consists of architectural and navigational design.

The activities of the design process**:**

1. Interface design-It layouts the structural and the organization of user interface.Interface design contains representation of screen layout, definition of modes of interaction and description of navigation techniques. To initiate navigation options for Interface Control mechanisms,the designer selects from the interaction mechanism.
   a. Navigation menus
   b. Graphic icons
   c. Graphic images

   Interface Design work flow- the work flow starts from the user identification, task and environmental requirements. As soon as the user tasks are accepted,user scenarios are generated. These are being checked to explain a group of interface objects and actions.

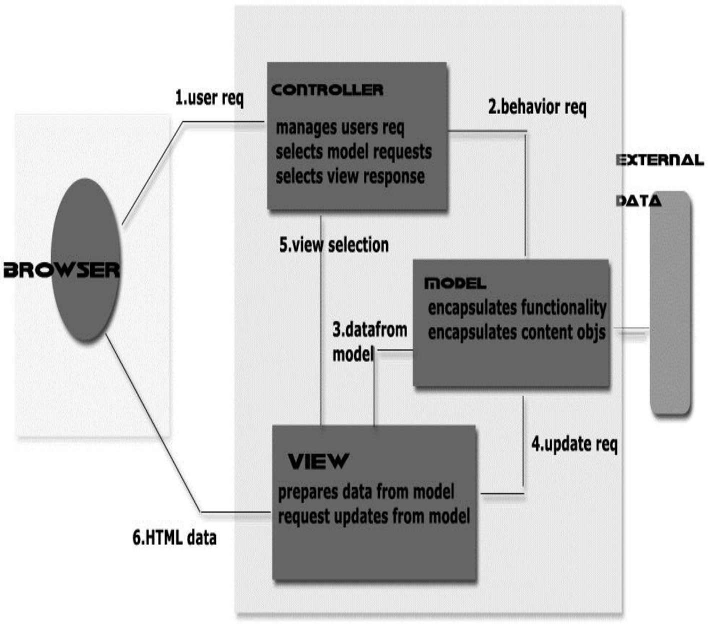
2. Aesthetic design-The design of Web App has been explained by Aesthetic design as "look and feel" .Aesthetic design is also called as graphic design. Graphics design consists of color schemes ,geometric layout, Aesthetic decisions ,use of graphics.text size ,font and placement.
   Content design-It explains the layout, structure and outline provided in Web App.
   Navigation design-It shows the navigational flow between contents objects and WebApp functions.

3. Architecture design-It helps find hyper media structure for WebApp.It enables the goals created from WebApp and user visits and navigation philosophy.

   a. Content architecture, deals with manner in which content objects and structured for presentation and navigation.

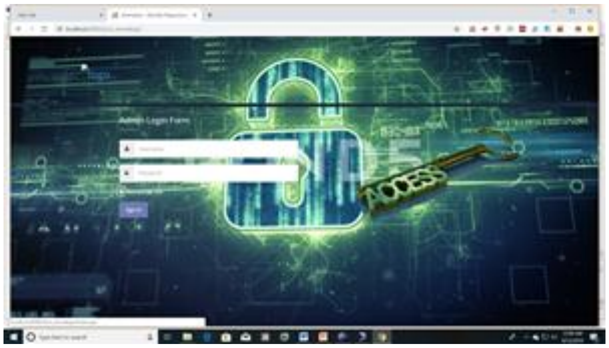
   b. Webapp architecture,slides into the manner the application is structured to manage user interaction,handle internal processing tasks,effect navigation and present content.It has explained the context of the development environment in which the apllication is to be implemented.

4. Component design-creates the entire processing logic wanted to implement functional components.



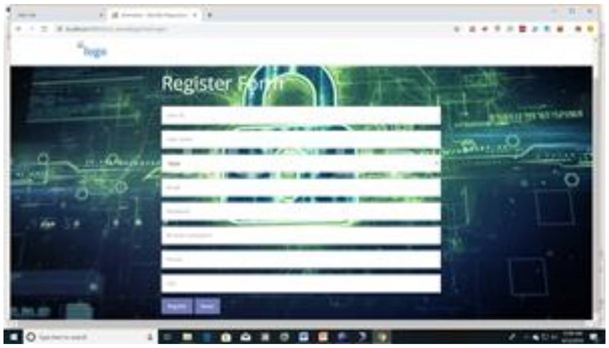
## V. IMPLEMENTATION

A. Login process



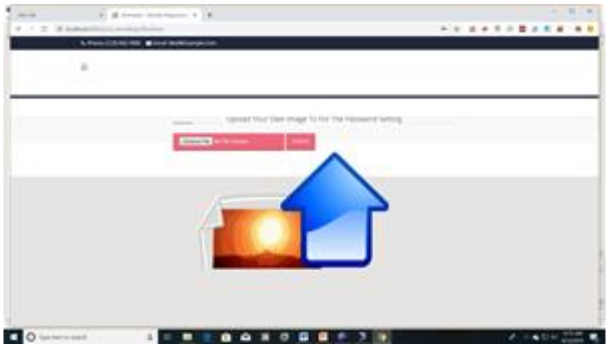
Admin Login Form

B. Registration



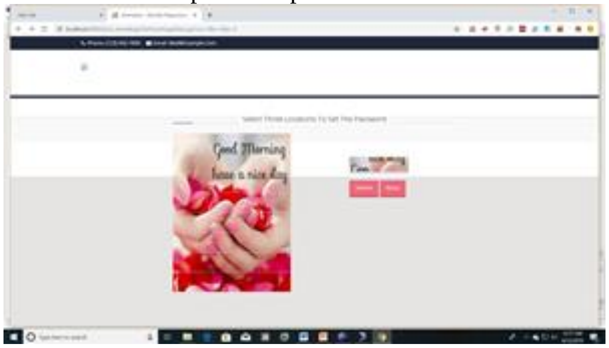
Register Form

C. Choose the image



Upload Your Own Image To For The Password Setting

D. Select 3 points as password



Select Three Locations To Set The Password

## REFERENCES

[1] Stajano, "The quest to replace passwords: was written by J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano,

[2] M. Harbach, A. De Luca, and S. Egelman, "The anatomy of smartphone unlocking,"

[3] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every eleven wallets? the security of customer-chosen banking pins."

[4] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens."

[5] A. Oliva, A. Torralba, and P. G. Schyns, "Hybrid images," ACM Transactions on Graphics (TOG)

[6] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. W. Nicholson, J. Nicholson, and P. Olivier, "Multi-touch authentication on tabletops."

[7] L.-W. Chan, T.-T. Hu, J.-Y. Lin, Y.-P. Hung, and J. Hsu, "On top of tabletop: A virtual touch panel display,"

[8] W. Matusik, C. Forlines, and H. Pfister, "Multiview user interfaces with an automultiscopic display,"

[9] C. Harrison and S. E. Hudson, "A new angle on cheap lcds: making positive use of optical distortion,"

[10] S. Kim, X. Cao, H. Zhang, and D. Tan, "Enabling concurrent dual views on common lcd screens,"

[11] E. Hayashi, R. Dhamija, N. Christin, and A. Perrig, "Use your illusion: secure authentication usable anywhere,"

[12] I. Jermyn, A. J. Mayer, F. Monrose, M. K. Reiter, A. D. Rubin et al., "The design and analysis of graphical passwords."

[13] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, "Shoulder surfing defence for recall-based graphical passwords,"

[14] D. S. Tan, P. Keyani, and M. Czerwinski, "Spy-resistant keyboard: Towards more secure password entry on publicly observable touch screens,"

[15] V. Roth, K. Richter, and R. Freidinger, "A pin-entry method resilient against shoulder surfing,"