Second International Conference on Nexgen Technologies
Sengunthar Engineering College, Tiruchengode, Namakkal Dist. Tamilnadu (India)
8th - 9th March 2019 www.conferenceworld.in ISBN : 978-93-87793-75-0

SHOULDER PEAK RESISTANT PIN ENTRY SCHEME USING CONCENTRATE HAPTIC FEEDBACK

Abinaya.S[1], Angel Rini Mejola.J[2], Dinesh Babu.B[3],
Dr. R.Sabitha[4], Dr.T. Kalaikumaran[5]

[1,2,3,4,5] *Department of Computer Science and Engineering,*
SNS College of Technology, Coimbatore (India)

ABSTRACT

PIN-passage plans are vulnerable to perception assaults. To improve the protection from perception assaults, some safe PIN-passage plans for cell phones dependent on sounds or haptics have been proposed. Be that as it may, none of existing perception assaults safe PIN-section plans can accomplish both great security and high ease of use. Here,we propose another perception assaults safe PIN-passage conspire, Loc-HapPIN, for touchscreen gadgets giving confined haptic criticism. By utilizing the haptic input innovation, the ease of use and the protection from perception assaults are improved. Moreover, the client can pick the productivity security setting appropriate for individuals.

Keywords: observation attack,PIN entry scheme, password authentication,shoulder surfing.

I. INTRODUCTION

In existence without the proper usage of security or locks in Mobile Phones which leads to susceptibility of hacking others personal information. This personal information involves misusing others photo's, banking details, getting some important documents being misused by others without proper security scheme. The problem of security is growing very bad due to smart phone usage.

This project is a mobile application based project to enhance security. "PIN SECURITY SCHEME USING HAPTIC FEEDBACK" is a user-friendly software application. The purpose of this project is to provide a better security, a software solution that delivers a scalable, secure, and reliable application that maintains and manages the application details. The following Document will outline the feature of the "PIN SECURITY SCHEME USING HAPTIC FEEDBACK" and the requirements that the project will adhere to developing the software for the user security purpose.

II.LITERATURE SURVEY

A unique mark scanner is a sort of innovation that distinguishes and validates the fingerprints of a person so as to allow or deny access to a PC framework or a physical office [4].A secret word is a series of characters used to check the personality of a client amid the verification procedure. Passwords can vary in length and can contain letters, numbers and special characters[1].The PIN lock is an authentication measure for mobile phones that

requires the entry of a personal identification number (PIN) code before a device can be used. Most mobile phone users lock their devices with PIN codes to prevent fraudulent use in case the phone set is lost or stolen[5].[8]proposed an audio based observation attacks resistant four digit pin entry scheme using earphones, the audio version of phone lock. However, as the user's operation burden is rather high, its usability is insufficient. In the same year, an audio based observation attacks resistant four digit pin entry scheme using earphones, spin lock was proposed.

III.PROBLEM DEFINITION

A. In finger print scanning scheme, the lock can be easily grabbed by other person if we have gently kept the finger in any of the objects.

B. In password lock, passwords can be effortlessly grabbed using shoulder surfing attack where the other person can easily misuse the observed password.

C. In PIN lock schemes, PIN can contain only 4digits which can be easily guessed and it also undergoes shoulder surfing attack.

IV. PROPOSED SYSTEM

The key clue behind this application is to enhance the security. Initially the user register the required fields and get the OTP. Haptic feedback system is available to prevent shoulder surfing attacks that sends OTP to any registered mobile GSM device. The Random vibration for the each pin is generated. If someone try to misuse the pin their image is been capture and sent to the owner's registered mobile number.

The methods that I have used for this application are as follows:

a. A pseudo-arbitrary number generator is a program composed for, and utilized in, likelihood and insights applications when huge amounts of irregular digits are required. A large portion of these projects produce unlimited strings of single-digit numbers, for the most part in base 10, known as the decimal framework.When large samples of pseudo-arbitrary numbers are taken, each of the 10 digits in the set {0,1,2,3,4,5,6,7,8,9} occurs with equal occurrence, even though they are not evenly distributed in the sequence.

b. Pseudo Random method which can be reproducible if the algorithm is found. The very actuality of the algorithm, no matter how refined, means that the next digit can be foreseen! This has given rise to the term pseudo-arbitrary for such machine-generated strings of digits. They are equivalent to arbitrary-number sequences for most applications, but they are not truly random according to the severe definition.

The Haptic input is a security conspire in which we have to enlist the required subtleties and a telephone number is enrolled for recuperation reason and an OTP is created. A confirmation is finished by sending an OTP to the enlisted number and a security question and answer is been set to recoup the overlook secret word. In the event that somebody endeavor to get to it will catch the people picture and will send to the enlisted number .

Haptic Feedback, regularly alluded to as essentially "haptics", is the utilization of the feeling of touch in a UI configuration to give data to an end client. When alluding to cell phones and comparative gadget, this by and large methods the utilization of vibration from the gadget's vibration.The objective of my project is to secure a proper app lock for different applications.This is done by random vibration technique using a pure random variable is based on atmospheric parameter so it cannot be reproduced. This vibration is used to count the already registered pin. After vibration if you press enter the apps that are secured will be shown.

IV .1HRNG

A Hardware Random Number Generator (HRNG) is a device that generates arbitrary numbers from a physical process, rather than by means of an algorithm. Such devices are often based on microscopic phenomena that generate minimum-level, statistically random "noise" signals, such as thermal noise, the photoelectric effect, involving a beam splitter, and other quantum phenomena. These stochastic processes are, in theory, completely volatile, and the theory's assertions of irregularity are focused to experimental test. This is in contrast to the common model of pseudo-arbitrary number generation commonly applied in computer programs or cryptographic hardware.

A hardware arbitrary number generator stereotypically consists of a transducer to convert some characteristic of the physical phenomena to an electrical signal, an amplifier and other electronic circuitry to increase the amplitude of the random oscillations to a measurable level, and some type of analog to digital converter to convert the output into a digital number, often a simple bit 0 or 1. By repeatedly sampling the randomly varying signal, a series of arbitrary numbers is attained.

The foremost solicitation for electronic hardware arbitrary number generators is in cryptography, where they are used to generate arbitrary cryptographic keys to communicate data firmly. They are extensively used in Internet encryption protocols such as Secure Sockets Layer (SSL).

The project is about the PIN security scheme using Haptic Feedback. The objective of this application is to find whether the existing app locks are protected are not. This is done by arbitrary vibration using Sqlite. This is used to compute the registered PIN with the vibration.These are the modules of PIN security scheme using Haptic feedback.

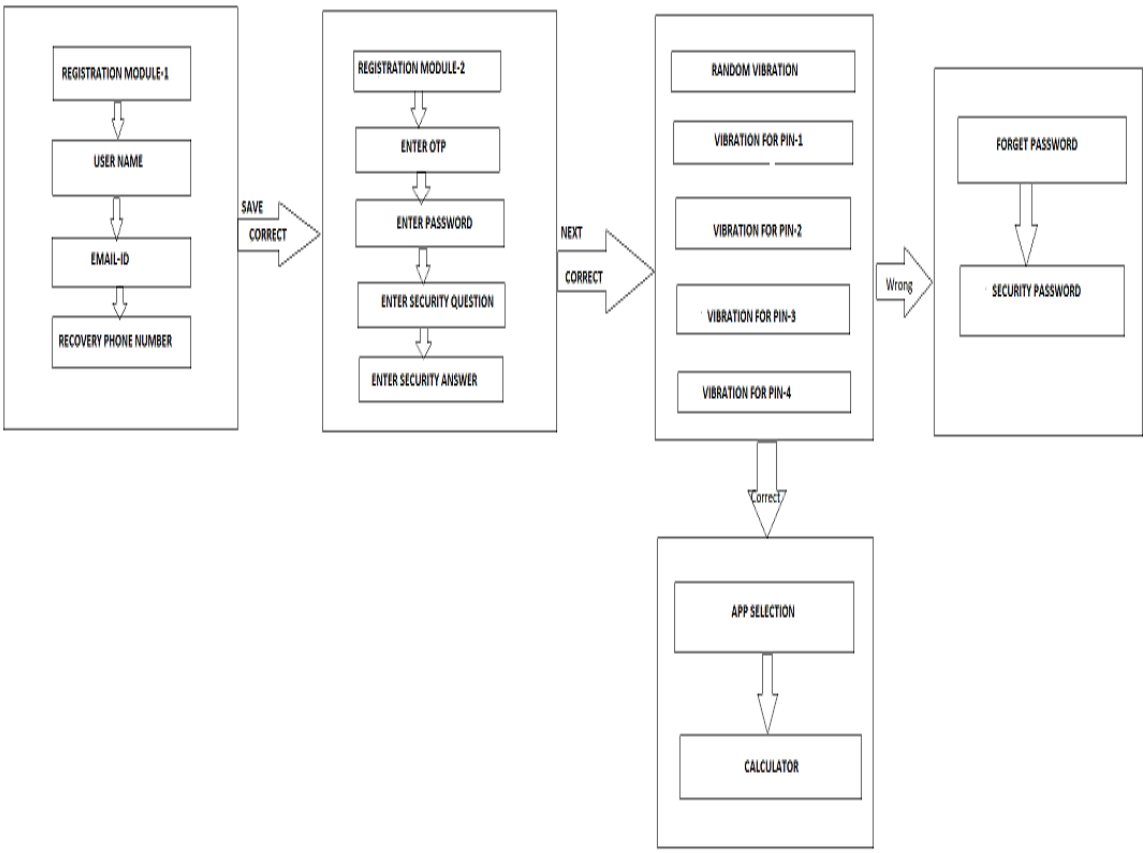

Fig.1 System design

4.2 Registration module-1

The user need to register the required details to know that the required person use the mobile Username, mail-id and the recovery phone number is set first and warehoused in the Database after the completion of first page as illustrated in Fig.2.The second page with further details get displayed by clicking next.

Fig.2

4.3Registration module-2

One Time Password is sent to the registered number after submitting the first page as illustrated in Fig.3. Enter the OTP as shown in Fig.4, if you enter any number randomly you will get error message that your OTP is wrong. You are able to enter the password the limit of the password is restricted only to 4digit, the security question can be entered by the user and the security answer is also set by the user all the details are deposited in the Database by clicking next.

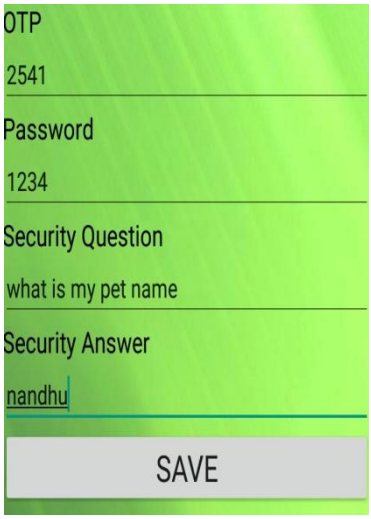

Fig.3 Fig.4

4.4 Random vibration technique

From the registration module-2 we have saved a password for the password for each pin we get vibration between (1-5)times. Enter the pin after the vibration stops then the vibration starts for the second pin this step repeats for each registered pin. After the pin is entered. Press entered as illustrated in Fig.5. If the password and the vibration matches if the pin that we have entered is right then we go to the next module the app which is secured will display.

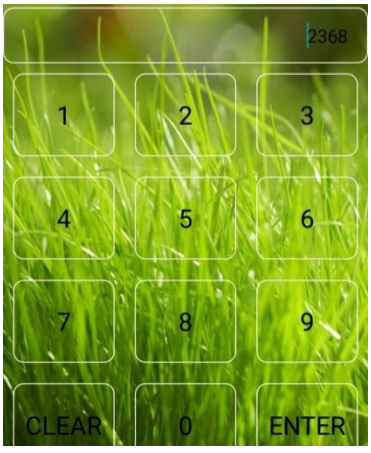

Fig.5

4.5Forget password

If the password is wrong we will get the forgot password the security question which we have registered is displayed in forgot password enter the correct answer for that question the password that we have saved is directed to the registered number as illustrated in Fig.6

Fig.6

4.6Image capture message

In this module, if anyone sees our generated one time password and then they try to retype and unlock any app, then their image will be captured and sent to registered mobile number as illustrated in Fig.7. So misusing of our mobile by others can be easily identified**.**

Fig.7

4.7 Advantages

a. Easy to implement
b. User friendly
c. No modification in the existing hardware

V. FUTURE WORKS

a. Same Mobile solicitation can be developed for others operating systems such as Windows, iOS etc.
b. Existing software is developed for Mobile phones of Android operating system with lollipop version and below. Same app can be developed for higher android version.
c. In future, the user could able to select any applications available in his mobile phone, so the selected applications can be secured.

VI. CONCLUSION

The project PIN security scheme using Haptic feedback is very simple in design and to implement. The mobile requires very low resources and works in almost all configurations and its interface is very user-friendly. It include registration of the user, then the random vibrations are counted which is added with already existing PIN and new password is generated every time. The generated new password is been typed to unlock an app.

REFERENCES

[1] Kahazima Irfan, Agha Anas , Sidra Malik and Saneeha Amir,*Text Based Graphical Password System To Abscure Shoulder Surfing*,2018 IEEE International Bhurban Conference on Applied Science And Technology(IBCAST),Islamabad,Pakistan.

[2] Yu-xuan Dan, Wei-chiku, *A Simple Observation Attacks Resistant Pin Entry Scheme Employing Audios*,2017 IEEE International Conference on Communication Software and Networks.

[3] Santhosh Kumar Behera, Suman Bhoi, Debi Prosad Dogra and Partha Partim Roy, *Robustness Analysis of Motion Sensor Guided Air Authentication System*,2018 IEEE Transactions on Consumer Electronics.

[4] N.Wakabayashi, M. Kuriyama and A. Kanai, *Personal authentication method against shoulder-surfing attacks for smartphone*, 2017 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV pp. 153-155, 2017.

[5] Khandelwal, Ankesh, Shashank Singh, and NirajSatnalika,*User Authentication by Secured Graphical Password Implementation International Journal of Computer Applications* pp 115-120, 2013.

[6] Davis, Darren, FabianMonrose, and Michael K. Reiter. *On User Choice in Graphical Password Schemes*,USENIX Security Symposium.Vol. 13. 2016.

[7] Man, Shushuang, Dawei Hong, and Manton M. Matthews. *A ShoulderSurfing Resistant Graphical Password Scheme-WIW*,Security and Management.

[8] A.Bianchi, I.Oakley, V.Kostakos, and D.S.Kwon,*The Phone lock:Audio and haptic shoulder surfing resistant pin entry methods for mobile devices*,Proc. Of 2011 5th International Conference On Tangible,Embedded and Embodied Interaction.