Special Issue of Engineering and Scientific International Journal (ESIJ)
Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College (TSRW-MCA-SAEC) – May 2015
ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Providing Security using Touch Screen Pattern

P.Rajeswari

Department of Computer Applications, S.A. Engineering College, Chennai.
rajimca47@gmail.com

***Abstract*—**Touch screen based system allows an easy navigation around a GUI based environment. As the knowledge advances, people may be able to operate computers without mice and keyboard. Number of peoples uses touch screen mobile phones, tablets, PDA's for the different purposes such as accessing online data, net banking, storing personal data [bank account details, contact numbers , official data etc] . If such mobile is lost or taken then it can be misuse by other peoples and also there is problem for recovering such the data. Hence providing security for such Smartphone devices, we are survey the techniques which provide safety to the Smartphone devices. To put off this type of activities and offer security for the field of computer science. In this paper, I recommend and provide an idea for uniqueness of the secret word using implicit authentication approach that enhanced the password pattern with additional security layer .I provide two security checks in two steps. The two authentication methods used are time taken to draw the pattern which is a behavioural biometric authentication method, password pattern .If two methods are satisfy then only the user allow to access.

***Key words*—** *pattern password, user authentication, touch screen device, retina recognizer*

1. Introduction

Today's phones already enable contactless payments, mobile folders and mobile banking, and these changes are the indication the need for secure services that can be performed wirelessly or with a Smartphone. Smartphone, tablets and other mobile devices continue to propagate and provide users with powerful, mobile network, multimedia computation options, hence the need to safeguard them. According to the handheld devices definition they are use for the storing data, accessing data that will be private or common data. Recently the use of hand held devices increases because it provides large storage capacity also fast internet access speed.

The study of over 6,000,000 secret code, 91% of all user passwords belong to a list of just 1,000 common passwords (e.g., 8.5% users use either "password" or "123456" as their passwords). I have proposed a major modification in graphical pattern passwords by using the 3*3 grid points using biometric pattern to provide more security during authentication.

To concentrate on the pressing demand for a more secure and user friendly mobile authentication solution technological advances in computing and I/O capabilities as well as network connectivity are shifting the focus from PCs to mobile devices. For the purpose of authenticating a user is the central task for almost every application running on any computer based devices.

Text-based username password scheme is the most used technique for user authentication, but it is well known and proved by various researchers that users typically choose weak passwords, and have problems to remember the stronger ones.

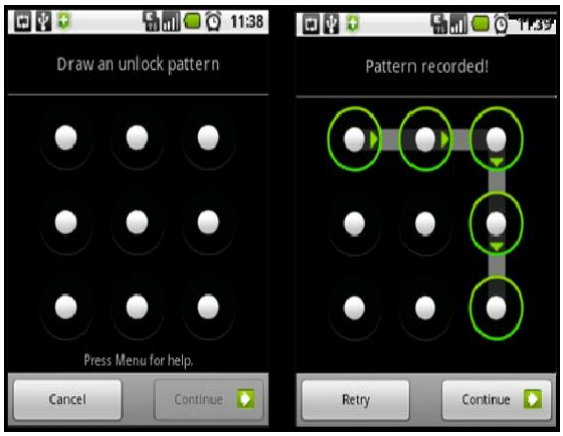

Fig.1: Layout of the password pattern Authentication system

2. Existing System

Existing System is based on implicit authentication approach that enhances password patterns with an additional security layer, transparent to the user .They have proposed security critical authentication model for the smart phones, which is purely based on the individuality of the password combinations and ease of access. This pattern uses different shapes which are used to prevent shoulder surfing harm. Different shapes are used to change the password pattern of user at runtime according to the arrangement of dots shown to the user. When user select random number series as pass code .The pattern is displayed on the device and then unlocks the Device. The graphical shapes are randomly select by the device. When user starts application, then graphical shape are shown

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

randomly which was same as selected by user during registration process. During verification user selects random number sequence. When user enters the number sequence as password the pattern was displayed on the device. If the sequence which the user selects is matched with the set of system generated pass code then the user is authenticated otherwise user have to choose sequence again for authentication. The front end proposed model has been written in HTML language. The first step leads the application towards the selection of the random shape selection, which is reproduced on screen where the user enters the prototype password. If the entered pattern password matches the pattern password created at the time of registration, the user gets authenticated and the grapple opens.

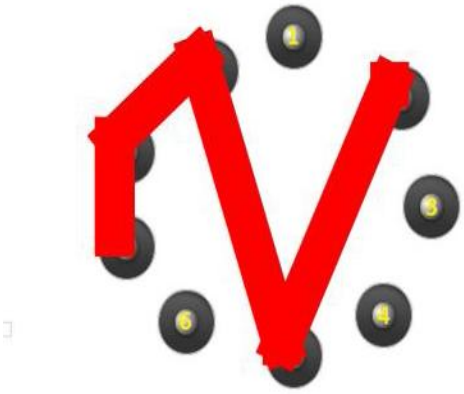

Fig.2: The circular shape with pattern drawn

3. Proposed System

Time user has to show their retina image in front of the touch screen which is recognized and save during authorizing phase. This system provide protection against shoulder surfing attack, dictionary attack, extreme force attack using text password as well as graphical password. In this system we are going to design a complete authentication system which is used to resist the all unauthorized attacks from any source The vulnerabilities of this method have been well known. One of the main problems is the complication of recalling passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember, disastrously, these passwords can also be easily guessed or broken. The Retina pattern biometric password used on Android devices is prone to the guessing attacks.

In my proposed System, I have used direction sensor for drawing the pattern without touch the smart device .Depending on product variant, the sensor provides either a speed and direction signal at the interface pins or two speed signals related to the switching of the two Hall elements. A Context class is responsible for managing the because of its somewhat elusive objective of preventing data structure on which Concrete Strategies operate. Unwanted application behaviour instead of enabling wanted computer behaviour.

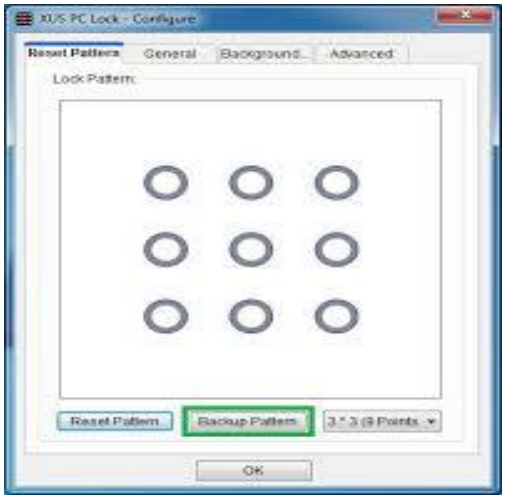

Fig.3:Pattern locking model

4. Methodology

Most Android-powered devices have integral sensors that live motion, orientation, and varied environmental conditions. These sensors area unit capable of providing information with high preciseness and accuracy, and area unit helpful if you wish to watch three-dimensional device movement or positioning, otherwise you need to watch changes within the close surroundings close to a tool. In my proposed System , I have to used the methodology direction sensor for drawing the pattern without touch the smart device in the 3*3 grid points along with biometric recognition technique. In this paper I have to suggest "RETINA PATTERN" for secure access and also prevent data or information from misuse. This method involves two steps:

First step is to recognize the retina of the user using "acknowledgement Technique" and save that image in a database.

Second step is to draw the pattern by using the retina of the user .The first process can be done by using the retina scanner which is shown in figure3.The retina of the user can be scan and recognize with the help of the above scanner. If the

Retina image can match the existing image of the retina saved at the time of registration. If the matches present then will go to next step to draw the pattern in the 3*3 grid points using the direction sensor without touching the screen by the finger. The second step include draw the pattern using the finger of the hand without the screen .this can be done by using direction sensor . First

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

show the retina image in front of the scanner it will scan and fix some measurement based on default settings which shows in the figure4, then recognize the retina image because every people have unique identity about their retina.

Fig.4: Scan and recognize the retina

Internal hardware like accelerometers, gyroscopes and proximity sensor square measures utilized by some applications retort further user actions. As an example, adjusting the screen from portrait to landscape counting on however the device is destined. Applications will more send notifications to the user to tell them of relevant information, like new emails and text messages

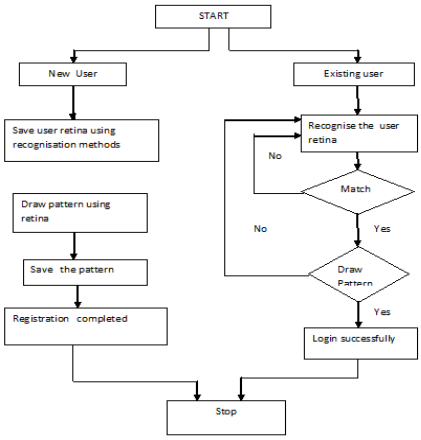

Fig.5: Architecture Diagram of the system

If someone can access others mobile without their permission that time first recognize the retina of that person using recognition mechanism and to check whether the current image is similar to existing one or not .If matches not found means the user not allowed to next process .If matches will be available then move on next step to draw the pattern using their retina by seeing and simply join the grid points to form pattern. If the drawn pattern is match to the stored pattern then the user will be allowed to access the device or otherwise not allowed. The access can be denied if any one of the identification is wrong. Both of the matches must be necessary for a successful login. The first conditions are not contented means then not allow to login. The retina images first captures and scan using the recognition technique that image is similar to old one, the user can be allowed for second process. The user should draw the pattern with their finger but not touch the screen .This must be done by using the direction sensor. The pattern automatically drawn at the knowledge of the user directed the finger.

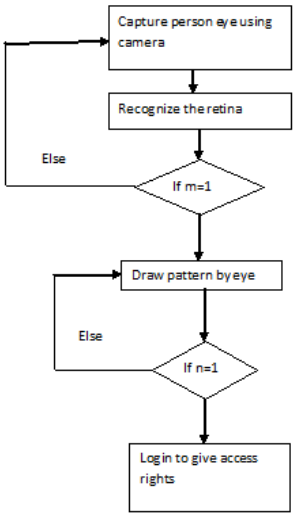

Fig. 6: Flow chart for the proposed system

In figure 6, shows the flow chart for capture the eye using the front camera and scan that image grab the retina then it can be recognize the image and find out matches in the existent saved image, this can be done by using two variables m and n. If m=1 then the user can allowed to second process (draw the pattern point out by the finger). The condition is false it will terminate .pattern can be drawn by the user that will also match to the saved one then only user allowed for the access.

5. Conclusion

The proposed scheme has been evaluated as effective, robust, ease of access and wide flexibility of the scheme for the various smart phone programs. The proposed scheme has been evaluated under various situations. The future work of this paper is to enhance the security level and try to overcome the drawback and limitation of the proposed system. A new scheme can be developed following design and pattern schemes with different methodology.

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

References

[1] Smart Authentication for Smart Phones by Arpit Agrawal Ashish Patidar Assistant professor, Department of Computer Engineering Institute of Engineering & Technology, Indore, India.

[2] Authentication Using Graphical Password by Mayur Patel1, Nimit Modi2 1Department of CE Sigma Institute of Engineering, Baroda, India 2 Assistant Professor Department of CE Sigma Institute of Engineering, Baroda, India .

[3] A Review on Knowledge-Based Authentication Mechanism Using Secure Persuasive Cued Click-Points By Naresh D. Kale1, Prof. V. A. Chakkarwar2 1PG Scholar, 2Professor, Department of CSE Government college of Engineering, Aurangabad, India.

[4] Enhancement of the Security of Pass-Go Pattern Password Using Shuffling Grid-Shapes by Deepika jyoti, Dr.Amandeep Verma M.tech student, Dept. of CSE., Punjabi University, Regional Center for IT and Management, Mohali, India Assistant Professor, , Dept. of CSE., Punjabi University, Regional Center for IT and Management, Mohali, India .

[5] Continuous Touch screen Mobile Authentication Using Several Gestures by Mr.S.M.Sangave Mr.B.A.Chaugule Department of Computer Engineering, Dnyanganga College of Engineering & Research, Narhe, and Pune, India.

[6] Qiang Yan, Jin Han, Yingjiu Li, Jianying Zhou, Robert H . Deng,"Designing Leakage-Resilient Password Entry on Touch screen Mobile Devices" Cryptography and Security Department, Institute for Infocomm Research, Singapore. ASIA CCS'13, May 8–10, 2013.

[7] Tao Feng, Ziyi Liu, Kyeong-An Kwon, Weidong Shi, Bogdan Carbunar, Yifei Jiangz and Nhung Nguyen, "Continuous Mobile Authentication using Touch screen Gestures" School of Computing and Information Sciences, Florida InternationalUniversity, 2011.

[8] Ajinkya Kawale," Fingerprint based locking system", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013.

[9] Tobias Stockinger, "Implicit Authentication on Mobile Devices", the Media Informatics Advanced Seminar on Ubiquitous Computing, 2011.

[10] Lakshmidevi Sreeramareddy, Jinjuan Feng, Andrew Sears "Preliminary Investigation of Gesture-Based Password: Integrating Additional User Behavioral Features", Dept. of Computer and Info. Science Towson University.

P.Rajeswari is holding a under graduation degree in B.Sc Computer Science from Dr.Umayal ramanathan college for women and pursuing post graduation in Master of computer applications from S.A.Engineering college. This paper is a part of curriculum covered under in (MC7413) Technical Seminar and Report Writing.