ISSN:0975-9646

Smart Authentication for Smart Phones

Arpit Agrawal
Assistant professor, Department of Computer Engineering
Institute of Engineering & Technology, Indore
Indore, India.

Ashish Patidar
Department of Computer Engineering
Institute of Engineering & Technology, Indore
Indore, India

***Abstract*— since past few years there has been a remarkable rise in the popularity of touch screen mobile phone devices. With respect to the data and information that can be stored on the mobiles as well as mobiles are nowadays are also used for accessing mail and connecting to social media, it is necessary to ensure the security of the data and information that is stored on the mobiles. User authentication is an important security measure for protecting the information stored on the mobile phone devices, because these devices have a higher risk of theft. In order to prevent unauthorized access to these devices, passwords and other pattern based authentication method are being used in recent time. However, password-based authentication has an intrinsic weakness in password leakage. While the patterns are easy to steal and reproduce. In this paper, we introduce an implicit authentication approach that enhanced the password pattern with additional security layer. We provide three security checks in two steps. The three authentication methods used are time taken to draw the pattern which is a behavioral biometric authentication method, password pattern (shape) and match the angle (3 dimensions) of mobile.**

Keywords-component; password pattern; implecit authenticatio; Angle of mobile

I. INTRODUCTION

Mobile devices are becoming essential tools in modern life, which seamlessly connect human beings to each other and outer world. A mobile phone (also known as a cellular phone, cell phone, and a hand phone) may be a device that may build and receive phone calls over a link whereas on the road a large geographical area It will therefore by connecting to a cellular network provided by a itinerant operator, permitting access to the general public phone network, additionally to telephone, fashionable mobile phones additionally support a large form of different services like text electronic communication, MMS, email, net access, short-range wireless communications(infrared, Bluetooth), business applications, vice and photography. A Smartphone, or smart phone, is a mobile phone with more advanced computing capability and connectivity than basic feature phones. Early Smartphones typically combined the features of a mobile phone with those of other popular consumer device, such as a personal digital assistant (PDA), a media player a camera, and/or a GPS navigation unit. Trendy Smartphones embrace all of these options and the options of a touchscreen laptop, together with internet browsing, Wi-Fi, and 3rd-party apps and accessories. [4]In the third quarter of 2012, one billion smartphones were in use worldwide. International smartphone sales surpassed the sales figures for options phones in early 2013. As of 2013, sixty five % U.S. mobile shoppers own Smartphones. Consumers own Smartphones. The European mobile device market as of 2013 is 860 million. In China, Smartphones represented more than half of all handset shipments in the second quarter of 2012. As of November 2011, 27% of all photographs were taken with camera-equipped Smartphones. A study conducted in September 2012 concluded that 4 out of 5 Smartphone owners use the device to shop. Worldwide shipments of Smartphones topped 1 billion units in 2013 (up 38% from 2012's 725 million) while compromising a 55% share of the mobile phone market in 2013 (up from 42% in 2012). Smartphones and feature phones may be thought of as handheld computers integrated within a mobile phone, however whereas most feature phones ar able to run applications supported platforms like Java American state, a Smartphone permits the user to put in and run a lot of advanced applications supported a selected platform. Smartphones run complete software package computer code providing a platform for application developers. Based on this feature, Smartphone user can develop any programs which are customized in specific needs, and this is a most powerful advantage of Smartphone. For example, Smartphone user will search hottest building, or nearest stop. Furthermore, Smartphone user can trade their assets like stocks or use the banking service with the wireless network. The Smartphone user can send or receive e-mails, too. However, to produce these services, Smartphone wants additional personal info than feature phone, thus, it's important to stay Smartphone secure. The most popular Smartphones today are powered by Google's Android and] Apple's IOS mobile operating systems. Android is associate degree ASCII text file platform based in Gregorian calendar month 2003 by Andy Rubin and backed by Google, beside major hardware and computer code developers (such as Intel, HTC, ARM, Motorola and Samsung) that type the Open telephone set Alliance. In Gregorian calendar month 2008, HTC free the HTC Dream, the primary phone to use humanoid. The software system suite enclosed on the phone consists of integration with Google's proprietary applications, like Maps, Calendar, and Gmail, and a full hypertext mark-up language applications programmer. Android supports the execution of native applications and third-party apps that square measure out there via Google Play, that launched in October 2008 because the robot Market. By Q4 2010, golem became the popular Smartphone platform. Once it involves security, most mobile devices area unit a target waiting to be attacked. Mobile devices typically don't have passwords enabled. Mobile devices typically lack passwords to manifest users and management access to knowledge hold on the devices. Several devices have the technical

capability to support passwords, personal identification numbers (PIN), or pattern screen locks for authentication. Some mobile devices conjointly embody a biometric reader to scan a fingerprint for authentication However; a subjective survey indicates that customers rarely use these mechanisms. to boot, if users do use a watchword or PIN they typically select passwords or PINs which will be simply determined or bypassed, like 1234 or 0000. While not passwords or PINs to lock the device, there's enlarged risk that purloined or lost phones' info might be accessed by unauthorized users UN agency may read sensitive info and misuse mobile devices. so as to stop unauthorized access to those services, user authentication is needed to verify the identity of a user. Authentication is that the method of determinative whether or not somebody or one thing is, one UN agency or what he/she claims to be. The 3 ways of authentication are: one thing the user is aware of that's watchword, unlock pattern etc., one thing the user has, and one thing the user is [4]. The most common technique used for authentication is matter watchword. The accepted vulnerabilities of this technique square measure eavesdropping, wordbook attacks, social engineering and shoulder water sport. Whimsical and long passwords will build the system secure, however the most downside is that the issue of memory these long passwords. Studies have shown that users tend to choose short passwords or passwords that square measure straightforward to recollect. Sadly, these passwords is simply guessed or broken. The choice techniques square measure graphical passwords. However these techniques have their own disadvantages. Another technique is statistics, like fingerprints, iris scan or identity verification has been introduced however not nonetheless wide adopted. The foremost disadvantage of this approach is that such systems are costly and also the identification method is slow. There square measure several graphical positive identification schemes that square measure planned in recent time. However most of them suffer from shoulder aquatics that are changing into quite massive downside. There square measure graphical positive identification schemes that are planned that square measure proof against shoulder-surfing, however they need their own drawbacks like usability problems or taking longer for users to login [5]. During this work we tend to are attempting to boost the safety by implementing multi-level authentication methodology. In this, we tend to square measure victimization 2 authentication classes that square measure one thing user is aware of and one thing user is. That is straightforward to recollect and can't be simply cracked or unseaworthy.

II. LITERATURE SURVEY

With the introduction of the Android operating system for mobile phones, an alternative to PIN-authentication on mobile devices was introduced and widely deployed for the first time. The password pattern, similar to shape-based authentication approaches like Draw-a-secret or Pass Shapes, enables user authentication by drawing a shape on the screen. The shape consists of an arbitrary number of strokes (or lines) between nine dots as shown in figure 1.

In a study by Clarke N.L. [2], 41% of their respondents expressed concerns with respect to PINs and alphanumeric passwords, supporting the need for alternative authentication techniques. In comparison to these approaches, shape based authentication better supports the way the brain remembers and stores information. The shape can be remembered as an image, therefore exploiting the pictorial superiority effect. Additionally, since the pattern is drawn manually in exactly the same way every time and repeated regularly, the user's motor memory further improves the memorability. This effect was shown to be effective [7], even when the shapes are performed by the user's gaze [8]. Despite its manifold advantages, this approach has major drawbacks, the most important one being security. Drawn passwords are very easy to detect on [8], which makes shoulder surfing, a common attack in public settings, a serious threat. Other attacks include the infamous smudge attack, in which finger traces left on the screen are used to extract the password. Due to its weak security properties, this authentication approach does not fully meet the requirement of adequately protecting the user's data stored on the device. Nowadays, not only private but also valuable business information is stored on the user's handheld [9]. Therefore, resistance to attacks is a major concern when designing respective authentication systems.

Apart from "something you know" authentication schemes, biometrics has been an often used alternative. According to Wood there are two types of biometric authentication approaches, physiological and behavioral biometrics. Physiological biometrics relies on "something the users are". In [10], Sonkamble et al. Presently an over-view of different possible features, including the user's fingerprint, face, hand geometry, voice or iris as physiological biometrics. In [11], multiple biometric features are combined to implement a person identification system. Biometric authentication systems on mobile devices were, for instance, using face and hand features. In general, however, they require additional hardware (e.g. Fingerprint scanners). Behavioral biometrics, on the other hand, is more commonly used for continuous authentication. As the term behavioral implies, these approaches are based on the users' behavioral cues and authentication may happen implicitly. Exemplary cues are the user's gait, location information or keystroke patterns. Their authentication system is based on multiple cues such as location information or communication. These features are combined with cloud computing to reduce the energy consumption of the mobile device [6]. The approach presented in this work employs additional behavioral biometrics, the way a user performs the password pattern, but immediately authenticates the user. Furthermore, we combine behavioral biometrics with the input of graphical passwords and match the angle of mobile.

Biometric authentication such as face recognition, fingerprints and iris scans have been introduced. But these techniques not widely adopted. These techniques have own disadvantages, such systems, process can be expensive and the identification process can be slow.

III. METHODOLOGY

Android is AN OS supported the UNIX system kernel, and designed primarily for touchscreen mobile devices such as Smartphones and tablet computers. ab initio developed by robot, Inc., that Google backed financially and later bought in 2005, robot was undraped in 2007 together with the creation of the Open phone Alliance a pool of hardware, software, and telecommunication firms dedicated to advancing open standards for mobile devices. The initial publically accessible Smartphone running robot, the HTC Dream, was free on Gregorian calendar month twenty two, 2008. The interface of Android relies on direct manipulation, mistreatment bit inputs that loosely correspond to real-world actions, like swiping, tapping, pinching and reverse pinching to govern on-screen objects. Internal hardware like accelerometers, gyroscopes and proximity sensors square measure utilized by some applications to retort to further user actions, as an example, adjusting the screen from portrait to landscape counting on however the device is destined. robot permits users to customize their home screens with shortcuts to applications and widgets, which permit users to show live content, like emails and weather info, directly on the house screen. Applications will more send notifications to the user to tell them of relevant info, like new emails and text messages.

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. as an example, a game would possibly track readings from a device's gravity device to infer complicated user gestures and motions, like tilt, shake, rotate, or swing. Likewise, a weather application would possibly use a device's temperature device and wetness device to calculate and report the temperature, or a travel application would possibly use the geomagnetic field device and measuring device to report a compass bearing. The mechanical man platform supports 3 broad classes of sensors:

3.1 Motion sensors

These sensors measure acceleration forces and rotational forces along three axes. This category Includes accelerometers, gravity sensors, gyroscopes, and rotational vector sensors.

3.2 Environmental sensors

These sensors measure various environmental parameters, such as ambient air temperature and Pressure, illumination, and humidity. This category includes barometers, photometers, and Thermometers.

3.2 Position sensors

These sensors measure the physical position of a device. This category includes an orientation Sensors and magnetometers.

You can access the sensors service available on the device. With the help of motion sensor we get the X, Y and Z rotation angle. Figure 1 shows that, In the particular mobile rotation the corresponding change in X, Y and Z value. Means When we rotate the mobile along x axis, then the value of x is change and similar to rest of two.

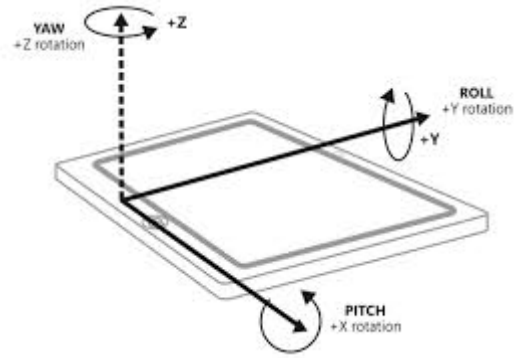

Figure 1. Show the rotation of angle.

IV. PROBLEM DOMAIN

The purpose of authentication is to ensure that access is only given to an authorized person or persons. Everyone store their essential information in mobile device like banking detail, personal diary and other official data. Whenever your mobile device has lost or misplace. Your information may be leaking. There are password is used to secure mobile device access from unauthorized person. Currently used password is not more, secure. Most common methods used for authentication is text password. But this not secure because of password leakage. Studies have shown that user tends to pick short password or password that is easy to remember. Password like drawing pattern is easily traced by someone. Biometric authentication is also used. There are two types of biometric authentication approaches, Physiological biometric and behavioral biometrics. In physiological generally face recognition and fingerprint scan have been introduced, But this is not widely used. The major drawback of this approach is that such a system can be costly and the identification processing can be slow. Behavioral biometrics general keystroke analysis has been used. Till now introduced authentication method is based one single authentication. And some is based one multi-factor authentication, but is based on serial way. It takes time to process and unlock. Hence, the problem is that some authentication is easy to trace and some have processing is very slow that is not widely used.

V. PROPOSED SYSTEM

In this paper, we provide a flexible way for authentication to overcome problems like slow unlocking process, easily traceable password, and extra sensor required like pressure. We perform three security checks I two steps, which is password pattern, time taken to draw password patterns and the angle of the mobile phone. At the First security check we match the angle of the mobile. In this, firstly user has to match the correct angle for unlocking the mobile that is X, Y, Z co-ordination. And this is calculated on the base of rotation of mobile. The option is available to choose the number of angles are included in the password. The user wants to select 1 angle, 2 angle or all the 3 angles it depends on the user. When all the three angles are selected, then security will be very high. Figure 1. Shows that, In the particular mobile rotation the corresponding change in X, Y and Z value. And in the second step two security checks are

done at one time. In second security check we use the password pattern. The Password pattern is like draw-a-secret shape on the screen. The shape consists of an arbitrary number of strokes between 9 dots shows in figure 2. Along with these security checks we calculate the time taken to draw a pattern; In this we capture the time taken to draw a pattern. When a user unlocks the mobile first time, we match time taken to draw with initial time (when user changes the pattern password), and we store his/her average time of initial and first time taken to draw patterns. When the user unlocks the mobile for the second time we match them with a new one. If time is matched, then the mobile will unlock, and new average time is calculated by the system for the next login. When user changed the password pattern at that time, no time taken to draw a new shape is calculated by the system. And then again above process is performed for every new password pattern.

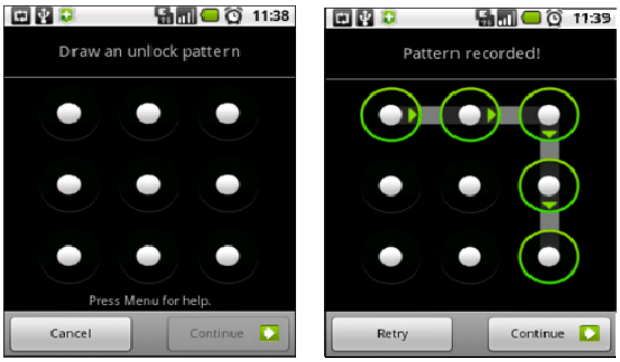

Figure 2. Layout of the password pattern authentication system.

VI. RESULTS

We collect the data from various users for continuous five days. This data is collected for the draw pattern password and time taken to draw the pattern is shown in table1. We collect data from 20 participants for the study with the age of between 16 to 30 years.

TABLE I. NUMBER OF FALSE POSITIVES, FALSE NEGATIVES, TRUE POSITIVES AND TRUE NEGATIVES AS WELL AS THE ACCURACY FOR ALL UNLOCK SCREENS

	True Positive	True negative	False Positive	False negative	Accuracy
Day 1	25	47	36	2	65%
Day 2	32	45	32	1	70%
Day 3	38	44	30	2	72%
Day 4	42	44	27	1	75%
Day 5	46	46	24	1	78%

The system was measured along the following parameters: True positives (TP): correctly accepted users.True negatives (TN): correctly rejected attackers. False positives (FP): wrongly accepted attackers. False negatives (FN): wrongly rejected users. The table 1 shows the results. The system accuracy is increased when the user become familiar with the authentication system. Accuracy is calculated in percentage on the basis of following formula.

$$\text{Accuracy} = \frac{\sum TN + \sum TP}{\sum TN + \sum TP + \sum FP + \sum FN}$$

In the results some user gets the maximum accuracy is 95%. And the low accuracy is 60%.

TABLE II. SECURITY LEVEL WITH NUMBER OF ANGLES USED

No. of Angle Consider	Convenient for user	Security	No of % user prefer to use
1 (X or Y or Z)	Easy to use	Low	30%
2 (XY or YZ or ZX)	Slightly difficult	Medium	60%
3 (XYZ)	Difficult	High	10%

The table 2 shows the security level depends on the number of angle is used for authentication. We collect data from 20 users.When user used all the three angles, then the security is very high, but from the user convenient it is difficult to match three angles of the mobile. It takes slightly more time to match rather than, considering two angles. In the case of two angle consideration user prefers to use XY angles rather than to include Z with Y or X. Because Z angle required horizontal rotation, that is slightly difficult for the user. We analyze that the angle deviation is 8° is prefer to accept the angle match.

VII. CONCLUSION AND FUTURE WORK

In this paper, first we study the previous authentication method. And develop a new authentication method that is more secure than existing one, and we use a new authentication method that is matched an angle of the mobile. And also use implicit authentication method. We apply three security checks in two steps. In a first step match the mobile angle and in second step two checks draw the pattern and time taken to draw the pattern are performed. Results show the performance of the system. The future work in these is to enhance the security check at a fine level. Try to implement more security checks at one level.

REFERENCES

[1] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, Heinrich Hussmann, “Touch me once and I know it’s you! Implicit Authentication based on Touch Screen Patterns”, Austin, Texas, USA,May 5–10, 2012.

[2] A. Buchoux and N.L. Clarke, “Deployment of Keystroke Analysis on a Smartphone”, Australian Information Security Management Conference, In Proceedings AIMS 2008.

[3] Shari Trewin, Cal Swart, Larry Koved, Jacquelyn Martino, Kapil Singh, Shay Ben-David, “Biometric Authentication on a Mobile Device: Study of User Effort, Error and Task Disruption”, ACSAC ’12 Dec. 3-7, 2012.

[4] K.Nivetha, M. Muthumeena, R. Srinivasan “Authentication Mechanisim For Session Passwords By Imposing Color With Text’’, International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 5, September- October 2012.

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

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

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

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

[9] 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.

[10] David Kim, Paul Dunphy, Pam Briggs, Jonathan Hook, John Nicholson, James Nicholson, Patrick Olivier, "Multi-Touch Authentication on Tabletops", CHI 2010, April 10 – 15, ACM Press (2010), Atlanta, Georgia, USA.

[11] Sausan Yazji, Xi Chen, Robert P. Dick, Peter Scheuermann, "Implicit User Re-Authentication for Mobile Devices", In Proceedings UIC 2009. Springer (2009), 325-339.with a ratio of quantities and units. For example,write "Temperature (K)", not "Temperature/K".