Volume 5, Issue 4, April 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Smarter Method for User Authentication in Mobile System

[1]Malika Verma, [2]Monica Sood
[1]Department of Computer Science, Lovely Professional University, Phagwara, Punjab, India
[2]Department of Information Technology, Lovely Professional University, Phagwara, Punjab, India

Abstract - User authentication is an important issue that needs to be taken seriously especially in case of smart phones where the statistics say that almost half of smart phone users use no authentication system since they need to unlock their devices quite frequently and that complex passwords are difficult to remember and time consuming while entering each time they need to log in. Other issues such as unauthorized access in case of password hack also need to be considered for better security. Biometrics claim to be more secure way for authentication purposes as physical and behavioral traits of a user are difficult to imitate just like writing your signature of fingerprints. This paper discusses the existing user authentication methods for smart phones, and current statistics of user authentication in smart phones explaining the reason why people do not like to have any authentication mechanism on smart phones despite having sensitive data and other confidential accounts logged in. A new user authentication method based on graphical password and behavioral biometrics has been proposed in this paper which is expected to be easier, secure and faster at the same time.

Keywords – Behavioral biometrics; Graphical Password; Password input mechanism; Smart phone authentication; User authentication.

I. INTRODUCTION

In digital world, the key to open any lock or a door is traditionally a password. Theoretically, it provides high security, as the only place to keep this secret key is user's mind. But, in practice, human mind is an awful place to remember complex passwords. People usually forget complex passwords. More the complexity more is the security but at the same time, more are the chances to forget. To recall, some people write down their passwords at places or use same password for multiple accounts. Even if the password is complex, attacks like key logger, social engineering or shoulder surfing are commonly being used.

A. Graphical passwords

When it comes to smart phones, graphical passwords are also very common. They are designed to make passwords more memorable. They serve as a solution to the remembering problem of traditional passwords. These include methods like drawing a pattern, locating some images, etc. They are easier to remember and recall as compared to traditional passwords.

B. Biometric Passwords

Biometric passwords are based on the concept of what a user possesses. Unlike knowledge based, which includes traditional and graphical passwords, this type of password work on user's physical characteristics or habits that are unique to a person and are very hard to imitate. It is very difficult to find similar biometric characteristics in different persons. These can be broadly classified as:

- Physical Biometrics- It includes the physical characteristics of a user like fingerprint, face recognition, iris scan, voice, size of palm etc. There usually require special hardware to be implemented for scanning and recognizing a user's physical traits.
- Behavioral Biometrics- It includes the behavior and habits of the user like the speed of typing, walking, speaking etc. These are just like writing your signature. It is difficult to write someone else's signature.

C. Security habits of smart phone users

The number of smart phone users is increasing swiftly, worldwide. Whether it comes to social networking, online banking, storing private data, the frequency of the usage of smart phones grows the call for stronger device protection method.

According to Info Security Magazine Report in 2012, More than half of Smartphone and tablet users did not perform the most basic security protection measure, such as password-protecting their devices, despite having them connected to sensitive online accounts and applications. This clearly shows that security does not coincide with usability when it comes to mobile devices.

1) Available authentication methods:

Android provides various types of authentication methods in its devices by default in different devices. Apart from the default available authentication schemes, many other are available in the form of android apps on Google play store. Some of the commonly used schemes have been discussed below:

- Slide lock-This lock screen is provided by android Operating System and it provides no security. Users simply slide horizontally to unlock the screen.
- Glass lock- This lock screen is provided by Samsung. It also serves no security and is similar to slide lock but is not just restricted to slide horizontal. Users can make any gesture pattern to unlock the screen.
- Pin lock- This lock provides a digit set of numbers 0 to 9. Users need to enter a specific pin which is a sequence of digits that serves as the key.
- Password- This lock provides a set of alphabets, numbers and special characters and provides a larger sample space than the pin lock.
- Pattern lock- This lock is one of the commonly used graphical password scheme in white nine dots are provided and user is required to draw a pattern by easy dragging. Apart from these some other biometric based locks such as face lock, finger print lock, voice lock etc. are also available in smart phones.

2) Current statistics

With the change in time and awareness among people, especially the youth, the results have improved and a change can be seen in the security habits of people in their smart phones. Some mobile authentication based questions were asked to people about their choices and preferences.

- 37% people had no password on their device, the reasons for which were given saying it consumes a lot of time each time they need to use their device. Some said they were not good at remembering passwords and some gave some other reasons.
- Out of the remaining 63% people, who had authentication schemes on their devices, 56% people use pattern scheme for authentication saying that it is much faster and easier to remember as compared to other authentication schemes.
- These poor security habits have likely come about because typing passwords on mobile devices is difficult and time consuming and so people prefer convenience over security.
- More than 30% people said that they often mistype their passwords because of small keys and ultimately remove password because of frustration. The inconvenience is greater for people who have put strong and complex passwords ultimately ending with people choosing easy and weak passwords or no passwords at all.
- More than 60% people reported that they need to unlock their devices for more than 15 times on an average daily. And the inconvenience caused for typing passwords is a big issue. 90% people agreed that they wish there was an easier way of authentication for mobile devices.

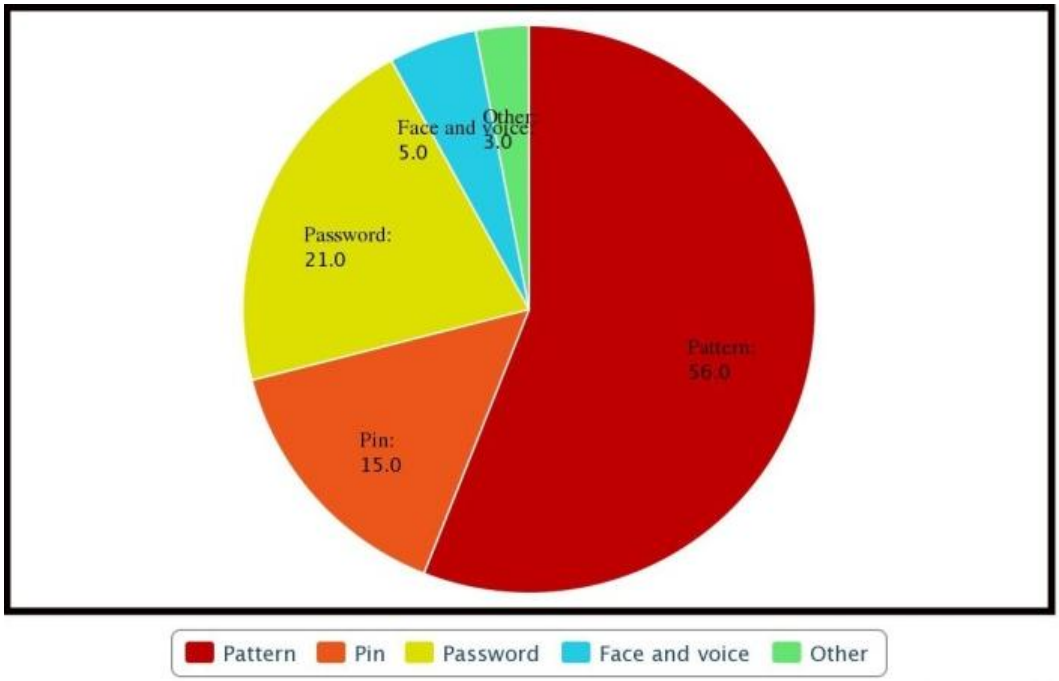

Fig. 1. Type of authentication method used (Survey)

The statistics of what users said when they were asked to tell how many times they need to unlock their smart phones on an average daily have been shown in figure 2. Most of them reported that they unlocked their smart phones for more than 15 times on an average daily.

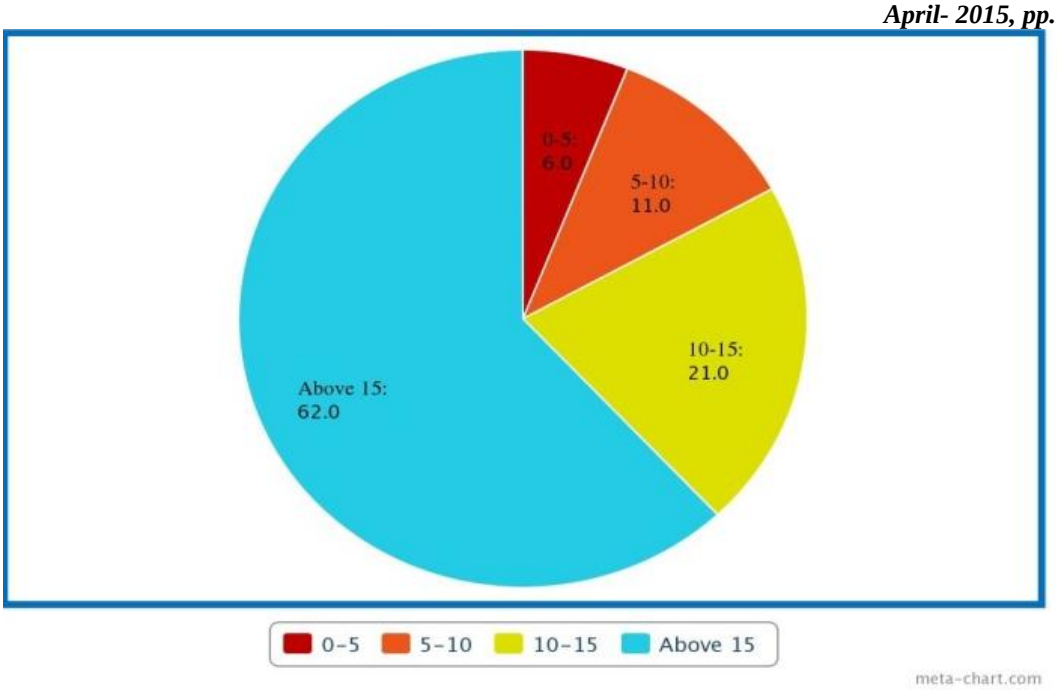

Fig. 2. Frequency of unlocking smart phone daily (Survey)

The results in Figure 1 and Figure 2 show that easier and faster way of authentication is preferred when it comes to mobile devices that are used very frequently. People prefer pattern lock for authentication which provides one million key spaces. However, if user chooses an easier pattern for the sake of convenience, security becomes weaker and if strong complex patterns are chosen, it becomes uncomfortable. As a result, there is a need of having an easier, faster and smarter way for authentication.

II. SYSTEM DESIGN

For providing a smarter way of authentication, in the terms of simplicity and security at the same time, a behavioural biometric based user authentication scheme has been proposed. The behavioural factors would be measured simultaneously while pattern is being drawn. This includes four main factors:

- Velocity 'V' while drawing the pattern.
- Pressure 'P' exerted on the touch screen while drawing the pattern.
- Portion 'G' of the screen where pattern is being drawn.
- Area 'A' covered by the thumb or finger of the user while unlocking the device.

A. Pattern input mechanism

As the user tries to unlock screen, and makes pattern on the glass lock screen of the device, the recording of the pattern begins based on the pixel values of the touched area. No concept of grid is used in this methodology. Instead, a string S is generated dynamically according to the traced path the user draws. A similar concept as in YAGP is used for string generation. A character is concatenated to the string depending upon the pixel value of the position in the path relative to the last pixel position traced. Since high resolution screens provide large number of pixels, some fixed number of pixels would be skipped for each concatenation in the string.

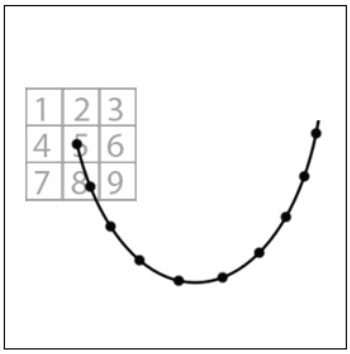

Fig. 3. Pattern to string mechanism

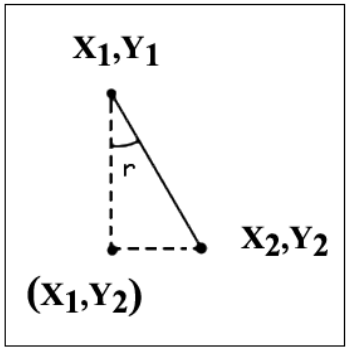

Fig. 4. Identifying the angle

A sample pattern drawn by the user is shown in figure 3. The corresponding string S can be generated using direction of pixel in comparison to last major pixel depending upon number of falling of next major pixel. In the pattern drawn in figure 3, the first letter of string S would be 8. Now the invisible box would move to next major pixel and the same process continues and numbers start appending in the S.

The methodology for identifying which number is to be chosen from the string generating list to be concatenated in string S, can be seen in figure 4. This generates three possible cases.

- If $(x_2-x_1>y_2-y_1)$, then r>45 and S=S.6
- If $(x_2-x_1<y_2-y_1)$, then r<45 and S=S.8
- If $(x_2-x_1=y_2-y_1)$, then r=45 and S=S.9

B. Comparing mechanism

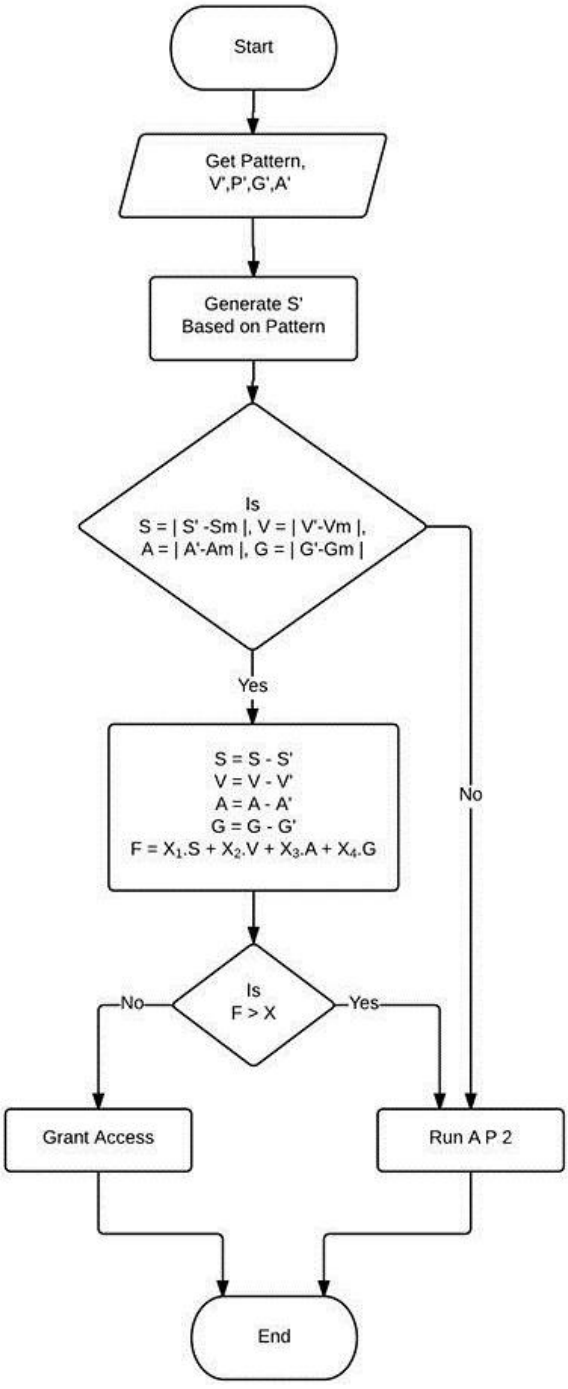

Fig. 5. Flowchart for comparing mechanism

Each user would have an already saved pattern of unlock while registering with the system. A string S would be present with the database of the system with which the new string S' is to be compared for authentication. Along with this, other factors i.e. velocity, area, position and pressure would be saved with the device.

If incase, the authentic user is unable to redraw the same pattern, another authentication procedure AP2 would run that has been discussed in section 2.3. The flowchart for comparing mechanism can be seen in figure 5. The string S' is generated depending upon the pattern drawn. It is then compared with the stored string S. If the pattern matches, rest of the factors are compared in the same manner keeping a tolerant margin value. Each factor may be assigned a specific fuzzy membership function that best suits the human habits for better comparison. This may vary from user to user and can be made adaptive in future. As the habits of users may vary with time, the algorithm can be made to adapt these changing habits with the concepts of neural network and thus the system can be made more intelligent and smart. The concept of clustering may be used to compare the pattern based on updated data that has been collected and added to the cluster in database during each login. For comparison of pattern S, any string matching algorithm may be used. As soon as the pattern gets matched with the saved one, instantly access of device is given. Users do not need to press any okay button or so for the same. The position, pressure, area and velocity may be calculated and recorded at the same time while the pattern is being drawn and is compared with that of stored values. Along with this, one final comparison is done that includes combining all the authentication factors altogether so that even if user could not redraw the pattern exactly the way it is stored, still the access is provided based upon other authenticating factors.

Authentication process 2, AP2 is another concept that makes the use of user's recall ability of his own activities with the device for authentication purposes. Only a valid user may be possible to answer the questions correctly based on its own activities for say last week. This process is more time consuming than the main gesture based process discussed in figure 6. Once all the parameters match individually, F' is calculated based on the synaptic weights of each parameter x_1, $x_2,\ldots x_n$. If this matches with the stored F, access is granted else AP2 runs. AP2 i.e. Authentication Process two has been explained in section 2.

C. Authentication Process 2

If incase authorized user is unable to draw the pattern in the same manner by mistake, a set of questions based on the user's own activity in the device can be asked. These questions may be related to the applications used in the smart phone in last one week period.

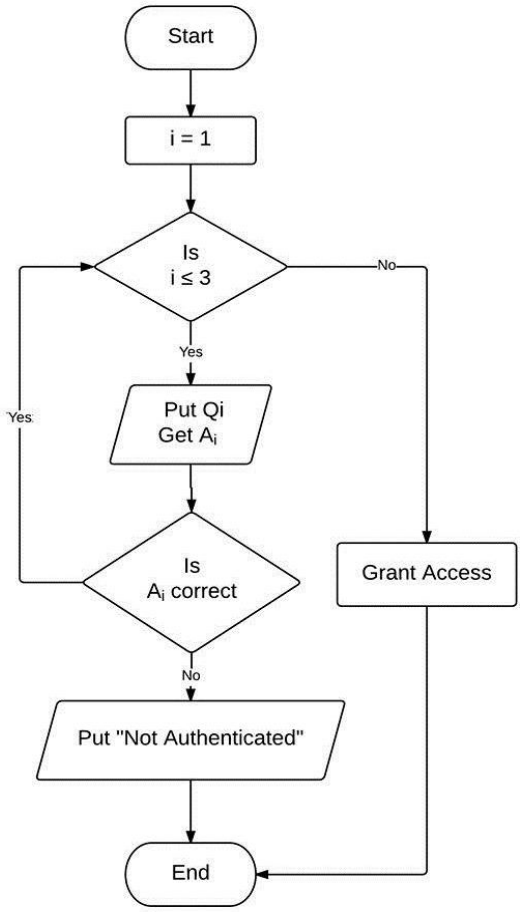

Fig. 6. Flowchart for Authentication Process 2

These memory based questions can only be answered correctly by the authorised user itself who has been using the smart phone. A set of questions Q_i, atleast three in number can be randomly asked to the user with a list of correct answers A_i associated to each. These questions may be like, "Did you call abc in last one week?" The flowchart in figure 5 explains the same process.

III. EXPECTED OUTCOME

The proposed system is expected possess following qualities:

- Easy to remember: Easy to remember so that the problem of forgetting passwords is solved and users do not remove their passwords in frustration. Since the proposed method does not contain any textual password to be remembered, this quality is expected.
- Fast and Quick: The system must be fast and quick so that the problem of users complaining about the time taken while authentication is solved. The proposed system is graphical based, so is expected to be quick.
- Difficult to hack: The system must be difficult to hack as biometrics cannot be copied, an unauthorised user cannot possess same gesture habits as authentic user and illegal access can be reduced. Also since biometrics cannot be observed or seen while drawing a pattern, it becomes difficult to hack.
- Cheaper in terms of cost: The system is expected to be cheaper as compared to physical biometric based systems that require special hardware like fingerprint scanner and other physical trait scanners that cost high.
- Adaptive of user's habits: The system is expected to learn and adapt user's changing habits with time by implementing a self learning algorithm which can be designed on clustering basis, in future.

IV. RESULT

Fig. 7. Recording a Pattern

As it is clear from the above results, time, area and the pattern drawn by the same user is almost similar each time. When the same pattern was made to be drawn by another user, different results were found saying where time played a huge role that was 1462 millisecond which is almost double of required one. Moreover, unauthorized used could not redraw the same pattern on same area and with similar pressure. This proves that behavioral biometrics play a big role in this field and can be used for authentication purposes. Even if the pattern is being shoulder surfed and known by some other invalid user, access cannot be granted as the pattern drawing habits of a different user won't match with the authorized one. The user is asked to draw the pattern for atleast four times so that a cluster can be made depending upon the average values and these values are then compared each time user wishes to login. This data was recorded in multiple devices with different users and one of the example is being shown in figure 7.

V. CONCLUSION

There is a strong need of a mechanism that is quick, secure and easy at the same time i.e. a smarter way of authentication is required. In this paper, a behavioural biometric based password scheme has been discussed that can be implemented on graphical pattern drawing just like a swipe performed on glass lock. The objective of this study is to provide a secure, cheap, easy and quick user authentication scheme that has been proposed in this paper. It is expected that the proposed solution would serve smart phone users worldwide.

REFERENCES

[1] Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang, and Xiyang Liu, *YAGP: Yet Another Graphical Password Strategy*, Annual Computer Security Applications Conference, 2008

[2] Imran M. Khan, Imama, K.M. Ushama, M. Abiniu , Lai Weng Kin and C. P. Lim, *Evaluation of Classifiers in a Pressure and Latency-Based Typing Biometric System*, 4th International Conference on Mechatronics (ICOM), 17-19 May 2011, Kuala Lumpur, Malaysia, 2011

[3] Kwang Il Shin, Ji Soo Park, Jae Yong Lee and Jong Hyuk Park, *Design and Implementation of Improved Authentication System for Android Smartphone Users*, 26th International Conference on Advanced Information Networking and Applications Workshops, 2012

[4] Neil Smyth, Techotopia, *Android 4.2 App Development Essentials – First Edition*

[5] Stan Z. Li, *Encyclopedia of Biometrics (*Springer Science & Business Media)

[6] Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang, A *Graphical Password Based System for Small Mobile Devices*, IJCSI International Journal of Computer Science Issues, 2011

[7] Xi Zhao, Tao Feng And Weidong Shi, *Continuous Mobile Authentication Using A Novel Graphic Touch Gesture Feature*, Applications and Systems (BTAS), IEEE Sixth International Conference, 2013

[8] Ziming Zhao, Gail-Joon Ahn, Jeong-Jin Seo and Hongxin Hu, *On the Security of Picture Gesture Authentication*, 22ND USENIX Security Symposium, 2013

