

New Security Login System Using Tap and Gesture on Smartphone Touchscreen

KiHwan Kim*, Bruce Ndibanje*, SuHyun Park**, HoonJae Lee**

*Department of Ubiquitous IT, Graduate School of Dongseo University

**Division of Information and Engineering, Graduate School of Dongseo University
Sasang-Gu, Busan 617-716, Korea

ghksdl90@naver.com, ndibanje.bruce.phd@ieee.org, subak@dongseo.ac.kr, hjlee@dongseo.ac.kr

Abstract— The usage of smartphone nowadays has been increasingly and most of people in the world use it. Following this development a wide variety of applications for mobile phones have been created. After all, most people use the smartphone to browse social networks, listen to music, play games, make memos upload photos to Instagram, accessing banking services, as well as data sharing through cloud system. Therefore, most important thing is to understand what kinds of information exist in smart phone. One of the most important aspects of Smartphone is security and how to protect data in smartphone from unauthorized users. To do so of the easiest way is coding of mobile phone. Most people know this method. There are many kinds of smartphone lock. For example, 4-digit number, pattern lock and fingerprints etc. This paper focus on login system based on smartphone. In this paper, we present a new security technique using tap and gesture method to protect data and devise. This method is implemented etc. testing on smartphone to check the feasibility. Furthermore, we extend this method to the cloud system.

Keywords— *smartphone; touchscreen; gesture; tap; cloud.*

I. INTRODUCTION

Today, most people are using smartphones has provided the necessary information on health status, online banking, real estate life [1]. In recent years, most smartphones can store your personal photos and videos to a private cloud account. However, if the banking and cloud Login outflows and the risk of personal information private and confidential data is leaked [2], it can lead to financial losses in the worst case [3][4]. Has recently proposed a cash payment structure improvement and use with a variety of online businesses, young people appeared to be using your smartphone as a most active [5]. However, a variety of attacks, many institutions and individuals saw the damage [6][7], trying constantly to prevent various financial damage [8]. In addition, high-speed communications technology and new hacking methods, the limit of detection technologies and various practical difficulties is a challenge to solve. So easy that you enter the number and direction through to provide authentication services by using the keys and directions to the cloud service sign quickly and tried to improve security.

II. BACKGROUND

Computer Input and output method is robust and diverse and colorful. But computers are not only available in a limited area. But Mobile is available free on the go portability features.

However, the space for input and output cannot but present an uncomfortable part for use in the same way as a computer, so limited.

A. Passwords Consisting Only by Numbers

Past users were simply prefer. They used a simple number passwords, and ease of use in mind without the use of complex passwords. However, using a computer events occur which access to confidential information or cause a loss of importance and began to instructions of the security is created. CPU performance is increasing at a faster rate spread has enough computing power as easily attack through a Brute Force Attack the number of six-digit password with only one computer in your home. All the computers there is an advantage that the authentication is possible by the password. However, the attacker also present the disadvantage of sudden attack where possible. The graphics will stay in the “second” column, but you can drag them to the first column. Make the graphic wider to push out any text that may try to fill in next to the graphic.

B. Certification

It exists as a pair with the public key private key required to verify a digital signature. You must also send your final manuscript on a disk, via e-mail, or through a Web manuscript submission system as directed by the society contact. You may use Zip or CD-ROM disks for large files, or compress files using Compress, Zip, Stuffit, or Grip.

C. OTP

The password that you use only once is called OTP. Creation and authentication methods to the S / Key system, time synchronization method, Challenge response system, including event synchronization method, there are a total of four. However, most of the OTP devices are used and the time synchronization method in recent years has used the OTP by the smart phone.

D. Pattern

The advantages that can be comfortably at regular intervals in such a manner as to draw a continuous line authentication a security is not high, but fell point exists

E. Fingerprint

The smartphone has been recently introduced is attached a device for recognizing the biometric information imposes the convenience of use.

In particular, the fingerprint for each individual will have a unique value, and the recognition is getting a lot of attention to the advantage of being convenient. But there is a problem that you cannot build a boat that fingerprint is available at all smartphones used because the high-end smartphones.

III.PROPOSED TECHNIQUE

A. Default behaviour

Select the key layout of the touch pad to give specific direction to push through a combination of numbers and vectors as the number, type and direction for granted, or how to create a new hash keys can be used to re-verification process in accordance with the number entered.

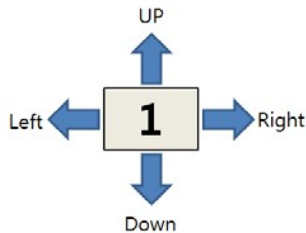


Figure 1. Numbers box and vectors combined approach

If the number is present boxes on the touch screen, press the number you want to enter in the first box. The second input value by dragging the vector for that number. Repeat this process at least four times, it is possible to authenticate a gesture has been added to the same format as the input keypad.

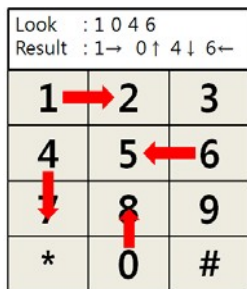


Figure 2. How to use examples and effects

If the number and 4 to release a four-digit password, enter the recipient vector bearing the number 16 kinds of values each number 0-15 and four Vector value if redundancy is allowed to obtain the following results.

$$(16 * 4)^4 = 64^4 = (2^6)^4 = 2^{24} = 16777216 \quad (1)$$

B. Application behaviour

Conventional input method only has the advantage that increases the number of cases of limited results, but the 0-9 level of safety which can be used for authentication on the Internet is difficult to ensure. Therefore, it is possible to seek a variety of input based on the advantages of a touch screen gesture recognition.

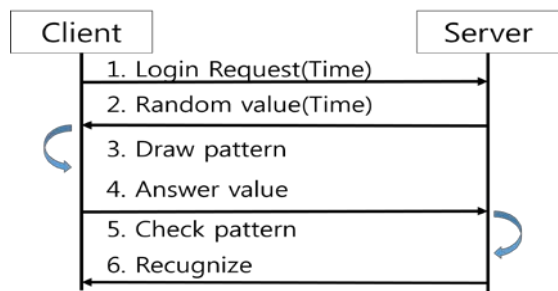


Figure 3. How to Request Certification

1) **Login Request:** Client and Server is before the membership is complete, there is another know the password. In addition to the Server sends the Client is synchronizing the time you want to sync. If the synchronization time of the two sides to share and know the password and synchronize time, where Server is the password can be attacked any time in the future because it operates as OTP and similar formats. All Client is requesting more time in the future to prevent this Server blocks.

2) **Random value:** Server is the Client to transmit any n-digit number is not possible to recognize the image. In general, the computer can not recognize the number cannot but who interactively.

3) **Draw pattern:** The user of the terminal screen, the points generated at random at predetermined intervals away from the internal to aid correct input arrangement is displayed on the screen. According to the order of the n-digit number drawn image it received from the Server to find the number of the screen. After the user input is directly transmitted to the input to the server. The data to be transmitted and transmits the Drag seaman.

4) **Answer value:** The server receives an input, there are two constraints. The first three challenges are possible. Second, recognize only one input minutes. To satisfy the condition of the two, the user's identity verification is performed.

5) **Answer value:** The server receives an input, there are two constraints. The first three challenges are possible. Second, recognize only one input minutes. To satisfy the condition of the two, the user's identity verification is performed.

6) **Check pattern:** It compares the patterns created by combining the direct image of a pattern by the user is transferred and verified.

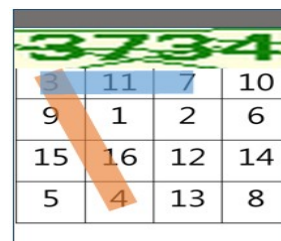


Figure 4. Draw pattern Example.

C. Mathematical approach

Either side is aware of the password and the time synchronization, information that could allow an attacker to obtain information that is required by the synchronization information and the user response time and server.

The above information is of course assuming that the defines should be encrypted transmission, but this is decrypted by the continuing attacks on and try to do the mathematical proof of how possible. If the user requests the server as the result of the n-digit value that consists of a duplicated as follows:

$$(n^2)^4 = n^8 \quad (2)$$

But people are vulnerable to a variety of memorizing a lengthy password. Also often used to duplicate or blend the information related to personal information. Therefore, the number of cases that occur when the information has a pattern of 4 digits in the example is shown below:

$$4^8 = 2^{10} \quad (3)$$

However, the pattern for use as a password encryption method increases the number of cases give a color to the pattern by the strength is too weak. Therefore, if the image of the primary RGB to adjust the intensity of the color by the number 255 for each color. Also, given the color change associated with the overlap and the starting point indicated by the input method for security vulnerability due to not separate the order of sequence of input it is possible to increase the encryption strength.

$$(n^2 \times (2^8)^3)^n = (n^2 \times 2^{24})^n \quad (4)$$

If you recalculate the number of cases relating to the 4×4 table above are as follows.

$$(4^2 \times 2^{24})^4 = (2^{(4+24)})^4 = (2^{28})^4 = 2^{112} \quad (5)$$

Color change as described in Figure 4, may also be used in a method for specifying color in advance, or through an exchange process through the false color can confuse the attacker. Also, adding a color change by adding a value of the connection portions of the straight line intersecting with each other by a pattern input, it is possible to levitate the diversity of input.

At this time, the number of cases that will intersect is too diverse, so also occur if you cross at a portion other than this point in time, complexity will be no choice but to become very large. It completed the image to send in lossless compression, resource consumption increases. Thus, send it to compress the whole Hash value, it can be replaced by extracting only specific parts. Or if a secure channel between the client and the server is not formed, a part of the image it is possible to use the AES encryption algorithm to the key value.

TABLE I. ALL POSSIBILITIES OF CALCULATION

	Vector	Basic Pattern	Color Pattern
Formula	$(n^3)^4 = n^{12}$	$(n^2)^4 = n^8$	$(n^2 \times 2^{24})^4$

N=4	$(4^3)^4 = 2^{24}$	$(4^2)^4 = 2^{16}$	$(4^2 \times 2^{24})^4 = 2^{112}$
N=8	$(8^3)^4 = 2^{36}$	$(8^2)^4 = 2^{24}$	$(8^2 \times 2^{24})^4 = 2^{120}$

Finally, it is possible to consider security related middle attack in procedures related portions to be transmitted to the server. As a countermeasure against this , if it intercepts a user's signal, the attacker when is sent to the server, using the method of transmitting transmission is divided into half the entire result value through the time delay measures the men in the meddle attack ,it is possible to take.

Applications

1) Mobile Cloud Services

The mobile suite of cloud services are all provided with a portion for free using iPhone, Android, etc. Often using pictures, automatically login to the cloud storage technology to store such movies automatically, but continued use automatic login and logout contrast due to the cyclical because it can lead to security risks caused by the loss.

2) Mobile banking services

Keypad input method has been used for initial use by entering a secret password safely to screen space with the user's input. As the computer screen, but using the public key encryption and digital signature certificate and various security methods developed thus Banking services are being commercialized.

CONCLUSION

Smartphone usage has been increased when comparing with desktop penetration usage. Most of people nowadays including aged ones prefer to use the mobile devices. In particular, the web services are mostly in high demand for the data transaction. In this regards, security is paramount requirements for the data and smartphone usage. This paper focus on login system based on smartphone. In this paper, we have presented new security technique using tap and gesture method to protect data and devise. This method has been implemented get tested on smartphone where the result has revealed that it is suitable throughout the pattern method using this mobile touch screen.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology. (Grant number: NRF-2011-0023076). And it also supported by the BB21 project of Busan Metropolitan City.

REFERENCES

- [1] Smith.: "U.S. Smartphone Use in 2015", Available: www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/
- [2] D. WAKABAYASHI (02.2014). Apple Investigating Reports of iCloud Vulnerabilities. Available: <http://www.wsj.com/articles/apple-investigating-reports-of-icloud-vulnerabilities-1409608366>
- [3] N. Perlroth. Federal Reserve Bank of St. Louis Confirms a Hacker Attack. Available: www.nytimes.com/2015/05/20/technology/st-louis-fed-confirms-hacking-attack.html?r=0
- [4] A. Kharpal:" Year of the hack? A billion records compromised in 2014",

- Available: <http://www.cnbc.com/id/102420088>
- [5] J. Marous 300 Mobile Payment and Digital Banking Trends. Available : <http://thefinancialbrand.com/41465/300-mobile-banking-digital-payment-strategic-planning-statistics/>, 2014
- [6] SUSANNAH FOX 51% of U.S. Adults Bank Online. Available: <http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/>, 2013.
- [7] Hackers steal \$1bn in series of online bank thefts says report. Available : <http://www.theguardian.com/technology/2015/feb/16/hackers-steal-1bn-in-online-bank-thefts-says-report>
- [8] Martin Arnold Hacking onslaught tests UK banks' defences. Available: <http://www.ft.com/intl/cms/s/0/3789c838-fd5f-11e4-9e96-00144feabdc0.html#axzz3bOgXDKkN>, 2015.
- [9] Kaspersky. One billion more: Kaspersky Lab counts up this year's cyber threats. Available: <http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-counts-up-this-years-cyber>, 2014.



Ki Hwan Kim

2013: BS at Dongseo University, Republic of Korea
 2014 ~ current: Master's course Dongseo University, Republic of Korea
 Research Interests: Cryptography, Information Security, Network Security



Ndibanje Bruce

2004 : BS at Ngozi University, Republic of Burundi
 2013 : MS at Dongseo University, Republic of Korea
 2016 : Ph.D at Dongseo University, Republic of Korea
 Research Interest: Information Security, Wireless Sensor Networks, Cryptography and Network Security, Side Channel Analysis



SuHyun Park

1986 : BS at Pusan National University, Republic of Korea
 1988 : MS at Pusan National University, Republic of Korea
 1999 : Ph.D at Pusan National University, Republic of Korea
 1996 ~ current : Professor of Dongseo University, Republic of Korea

Research Interests : Maritime IT, Artificial Intelligence, Intelligent System



HoonJae Lee

1985 : BS at Kyungpook National University, Republic of Korea
 1987 : MS at Kyungpook National University, Republic of Korea
 1998 : Ph.D at Kyungpook National University, Republic of Korea
 2002 ~ current : Professor of Dongseo University, Republic of Korea

Research Interests : Password Theory, Network Security, Side-Channel Attack, Information Communication/Information Network

