Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 7, No. 1, March 2019, pp. 59~67
ISSN: 2089-3272, DOI: 10.11591/ijeei.v7i1.936

Pattern lock and the app based on context, ease of use aspect in comparison

Farid Fajriana Pulungan, Dodi Wisaksono Sudiharto, Tri Brotoharsono
School of Computing, Telkom University, Indonesia

Article Info

Article historys:

Received Dec 31, 2018
Revised Jan 17, 2019
Accepted Feb 04, 2019

Keywords:

Android
Authentication
Context data
Ease of use

ABSTRACT

Smartphone has been a popular device utilized to support productivity in human life and has become an integral part of human activities such as for communication, entertainment and social interaction. Those activities can be related to the information which needs to be protected because of its high privacy. Therefore, the smartphone needs a procedure that demonstrates an ability to secure that user information. However, more protective the scheme, more difficult the usage. Based on that pattern behavior, a good security scheme which support the users for easy security feature is urgently needed. One of such kind security features is authentication feature. In that manner, the ease of use aspect for acquiring the system by using an easy authentication mechanism becomes critically important. The ease of use intended is the efficiency of interaction between the user and that security feature for doing authentication including the time needed for doing that. This study developed the app which utilizes the context data, namely Geofilock. The context data meant is the location data based on the GPS and MAC address of the Wi-Fi. The system detected both context data and determined whether the smartphone needs to show the pattern screen lock as authentication feature or not, based on the context data analysis. The functionality of Geofilock works properly as shown by less user interaction number and less time needed by the user for obtaining the access. In addition, the app is easy to operate, as suggested by the user feedback.

Corresponding Author:

Farid Fajriana Pulungan,
School of Computing,
Telkom University,
Jl. Telekomunikasi, Terusan Buah Batu, Bandung 40257, Indonesia.
Email: faridfpul@gmail.com

1. INTRODUCTION

Smartphone technology has driven the human to perform many activities for supporting their productivityas well as enjoying entertainment. However, as time goes on, problems related to how information in the smartphone can be retrieved and how it can be protected tend to grow. Essentially, this happens due to the privacy related to the accessed data and user information. The apps such as e-banking, e-mail, and social media are the example of apps which contain high privacy related to its data. Therefore, the user needs a system which can prevent illegal access by an unauthorized user into the smartphone [1]-[2].

Many authentication systems have been developed for identifying the user and preventing an illegal access to the system. Broadly, the authentication system can increase privacy protection. However, it also reduces the ease of use aspect.

The ease of use is a level in which the user can trust that the system usage can reduce the user effort for doing something [3]. Related to the system access like the pattern screen lock, the ease of use aspect still becomes a big challenge [2]. Several studies tried to handle the authentication system problem related to the ease of use aspect. Those studies used approaches such as Biometric method [4]-[6] or Context-based [7]-[11].

According to the study in [12], the environmental context is the context which is easy to be remembered and there is not any change in its infrastructure including the environment of the smartphone itself. The secure authentication system which only uses the data location as the context cannot be secure enough or cannot always identify the authorized user. It happens because the data location can be accessed by anyone physically. More threateningly, the data location based on GPS can be forged by illicit apps nowadays.

To avoid that weakness, this study utilizes the combination of Wi-Fi and GPS as the context data. Both context data are used as the parameters of the authentication including for system analysis of this study. The system is going to compare the real-time environmental context data and the context saved in the database. When the context data is matched then the system does not call the pattern lock screen function. The user can bypass the mechanism of authentication. By this way, the user becomes more pleasant to access the system.

The pattern lock screen function represents the function which shows an authentication mechanism for the user if the detected environmental context data is not matched with the saved context data in the database. By passing this function, the ease of use aspect of a secure access system can be improved.

2. RELATED WORKS

The studies related to the authentication system has been explored and there are many methods which are used for them. The comparative study of them can be examined in Table 1.

Table 1. The Comparative study of the authentication system on the smartphone

Reference	Title	Method
[4]	Face Recognition Technology Research and Implementation Based on Mobile Phone System	Convolution Neural Network, Face Detection
[6]	Unlocking Smart Phone Through Handwaving Biometrics	Accelerometer, Support Vector Machine
[5]	Context-Aware Mobile Biometric Authentication Based on Support Vector Machines	Support Vector Machine, Context data
[7]	Time Pattern Locking Scheme for Secure Multimedia Contents in Human-Centric Device	Time Pattern
[11]	Touch Me Once and I Know It's You! Implicit Authentication Based on Touch Screen Patterns	Dynamic Time Wrapping, Context data
[9]	Context Aware Mobile Application for Mobile Device	GPS, Geofence, Pattern Lock
[12]	Secure Location Validation with Wi-Fi Geo-fencing and NFC	Context data, Wi-Fi, GPS
[10]	Enhancement of VPN Authentication using GPS Information with Geo-Privacy Protection	GPS

The other feature which is more advance for authentication system has been developed widely and it differs from the standard lock screen (e.g. PIN, Swipe, Pattern). The methods used and the focus of the studies can be different from each other.

The first technique which is commonly used is by applying biometric. The biometric remains a method for identification by manipulating part of the human body as an authentication key. This approach is distinct into two physiological and behavioral types [11]. The example of the physiological biometric approach is face recognition [4]. This mode uses face as part of human body as a metric for passing the authentication procedure. On the other hand, the behavioral type of biometric approach can be seen in [5] and [6]. This behavioral approach treats the user behavioral movement as a metric for passing the authentication mechanism. The later type of biometric approach can exist in the background because the metric uses the user behavior [11]. Habitually, the biometric approach focuses on security because it implements complex processes such as feature extraction, data training, and data analysis.

The second method uses the context data. The context data is the data around the system which can be extracted by the system. It can be sensed by the sensor or another device attached on the smartphone. The example of the second approach can be considered in the studies of [7], [9], and [12]. Those studies use the context as a key to pass the authentication mechanism such as time, GPS, or Wi-Fi. The mechanism of this approach is by comparing between the presence context when user logs into the system and the other one which is saved by the system with error tolerance.

Each method displayed in Table 1 presents a weakness related to its characteristic. Time pattern has mobility defect because it requires more time to unlock the lock screen [7]. Face recognition has an imperfection as it cannot be used in every place or any condition because some place or some condition can trigger a noise which disturbs the clarification process [4]. The weakness of traditional text-based such as PIN and password is it can be attacked by using brute-force method [7].

Regarding the context, it is any information which can be exploited to describe a situation, a human, a place or a thing and it is relevant with the interaction between the human and the app [13]. The factors such as lumen, noise, communication bandwidth, or social situation become additional features of context description.

Related to the ease of use terminology, habitually, it is operated as the simplification of usability. As mentioned in ISO 9241-11 standard, the usability definition is how the product can be used by the certain user to get the specific and suitable goal with the effectiveness, the efficiency, and the satisfaction of the user related to the usage of it. The metric of usability is used for describing the user requirement, deciding the purpose of the system usage, and evaluating the usage of the system [14].

Based on [15], the security information covers 3 main purposes which are confidentiality, availability and integrity. Confidentiality is an aspect which guarantees that the information can only be accessed by an entity which has the authorization. Availability is an aspect which assures the available information which can be accessed by the entity which has an interest in accessing that information. Integrity is an aspect which ensures that the originality of the information and the information itself is not modified by an unauthorized entity. This study developed the authentication system which has an ability to be used for accessing the Android smartphone. Habitually, by using an authentication mechanism for accessing the system, all three aspects have been adopted.

This study developed the authentication system which provides an ability to be used for accessing the Android smartphone. Android is the operating system which is Linux-based and it is designed for a mobile device with touchscreen feature such as smartphones and tablets. This operating system is selected in this study to be explored because it becomes the most popular one [15]. This operating system was developed by Android Corp which has been acquired by Google in 2005. The interface of Android is the screen which can be manipulated by touching, sliding, or tapping.

By default, Android has the pattern screen lock and also Wi-Fi features. The pattern screen lock is a graphical-based authentication, as shown in Figure 1. The image-based authentication has several advantages which are not belonged by another method. It is resistant to be penetrated by using a dictionary attack, brute-force, and spyware which are easy to break text-based authentication. This method is cooperative to be remembered because the human tends to have an ability for remembering the image better than the text.

Wi-Fi is a technology for non-wired communication based on IEEE 802.11 standard. To connect into the Wi-Fi network, the device has to support Wi-Fi technology and in a covered area of Access Point (AP). Each AP allows unique identification called as SSID (Service Set Identifier) and MAC Address which become the physical address of it. When Android smartphone is connected to the AP, the device can obtain SSID and MAC address via Wi-Fi Manager.

According to location tracking, an API (Application Programming Interface) created by Google can be used to detect Android location by using GPS, mobile data, and also Wi-Fi [9]. In this study, the location variables captured from this API are a latitude and a longitude. The user location is determined by implementing the intersection of both lines.

Based on the study in [2], it shows that more than 30% of the respondents do not use a secure lock screen because they assume the feature is too complex. More than a half of respondents who use secure lock screen feel being disturbed because when they feel they are in a safe place, they still have to do an authentication procedure. Based on the information above, this study is going to develop a secure lock screen feature on the Android smartphone which can automate the unlock screen procedure when the similar context data is recognized by the Android device.

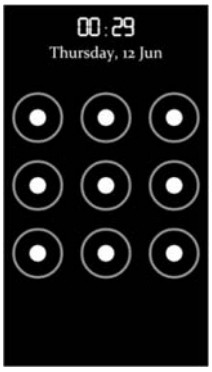

Figure 1. The pattern screen lock

3. PROPOSED SYSTEM AND METHOD

The proposed system was designed based on the traditional lock screen feature on the Android smartphone. The lock screen is unlocked automatically if the environmental context is recognized by the system. The automation described means the user does not have to input the information related to the context data which is needed by the system. By this way, the interaction needed between the user and the device can be reduced.

To make a lock screen app which can perform easier authentication mechanism than before, it needs a key variable which can be trusted by the user. This study uses context data which are GPS location-based and MAC address of Wi-Fi. The usage of these context data can vary the level of smartphone security.

To determine the system security level, the context data have to be known first so they have to be saved in a database or other structured file. The purpose of the system developed is the Android smartphone system can determine its security level automatically based on the captured context data. The process is shown in Figure 2.

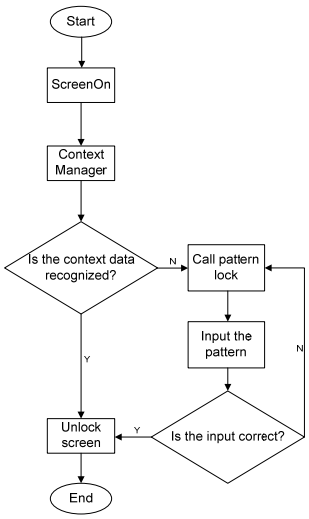

Figure 2. The flowchart of the proposed system

The function of the pattern lock will not be called if the environmental context is recognized by the system (this is the function of Geofilock). Figure 3 explains the use case diagram. The user is an actor who interacts to the MainActivity. The MainActivity can manage the pattern lock via LockSetting and can check the context by using GetWifi and GetLocation. GoogleService is an actor which gives a location data to GetLocation. ScreenOn is a service registered when the MainActivity is run. ScreenOn also acts as a receiver which captures the screen broadcast of the smartphone when the screen turns on. When the broadcast is caught by the receiver, the ScreenOn calls the functionality of GetLocfi which contains the function of ContextManager. The ContextManager itself consists of GetLocation and GetWifi which are used to detect the context data in real time and also compares between that context and the saved context. Therefore, the ContextManager also has an ability to get the saved context data from the system information storage. Next, if the context is recognized then the function of unlock screen is called. If it is unknown then Getlocfi is going to call ScreenLockActivity to shows the pattern screen lock function.

In this proposed system, there are two types of data which are used as variables to determine the decision for configuring access mechanism. Firstly, the coordinate location as the context is used to recognize the environmental context. This data has a constant value and is captured by utilizing GPS tracking. Google API service is used to support user location data and it is added by getting a fence to improve the sensitivity of point location so the error location can be reduced. Secondly, MAC address of Wi-Fi or the physical address can be counted as a unique information for addressing the AP. This unique value becomes the reason why the MAC address is used as added information.

There are two levels of a scenario which are executed by the system according to the condition around the user smartphone in real time. Level 1 is the highest one which is applied by the system. It is implemented because the smartphone position is in a place which cannot be recognized by the system. In this level, the user has to do an authentication procedure by using pattern lock screen. Level 0 is the most modest security which

is given by the smartphone system. It is given because the device system can recognize the environmental context. In this level, the user does not have to do an authentication process when the user accesses the smartphone home screen. This level can be achieved by the Geofilock app.

There are software and hardware needed for developing the proposed system. They can be followed in the next sub-section.

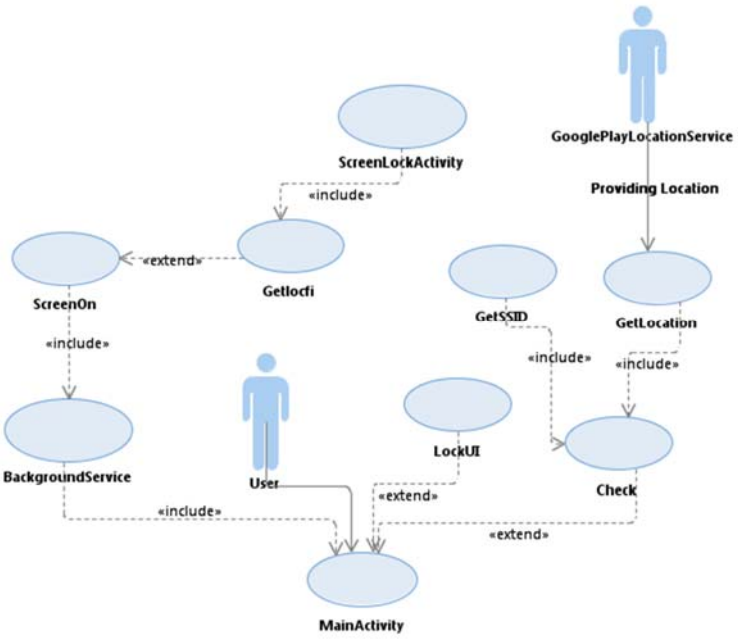

Figure 3. The use case diagram of the proposed system

3.1. The Software

The software needed for developing the proposed system are:

a) Windows 7 64-bit Operating System
b) Android Studio 2.3.3
c) Gradle Build 3.3
d) FakeGPS
e) Me.zhanghai.android.patternlock:library:2.1.2
f) Io.nlopez.smartlocation:library:3.3.1
g) com.scottyab:aescrypt:0.0.1

3.2. The Hardware

The hardware needed for developing the proposed system are:

1. The laptop which is used for making the app. Its specifications are:
   a. Processor Intel Core I5-2450M
   b. RAM 4 GB
2. Modem Andromax M2Y (Pengujian Wi-fi)
3. Smartphone MI Redmi 3 which is used for assessing the app. Its specification is:
   a. Snapdragon 616 Octa-core Max 1,5Ghz
   b. RAM 2GB
   c. OS Android 5.1.1 Lollipop
4. The minimal specification for porting the Geofilock app is OS Android 4.4 Kitkat

3.3. The Assessment

There are several scenarios which are used to assess the proposed system.

3.3.1. The Functional Assessment

The functional assessment is to know whether the app has an ability to implement the designed system produced. This assessment is performed by using MI Redmi 3 smartphone itself. The Black Box Testing and the Confusion Matrix is used to complete an assessment [16]. The Black Box Testing is used to identify the functional system succeed for running its function. Table 2 consists of scenarios with their context values, modes, and the results.

Table 2. The assessment scenario by using confusion matrix

Testing Number	Condition			The Result Needed
	Location	MAC address	Recognition Mode	
1	True	True	Location	Succeed
2	True	False	Location	Succeed
3	False	True	Location	Failed
4	False	False	Location	Failed
5	True	True	Wi-Fi	Succeed
6	True	False	Wi-Fi	Failed
7	False	True	Wi-Fi	Succeed
8	False	False	Wi-Fi	Failed
9	True	True	Wi-Fi & Location	Succeed
10	True	False	Wi-Fi & Location	Failed
11	False	True	Wi-Fi & Location	Failed
12	False	False	Wi-Fi & Location	Failed

According to the scenario, it can be presented that login is successfully done if the environmental context detected is the same as the saved context. However, it depends on the recognized mode selected. For example, if the recognized mode is related to the location, then the context which is location data detected have to be right. If a recognized mode is related to Wi-Fi, then the context which is MAC address must be correct. If both Wi-Fi and GPS location-based are used, then both parameters definitely have to be right.

To estimate the level of Recall, Precision, Accuracy, and Error Rate of the recognition, then the followed justifications are used:

a) If the prediction result is negative and the truth (based on the assessment) is absolutely negative, so the value is set as 7.
b) If the forecasting outcome is positive and the truth is absolutely negative, so the value is set as 0
c) If the prediction result is negative and the truth is definitely is positive, then the value is set as 0.
d) If the forecasting outcome is negative and the truth is definitely positive, then the value is set as 5.

Thus, the values are going to be filled into (1)-(4), [5] [17]:

$$Recall = \left(\frac{d}{c+d}\right) \times 100\% \quad (1)$$

$$Precision = \left(\frac{d}{b+d}\right) \times 100\% \quad (2)$$

$$Accuracy = \left(\frac{a+d}{a+b+c+d}\right) \times 100\% \quad (3)$$

$$Error\ Rate = \left(\frac{(b+c)}{a+b+c+d}\right) \times 100\% \quad (4)$$

3.3.2. The Interaction Time Assessment

This observation is executed to determine whether the goal of the system creation is fulfilled or not. The goal of the proposed system development is to reduce the number of user interactions including the time needed by the user to access the system. The frequent number of interaction and the time needed which is mentioned above become the components of a usability parameter which is efficiency. The scenario of this assessment is by comparing the average time needed between the pattern screen lock function and the Geofilock function when the context is recognized. The parameters used for the comparing are the number of user screen touching and the time needed by the user to pass the authentication mechanism. Two authentication mechanisms are pattern screen lock and Geofilock. The observation is done in 30 times and the MI Redmi 3 smartphone is used.

3.3.3. The User Satisfaction Measurement

User satisfaction is a satisfaction felt by the user when the user uses the app. 30 respondents try the app for testing. Indicator 1 means the user satisfaction, and indicator 2 means the ease of use [8].

The value of each indicator is determined by using the followed (5), (6):

$$Indicator\ value = \frac{actual\ score}{ideal\ score} \times 100\% \quad (5)$$

The actual score is the total score created by the questionnaires. The ideal value of each indicator is 120. The assessment category is created by using interval, and the interval used is:

$$Interval = \frac{100\%}{the\ number\ of\ \ criteria\ score} \quad (6)$$

The (6) is used for the estimation value of each category. The categories used are:

1. 0 – 24.9% of the users feel unsatisfied.
2. 25 – 49.9% of the users say it is enough (moderate or average).
3. 50 – 74.9% of the users feel satisfied.
4. 75 – 100% of the users feel very satisfied.

4. RESULTS AND ANALYSIS

The analysis is done by several observations. They can be followed in the followed sub-section.

4.1. The Functional Assessment

This experiment is done by using The Black Box Testing and the Confusion Matrix.

4.1.1. The Black Box Testing

The goal of this assessment is to recognize the functional system succeed for running its function, as listed in Table 3. The result is absolutely proper if the functional test result is the same as the result required.

As an example, Figure 4 shows the valid values of latitude and longitude, including SSID valid value. The toast function is also work properly. Based on Black Box testing, all scenarios have been adequate so it can be said the feature of Geofilock is performed well.

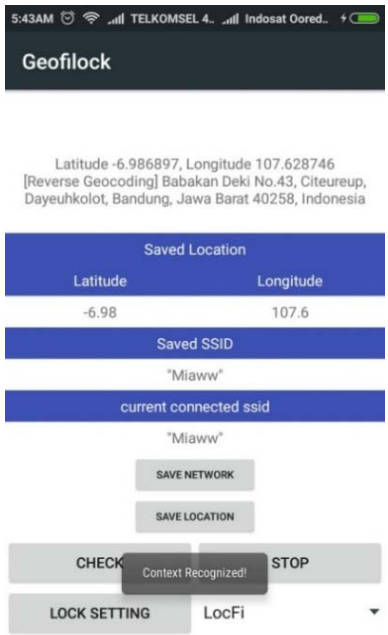

Figure 4. The Geofilock is loaded

Table 3. The black box testing

Functional Required	The Result Required	The Captured Result	Validation
Showing the information of the location and Wi-Fi	The app is going to presents the coordinate location and SSID	The location data and SSID are shown	Valid
Saving the information of detected location and detected Wi-Fi	The app is going to save the data of location and Wi-Fi. It is also going to presents the last saved data	The data of location and Wi-Fi are saved into the database, then the app shows them	Valid
The app can recognize the detected environmental context and the Geofilock function is automatically loaded	The system shows toast "Context Recognized"	The system shows toast "Context Recognized"	Valid
The app can recognize the detected environmental context and the pattern screen lock function is automatically loaded	The system shows the pattern screen lock	The system shows the pattern screen lock	Valid

4.1.2. The Assessment by Using Confusion Matrix

The observation is executed to know the accuracy level of the functionality to recognize the context. The assessment is conducted by making a prediction table and actual table related to the result after the assessment is done [2]. The assessment result by using the Confusion Matrix can be seen in Table 4.

Table 4. The result of the confusion matrix assessment

No.	Condition			Result
	Location	Mac Address	Recognition Mode	
1	-6.9869056, 107.6287457	fc:dd:55:26:0c:d4	Location	Succeed
2	-6.9868960, 107.6287435	Null	Location	Succeed
3	-6.986027, 107.624179	fc:dd:55:26:0c:d4	Location	Failed
4	-6.986027, 107.624179	Null	Location	Failed
5	-6.9869026, 107.6287537	fc:dd:55:26:0c:d4	Wi-Fi	Succeed
6	-6.9868956, 107.6287458	Null	Wi-Fi	Failed
7	-6.986027, 107.624179	fc:dd:55:26:0c:d4	Wi-Fi	Succeed
8	-6.986027, 107.624179	Null	Wi-Fi	Failed
9	-6.9869036, 107.6287457	fc:dd:55:26:0c:d4	Wi-Fi & Location	Succeed
10	-6.9869030, 107.6287454	Null	Wi-Fi & Location	Failed
11	-6.986027, 107.624179	fc:dd:55:26:0c:d4	Wi-Fi & Location	Failed
12	-6.986027, 107.624179	Null	Wi-Fi & Location	Failed

4.2. The Measurement of Interaction Time

The average time which is required to open the pattern screen lock is 0.91 seconds, as shown in Figure 5. The touch required to unlock this pattern screen lock, until the home screen loads, is 2 touches. The touches are pressing the button to turn on the screen, and swiping the screen without interruption. The average time required to access the home screen by using Geofilock is 0.1 seconds and only one touch needed. The observation collects 30 sample data by conducting the app to 30 persons. The timer starts since there is a touch action until the locked system is broken. The feature of the timer is attached in the system and generates log data. Actually, Geofilock has started to recognize the environmental context in the background before the triggered action executed to unlock the system. It is the reason why time measurement of 0.1 seconds is possible to be realized.

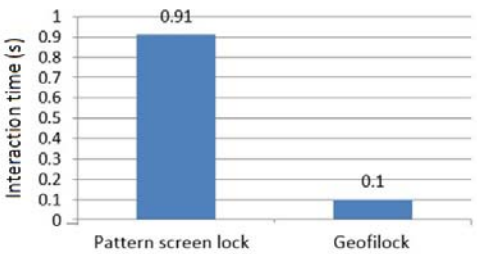

Figure 5. The average of interaction time between pattern screen lock and Geofilock

4.3. The Result of User Satisfaction Measurement

The indicator used is the range of user satisfaction after using the Geofilock system and the range of the user for knowing the Geofilock functionality [8]. By querying 30 respondents, the result of the actual score is 78 for indicators 1 and 82 for indicator 2. The ideal value of each findicator is 120. Therefore, the measurement of the Geofilock system is 65% for indicator 1 and 68.3% for indicator 2. This result implies that Geofilock is categorized as satisfactory and easy to learn, according to Section 3.3.3.

5. CONCLUSION

Based on the assessment results, Geofilock app based on environmental context gives the user less time and less interaction to perform authentication, compared to pattern screen lock. Based on the survey result, the user feels the Geofilock system is easier to learn and run. In addition, the authentication by using pattern screen lock is no longer needed when the environmental context data is recognized. Furthermore, the user also states no objection if necessary to do some touches as long as it makes the context can be saved and can be reused for the another time.

REFERENCES

[1] Harbach M, De Luca A, and Egelman S., "The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens," *In Conference on Human Factors in Computing Systems (CHI)*, pp. 4806–4817, 2016.

[2] Nathan M, Marian H, De Luca A, and Egelman S., "The Anatomy of Smartphone Unlocking: Why and How Android Users Around the World Lock Their Phones," *GetMobile: Mob. Comp. Comm*, vol. 20(3), pp. 42–46, 2017.

[3] Davis FD., "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Q*, vol. 13(3), pp. 319–340, 1989.

[4] Li H, and Zhu X., "Face Recognition Technology Research and Implementation Based on Mobile Phone System," in *Natural Computation, Fuzzy Systems and Knowledge Discovery, 12th ICNC-FSKD 2016*, pp. 972–976, 2016.

[5] Witte H, Rathgeb C, and Busch C. "Context-Aware Mobile Biometric Authentication Based on Support Vector Machines," in *Emerging Security Technologies, 4th EST 2013*, pp. 29–32, 2013.

[6] Yang L, Guo Y, Ding X, Han J, Liu Y, Wang C, and Hu C., "Unlocking Smart Phone Through Handwaving Biometrics," in *IEEE Trans. Mob. Comput*, vol. 14, pp.1044–1055, 2015.

[7] Kim HW, Kim JH, Park JH, and Jeong YS., "Time Pattern Locking Scheme for Secure Multimedia Contents in Human-Centric Device," *Sci. World J*. 2014; 2014.

[8] Thorpe J, MacRae B, and Salehi-Abari A., "Usability and Security Evaluation of GeoPass," in *Symp. Usable Priv. Secur. - 9th SOUPS 2013*, vol. 14, 2013.

[9] Masango M, Mouton F, Nottingham A, and Mtsweni J., "Context Aware Mobile Application for Mobile Devices," in *Information Security for South Africa (ISSA)*, pp. 85–90, 2016.

[10] Jin Y, Tomoishi M, and Matsuura S., "Enhancement of VPN Authentication Using GPS Information with Geo-Privacy Protection," in *Int. Conf. Comput. Commun. Networks - 25th ICCCN 2016*, 2016.

[11] De Luca A, Hang A, Brudy F, Lindner C, and Hussmann H., "Touch Me Once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns," in *Proc. 2012 ACM Annu. Conf. Hum. Factors Comput. Sys*, pp. 987-996, 2012.

[12] Avdyushkin M, and Rahman M., "Secure Location Validation with Wi-Fi Geo-Fencing and NFC," in *Int. Conf. Trust. Secur. Priv. Comput. Commun. - 14th Trust. 2015*, pp. 890–896, 2015.

[13] Day AK., "Understanding and Using Context," *Personal and Ubiquitous Computing*, vol. 5(1), pp. 4–7, 2001.

[14] Kainda R, Flechais I, and Roscoe AW., "Security and Usability: Analysis and Evaluation," in *Availability, Reliab. Secur. - 5th ARES 2010*, pp. 275–282, 2010.

[15] Tofan DC., "Information Security Standards," *J. Mobile, Embed. Distrib. Syst*, vol. 3, pp. 128–135, 2011.

[16] Xu W, Zhang F, and Zhu S., "Permlyzer: Analyzing Permission Usage in Android Applications," in *Int. Symp. Softw. Reliab. Eng. - 24th ISSRE 2013,* pp. 400–410, 2013.

[17] Junker M, Hoch R, and Dengel A., "On the Evaluation of Document Analysis Components by Recall, Precision, and Accuracy," in *Int. Conf. Doc. Anal. Recognition (ICDAR)*, pp. 717–720, 1999.