


Threats of Password Pattern Leakage Using Smartwatch Motion Recognition Sensors

Jihun Kim and Jonghee M. Youn * 

Computer Engineering, Yeungnam University, Gyeongsan, Gyeongbuk 38541, Korea; f1352@ynu.ac.kr

* Correspondence: youn@yu.ac.kr; Tel.: +82-53-810-2552

Academic Editor: Laurence T. Yang

Received: 3 March 2017; Accepted: 26 June 2017; Published: 30 June 2017

Abstract: Thanks to the development of Internet of Things (IoT) technologies, wearable markets have been growing rapidly. Smartwatches can be said to be the most representative product in wearable markets, and involve various hardware technologies in order to overcome the limitations of small hardware. Motion recognition sensors are a representative example of those hardware technologies. However, smartwatches and motion recognition sensors that can be worn by users may pose security threats of password pattern leakage. In the present paper, passwords are inferred through experiments to obtain password patterns inputted by users using motion recognition sensors, and verification of the results and the accuracy of the results is shown.

Keywords: side-channel attack; smartwatch; motion sensor; keystroke

1. Introduction

Before smartwatches were released onto the market, the watches were simply intended to identify time. However, thanks to the release of smartwatches embedded with a processor and an operating system, watches began to include instruments (smartwatches) that are used not only to identify time, but also to perform diverse functions simultaneously, and have been becoming more and more convenient to use [1]. One of representative functions of smartwatches is the fitness function, such as the measurement of step counts and calorie consumption [2]. The fitness function of smartwatches operates by calculating the rotation, direction, and movements of watches using gyroscopes that sense movements, measurement sensors such as acceleration sensors, gravity sensors, and terrestrial magnetism sensors that sense directions. Application developers utilize these measurement sensors as motion sensors to understand users' motions, that is, as motion recognition sensors, which recognize users' motions to perform certain functions, and are used as controllers, such as those that turn off the screen or maintain the screen dark as a default, and brighten the screen when the user has raised his/her hand [3].

The present paper noted the fact that most smartwatches support motion recognition sensors as described above, while being wearable devices that are worn on users' wrists [4]. Since smartwatches are worn on users' wrists, users' wrist movements can be exposed to motion recognition sensors. The exposure of wrist movements can easily break down individuals' privacy and important security elements [5]. This is closely related to modern trends where analog devices are replaced by digital devices. For instance, most private houses' front doors are opened and locked using digital door locks by entering passwords instead of using mechanical keys, and banking is done through automatic teller machines (ATMs) instead of through bank clerks using paper bankbooks. In a digitalized society, attackers intending to make ill use of the convenience of digital systems are most interested in 'passwords' that are individuals' unique character strings based on agreements made in advance for security. Passwords for digital door locks on front doors or those used for banking are four-digit

numbers without any character string in most cases, and the positions of numbers on password input panels are invariable in most cases. Furthermore, security keys such as passwords or personal identification numbers (PINs) are input directly with the users' fingers. To input security keys, users make upward, downward, leftward, and rightward wrist movements, and the possibility of leakage of these movements through motion recognition sensors in smartwatches is a major subject in the present paper.

To confirm the issue as such, in the present paper, after users wearing a smartwatch input passwords into password input panels of machines such as automated teller machines, the patterns of the wrist movements was analyzed to estimate the passwords entered by the users.

The present paper is composed as follows. In Section 2, the proposed method devised to achieve the objective are explained and in Section 3, experiments conducted based on the method proposed in the present paper are explained and the results are shown. The results are verified in Section 4 and in Section 5, motion recognition sensor related works are mentioned and conclusions are drawn in Section 6.

2. Proposed Methods

Figure 1 is a diagram of the method proposed in the present paper. The method proposed in the present paper consisted of a smartwatch, a smartphone connected to the smartwatch, and a server for prediction of passwords. We identified the wrist movements relevant to password input using the measured values from the accelerometer sensor of the smartwatch and the measured values of the gyroscope sensor. The smartwatch was used to simply transmit the relevant measured values to the smartphone. In the smartphone, the password pattern was converted into an image based on the measured value transmitted from the smartwatch, and the relevant image was transmitted to the server. The server predicted the password based on the transmitted image by applying the algorithm to the image.

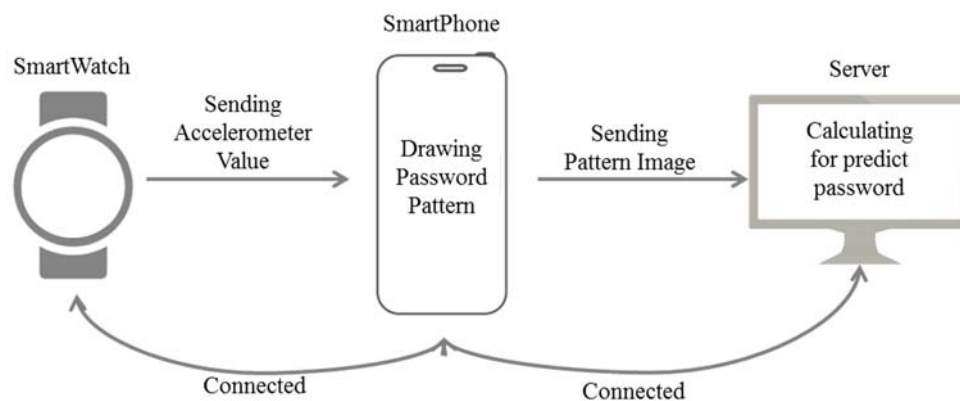


Figure 1. Proposed method structure.

2.1. Identifying User Behaviors

When seen from the perspective of an attacker trying to steal the password of a user wearing a smartwatch, the accurate password pattern cannot be easily obtained if the movements of the smartwatch are continuously collected because the user wearing a smartwatch walks and conducts other activities of daily living, such as typing on a computer keyboard and eating meals. Therefore, we inferred certain behavior patterns of users when they pressed their password at an ATM, and assumed the points of the start and end of transmission.

1. Raise the arm
2. Take the actions to input a password
3. Lower the arm

The sensor-measured values for the movements of the smartwatch immediately following the behavior set forth above were transmitted to the smartphone.

2.2. Start Transmission and Measurement Values

Figure 2 shows an example of the behavior that indicates the start of sensor transmission assumed in Section 2.1. The figures on the top show the process of raising the arm to enter the password, and the smartwatch screens on the bottom show the related states of the smartwatch with regard to the transmission of the sensor values. Table 1 shows that The English words displayed on the smartwatch screen explain the following states.

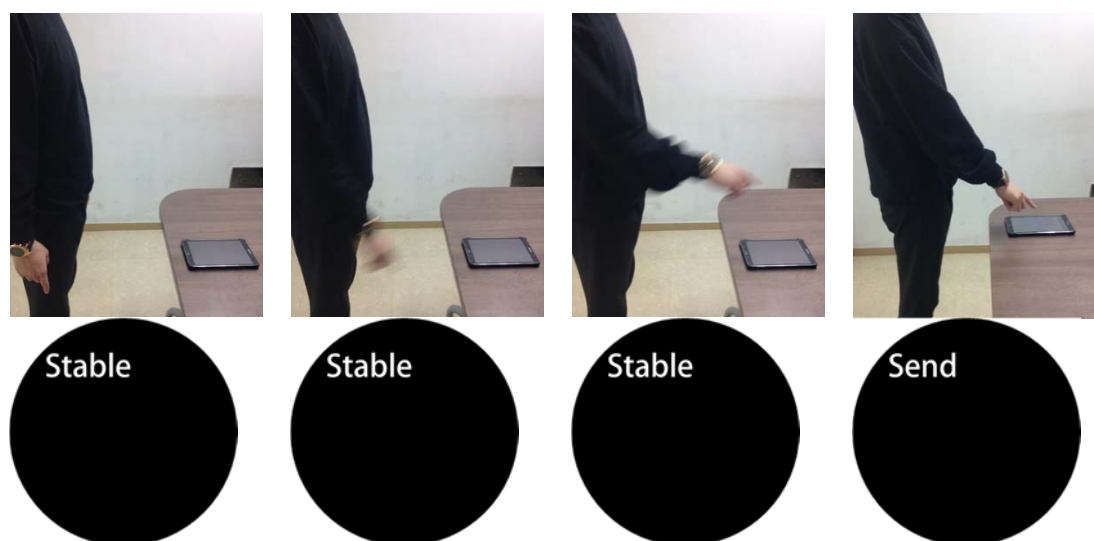


Figure 2. States of the smartwatch according to user motions.

Table 1. States of smartwatches according to the time points of measurement recording.

State	Explanation
Stable	The measured values were not transmitted.
Send	The measured values were transmitted.

2.3. Transmission of Sensor Measured Values

In the present paper, among motion recognition sensors, only accelerometer sensors were used for recording of measured values because accelerometer sensors are fusion sensors that can also sense gravity and angular speed, and they can produce the results of many sensors without using other sensors, through the inclusion of several calculation methods.

2.3.1. Acceleration Sensor

In general, the dictionary definition of ‘acceleration’ is the degree to which speed changes over time [6,7]. For instance, acceleration is related to the feeling of the body being pushed into the car seat when the accelerator pedal has been pressed down. Therefore, it may be difficult to be certain of acceleration acting downwards on a mass even when it remains still due to the effects of gravity. However, in the formula $F = ma$, acceleration a is associated with force F through the proportional constant termed mass. Therefore, acceleration proportional to force exists everywhere that force exists. In addition to the above theory, there is a kind of acceleration that we always feel on earth, termed gravitational acceleration [7,8].

Therefore, sensors embedded in devices also measure an acceleration of 9.8 m/s^2 when they are in the direction of gravity. Given the foregoing, it can be seen that the concepts of gravity sensors and acceleration sensors are not apart from each other [9,10].

Because acceleration is physically composed of vector quantities that have sizes and directions, in the present paper, the sizes and directions of movements of smartwatches are measured based on the measured values of acceleration sensors along the x-, y-, and z-axes.

The measurements of coordinate systems and movements are also calculated based on device coordinate systems as shown in Figure 3. As shown in Figure 3, if the device is moved left, the x-axis measured value will decrease, and conversely, if the device is moved right, the x-axis measured value will increase (Figure 3a). Here, a general range of measurement is approximately ± 4 . With regard to up-down movements, that is, changes in location along the y-axis, if the device is moved upward, the y-axis measured value will increase and if the device is moved downward, the y-axis measured value will decrease (Figure 3b).

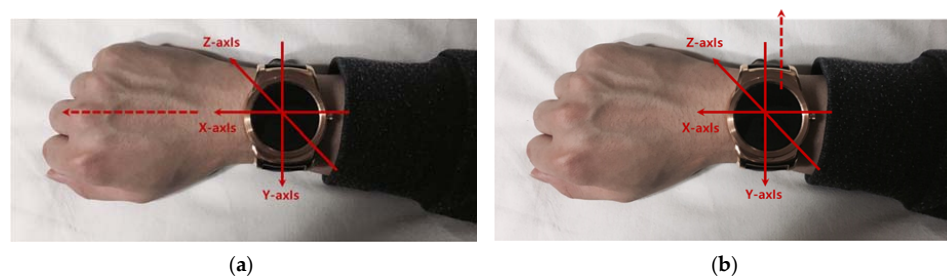


Figure 3. Changes in acceleration sensor coordinate systems according to smartwatch movements. (a) Decrease in the x coordinate system value. (b) Increase in the y coordinate system value.

2.3.2. Simple Movements of Smartwatches in the Process of Inputting Passwords

The left drawing in Figure 4 (Figure 4a) is a view of movements when the user inputs a four-digit password 5980, the central drawing is the smartwatch movement pattern for the user's movements, and the right drawing is the resultant changes in the acceleration sensor's measured values. As can be seen from the drawings in Figure 4b, user's movements to input passwords and the related movements of the smartphone can be regarded to be quite similar to each other. The related acceleration sensor's measured values are recorded using the x- and y-axes measured values because the movements are simple upward, downward, leftward, and rightward movements.

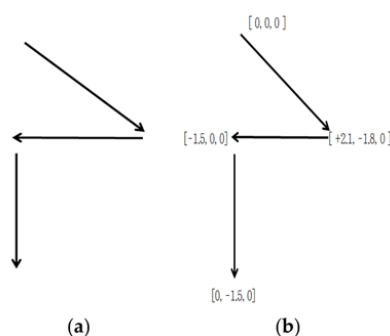


Figure 4. User's password input and related movements of the smartwatch. (a) Smartwatch movement. (b) Changes in measured values of the acceleration sensor.

2.3.3. Smartwatch Movements when Password Pressing Actions are Taken

If the user presses a pattern that is drawn only in the horizontal direction, such as 1333, the movements of the smartwatch and the acceleration sensor's measured values will be recorded as

shown in Figure 5. In this case, although the pattern of the password can be deduced, the password cannot be easily estimated.



Figure 5. Movement of the smartwatch when there are overlapping numbers. (a) Movement of the smartwatch. (b) Changes in measured values of the acceleration sensor.

To solve such exceptions, motions made when passwords are pressed were identified. To this end, decreases in the z-axis values of the acceleration sensor were utilized. That is, as shown in Figure 6, pressing actions were recorded when the measured value of the z-axis had decreased and increased thereafter.

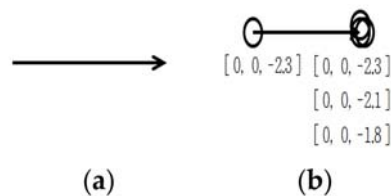


Figure 6. Pattern acquisition utilizing the z-axis of the acceleration sensor. (a) Movement of the smartwatch. (b) Changes in measured values of the acceleration sensor.

2.4. Terminate Transmission a Measurement Values

In the present paper, the transmission of the measured values was terminated at the motion of the user to ‘lower the arm’ after taking the motion to enter the password.

Figure 7 shows the time point of termination, that is, the user’s motion to lower the arm and resultant states of the smartwatch. While the user was inputting the password, the measured values of the smartwatch were recorded and transmitted as a ‘Send’ state. However, at the time point where the arm was completely lowered, the smartwatch was put into a stable state and the recording of measured values was terminated.

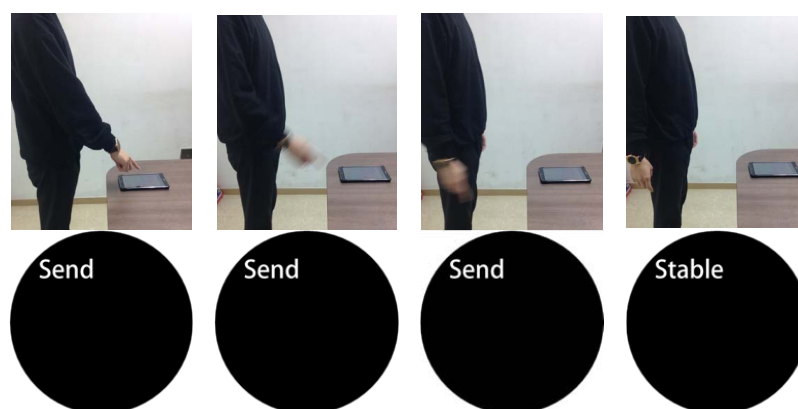


Figure 7. States of the smartwatch according to the motion of the user (termination).

2.5. Password Estimation

In the present paper, password patterns were acquired through the movements of users wearing a smartwatch when they pressed passwords. Upward, downward, leftward, rightward, and diagonal movements were recorded as the movements of the acceleration sensor along the x-axis and the y-axis, and the actions to press passwords were measured with changes in the acceleration sensor's positions along the z-axis. However, there were difficulties in estimating actual numbers pressed by users when based on only these movement patterns.

To solve this problem, in the present paper, acquired patterns were used as information to estimate the numbers actually pressed by users.

Figure 8 shows the method proposed in the present paper that was used to estimate pressed passwords based on acquired patterns. Let us assume that a pattern of a four-digit password was acquired as shown in the left figure. Here, the numbers on the pattern indicate actions taken to press the panel, that is, the sections in which the z-axis measured values decreased and increased thereafter and the numbers do not indicate the numbers in the password pressed by the user but the order of pressing. That is, the user took actions to pressed the password input panel in order of the numbers 1, 2, 3, and 4.

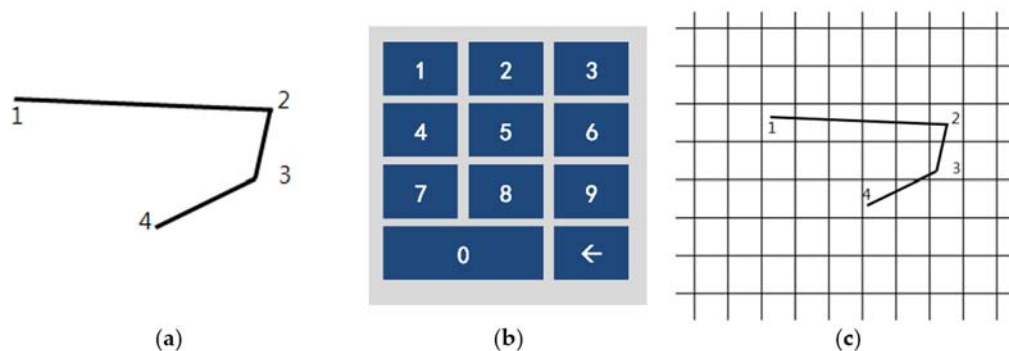


Figure 8. Assumption of patterns. (a) Acquired password pattern; (b) Password input panel; (c) Password pattern on a grid plate.

In the present paper, the user's password input panel was assumed as shown in the central figure in Figure 8. The password input panel as such was simply regarded as a grid plate. In the present paper, the pattern was shown on a grid plate, as shown in the right figure in Figure 8. Before estimating actual numbers, the sizes of coordinates, that is, the range to be used in calculations, was set simply for the accuracy of estimated numbers.

Figure 9 shows the method of setting the range of estimation. First, 1 is located at the left end and 2 is located at the right end. The horizontal range of estimation is set based on 1 and 2, that is, the left end and the right end. In addition, 1 is located not only at the left and but also at the top and 4 is located at the bottom. The vertical range of estimation is set based on 1 and 4, that is, the uppermost and the lowermost coordinates.

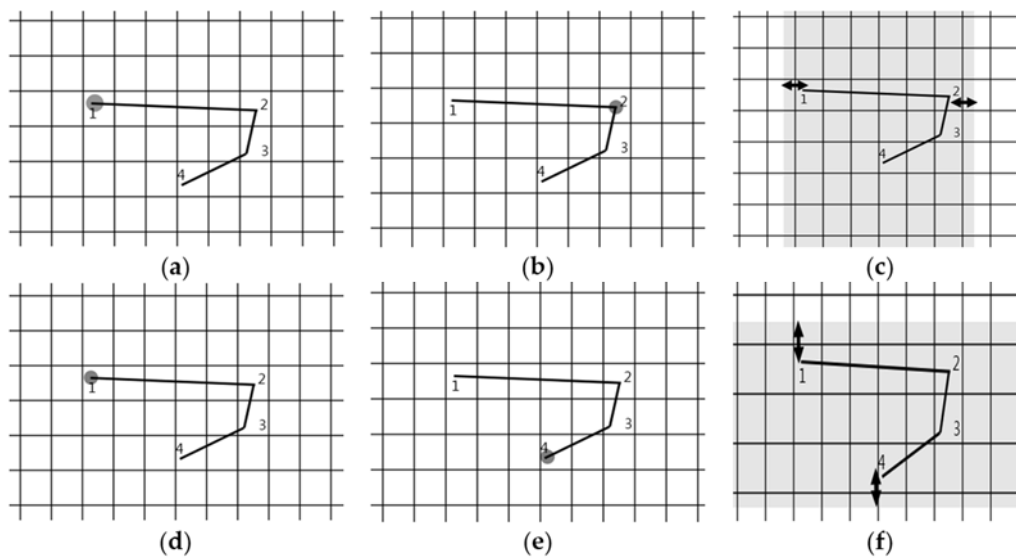


Figure 9. Setting of ranges of estimation. (a) Leftmost coordinate; (b) Rightmost coordinate; (c) Range of estimation (horizontal direction); (d) Uppermost coordinate; (e) Lowermost coordinate; (f) Range of estimation (vertical direction).

The final range of estimation can be indicated as shown by the left drawing of Figure 10 which shows the common segment of the horizontal range of estimation and the vertical range of estimation.

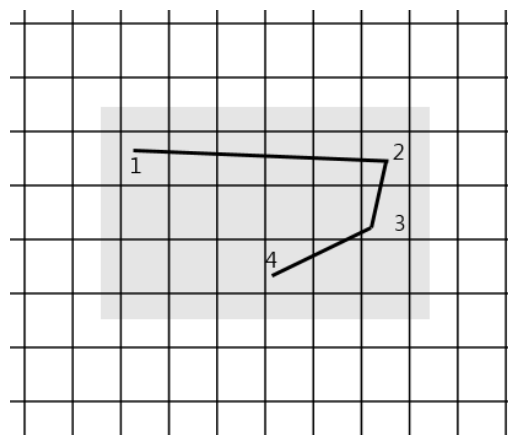


Figure 10. Final range of estimation.

Next, the estimations of actually pressed numbers are calculated. In the present paper, the estimations were calculated based on the coordinates where pressing actions were taken. In particular, the leftmost, rightmost, uppermost, and lowermost coordinates are used as important information for estimation. For instance, let us estimate the actual numbers pressed by the user from the first number to the last one, based on the acquired pattern shown in Figure 10. First, calculations as such can be easily understood by assuming that the pattern is drawn on the central figure in Figure 8 that is, the password input panel. Let us think about the location where the first pressing action was taken, that is, the location where 1 was output and the location where the second pressing action was taken, that is, the location where 2 was output.

Since the location where the last pressing action was taken, that is, the location where 4 was output, is located between locations 1 and 2, the password input numbers 1 and 3, 4 and 6, and 7 and 9 are expected for the locations 1 and 2. Next, the location where the third pressing action was taken,

that is, the location where 3 was output, is located below the location where 2 was output, and 3, 6, and 9 in the password input panel are located on the same vertical row. Therefore, regardless of whether the estimated number pressed by the second pressing action is 3 or 6, the estimated number pressed by the third pressing action becomes 6 or 9. In the same manner, since 1, 2, or 3 is located at the location where the last pressing action was taken, that is, the location where 4 was output, 1 was output on the left and 2 and 3 were output on the right, the password input numbers 8 or 0 can be expected.

The estimated numbers explained as above are set forth in Table 2. According to the acquired pattern shown in Figure 8, the finally expected passwords are 1368, 1360, 1390, and 4690.

Table 2. Estimation of passwords according to the locations where pressing actions were taken.

	Estimated Number				
	(1, 3)	(1, 3)	(1, 3)	(4, 6)	(7, 9)
First and second	(1, 3)	(1, 3)	(1, 3)	(4, 6)	(7, 9)
Third	6	6	9	9	←
Fourth	8	0	0	0	none
Finally estimated number	1368	1360	1390	4690	none

2.6. Computational Complexity

Prediction of passwords in the present paper was calculated based on the obtained pattern images. Coordinate values were judged to have been pressed on the grid plate, and the areas above, below, left, right to the stored nodes were explored to predict the password. If the password was pressed on one coordinate value only, as with 3333, the computational complexity was shown as $O(1)$ because there was no need to explore the areas above, below, left, or right of the coordinate value, and even in the worst case where all the areas above, below, left, right to the coordinate value were explored, the computational complexity was shown as $O(n^2)$.

2.7. Filter and Inertia

Pure measured values of sensors involved errors such as noises, drifts, and zero offset. Various filters were necessary to improve the accuracy and precision of the sensors' measured values.

2.7.1. Low-Pass Filter

Low-pass filters are used in acceleration sensors to remove gravity acceleration [11]. Since the measured values used in the present paper required pure acceleration removed of gravitational acceleration, gravitational acceleration was removed from measured values of acceleration. Low-pass filters as such were used during data equalization to minimize noise. A general method of applying low-pass filters for data equalization is used by obtaining the newest value through weighting of the previous average value. The equalization parameter a is used as follows Formula (1):

$$(\neq w \text{ value}) = (\text{previous value}) + x_i \times a - (\text{previous value}) \times a \quad (1)$$

where x (the value collected the most recently) weighted by a is added to the value calculated previously, and the previous value weighed by a is deducted to obtain the difference. If a is close to a value of 1, the new value will be x , and if a is close to zero, the new value in the calculation formula will not be different from the previous value. Here, x can have the desired level of effects on the new value.

2.7.2. Kalman Filter

Purely measured sensor values cannot be easily utilized accurately, due to interference and noises. To solve this problem, an optimum mathematical calculation process was introduced that enabled the prediction of locations after a certain time, by analyzing existing measured values mixed with noises through the least-squares method. This calculation process is called the Kalman Filter [12]. To mention

with expansion, the Kalman Filter is based on measurement progression over time. More accurate results can be expected from the Kalman Filter than from using the results of measurements conducted only at relevant moments. The Kalman Filter recursively processes input data including noise, and enables optimum statistical deduction of the current states. The entire algorithm can be divided into two parts; prediction and update. The prediction refers to the prediction of the current states and the update refers to the enabling of more accurate prediction by including the measurements observed in the current state. As shown in Figure 11, the measured values of the smartwatch accelerometer sensor before applying the Kalman Filter pose difficulties in accurate measurement due to noise. This poses difficulties in acquiring the smartwatch's movement patterns, and the application of the Kalman Filter reduces noise in measured values to assist in the acquisition of accurate patterns.

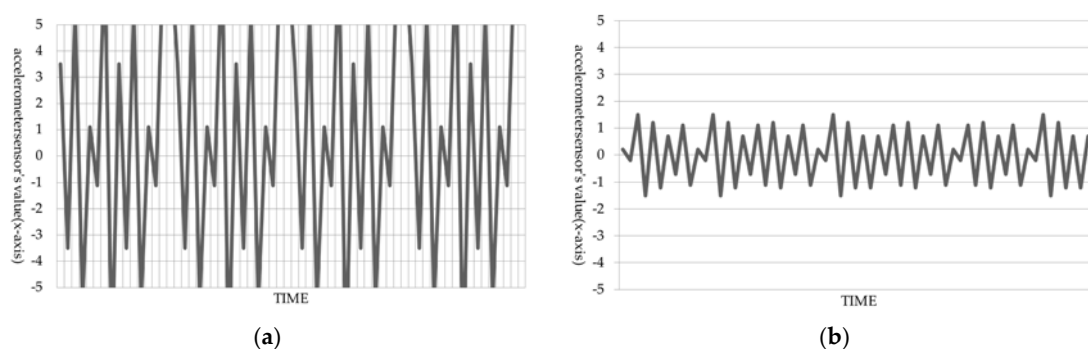


Figure 11. Application of the Kalman Filter to the measured values of the accelerometer sensor. (a) Before applying the Kalman Filter. (b) After applying the Kalman Filter.

2.7.3. Inertia

Inertia refers to the tendency to maintain the state of movements, and the resistance of objects when the state of movements is changed. All movements on the earth follow this law of inertia and the movements of sensors are not exceptional.

After moving a smartwatch laid onto a plane, the values as shown in Figure 12 were measured in real life.

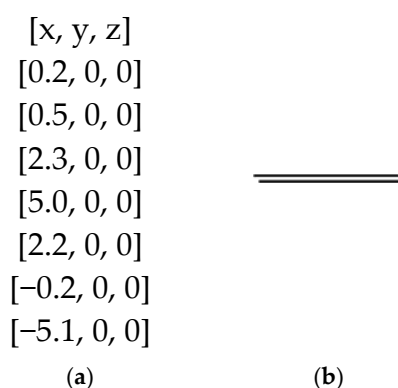


Figure 12. Movement of smartwatch and measured values of acceleration sensor in relation to inertia. (a) Changes in the measured values of the acceleration sensor; (b) Record of movement.

As shown in the right-hand figure in Figure 12, the smartwatch's movement, which should be recorded with one line, was actually recorded by two lines.

Changes in the acceleration sensor's measured values, and the portion actually relevant to the present paper, are shown in Figure 13.

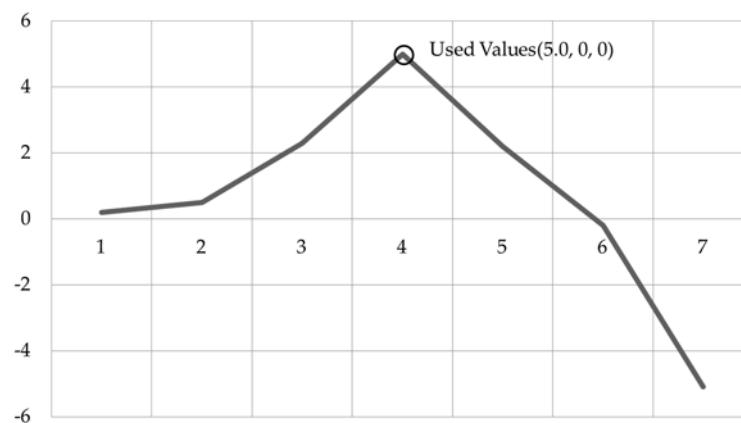


Figure 13. Changes in measured values of acceleration along the x-axis in relation to inertia.

Since the smartwatch was moved to the right, the values of movement along the x-axis should be positive numbers. When moved to the right, among the measured positive numbers, only the maximum value was recorded, and other values were omitted.

3. Experiment

In this section, the objective of the present paper is presented and methods that were planned and implemented in the present paper were proposed.

3.1. Experimental Environment

First, we used the LG Urbane smartwatch (LG Electronics, Seoul, South Korea) [13], and the Samsung Galaxy 6 (Samsung Electronics, Suwon, South Korea) [14] as a smartphone connected to the smartwatch. In addition, we made an effort to perform the experiment in an environment very similar to the actual environment where passwords are entered into an actual ATM. To this end, we first checked the exterior specifications of ATMs. The ATM selected for the study was the ATM of the bank used the most frequently in the area where we were located, and we selected one of the most crowded places containing ATM users.

Figure 14 shows an experimental environment assumed to configure an environment maximally close to a real ATM. In the place where the actual user was standing, the height of the screen was approximately 85 cm. Therefore, a test password input device tablet was placed on a table, which was approximately 85 cm high to replicate the same height for the test. In addition, the screen used to enter actual passwords was 7 cm wide and 10 cm long, and the experimental application for the tablet used in the test was also made in the same size. The password input device of actual ATMs was tilted by approximately 5° . Since this is almost the same as a flat surface, the experimental tablet was set to be placed on a flat surface.



Figure 14. View of the experimental environment.

In the experiment, we wore a smartwatch on the right wrist because most people enter their password with their right hand. Most people wear the watch on the left wrist regardless of whether they are left-handed or right-handed [15,16]. However, in general, right-handed women tend to wear a smartwatch on their right wrist, and some forums argue that they generally wear a smartwatch on their right wrist [17,18]. Furthermore, according to a study conducted by [19], approximately 30% of all people are ambidextrous, and their hands where they wear accessories vary with certain working environments. In addition, manufacturers of smartwatches such as Samsung and Apple have announced that left-handed people wear smartwatches on their right wrist [20,21] and they separately support left-handed people's mode for such users [22,23]. Moreover, among smartwatch applications, fitness applications such as those that measure the trajectory of the wrist to help the correction of exercise postures have been released. Unlike general watches, these applications should be worn on the right wrist because they are loaded on smartwatches. The smartwatch market will continue to develop, and these fitness applications are a reason for why many people wear the smartwatch on their right wrist.

3.2. Scenario

In the present paper, users wearing a smartwatch input passwords as four-digit numbers into the password input panel on a plane like an ATM, the password patterns were acquired, and the passwords were estimated based on the patterns.

3.3. Test Case

In the present paper, a total of 10 test cases were fabricated. Table 3 shows 10 patterns and the characteristics of the patterns.

Table 3. Password test cases.

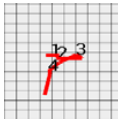
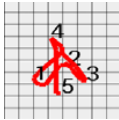
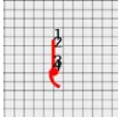
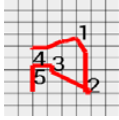
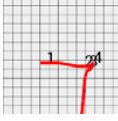
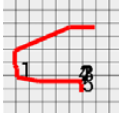
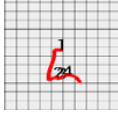
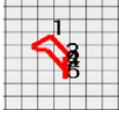
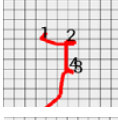
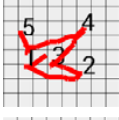
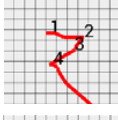
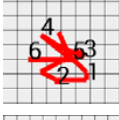
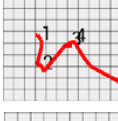

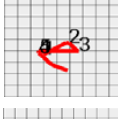
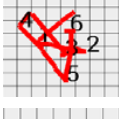
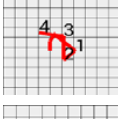
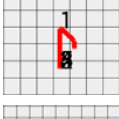
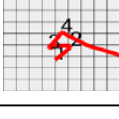
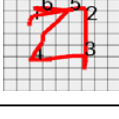
Test Case	Password	Characteristics of the Patterns
1	1234	horizontal
2	2580	vertical
3	1333	horizontal, overlapping
4	2000	vertical, overlapping
5	1399	↵-shaped, overlapping
6	1357	horizontal, diagonal
7	1733	vertical, diagonal
8	7597	triangle
9	9054	random
10	8642	random
11	75920	5-digits
12	39547	5-digits
13	13333	5-digits
14	10000	5-digits
15	79831	5-digits
16	976154	6-digits
17	391736	6-digits
18	798105	6-digits
19	800000	6-digits
20	139712	6-digits

The passwords consisted of four-digit numbers, and for the 10 test cases, seven passwords had characteristic shapes such as horizontal, vertical, triangle, and diagonal, and in addition to the characteristic shapes, passwords that contained overlapping numbers were also included. In addition, two test cases were randomly input to conduct experiments on password pattern acquisition.

3.4. Pattern Acquisition

Table 4 shows the passwords in the test cases, the characteristics of the passwords, and the password patterns acquired in the experiments.

Table 4. Acquired patterns by test case.

Test Case	Password	Characteristics of the Patterns	Acquired Patterns	Test Case	Password	Characteristics of the Patterns	Acquired Patterns
1	1234	horizontal		11	75920	5-digits	
2	2580	vertical		12	39547	5-digits	
3	1333	horizontal, overlapping		13	13333	5-digits	
4	2000	vertical, overlapping		14	10000	5-digits	
5	1399	┐-shaped, overlapping		15	79831	5-digits	
6	1357	horizontal, diagonal		16	976154	6-digits	
7	1733	vertical, diagonal		17	391736	6-digits	
8	7597	triangle		18	798105	6-digits	
9	9054	random		19	800000	6-digits	
10	8642	random		20	139712	6-digits	

3.5. Pattern Acquisition by Angle Change

We tried to prepare an environment very similar to the actual ATMs. Also, the password input device of actual ATMs was tilted by approximately 5°, which is almost the same as a flat surface, and the experimental tablet was placed on a flat surface. Since the acceleration sensors mounted on the smartwatch are fusion sensors that can also sense gravity and angular speed, the acquired password

pattern can be different depending on the angle of the ATM's keypad. For this reason, we discussed how the password patterns were acquired as the keypad angle increased by 10° . Table 5 shows acquired password patterns as the angle increases by 10° , using the same password (9054) within the experiment to compare. As the angle changed, there was no significant difference in the acquired password pattern, but when compared to the flat surface (0°), additional lines were drawn. This was indicated by a hatched rectangle, and it confirmed that the greater the angle increased, the longer the length increased. However, in this paper, we estimate the action to press passwords as changes in the z-axis, so even if such lines are added, there was still no difficulty in estimating the password.

Table 5. Pattern acquisition by angle change.

Tablet Angle	Acquired Patterns	Tablet Angle	Acquired Patterns	Tablet Angle	Acquired Patterns
0°		10°		20°	
30°		40°		50°	

3.6. Results of Password Estimation

Table 6 shows the results of the password estimation analysis.

Table 6. Estimated passwords by test case.

Test Case	Password	Characteristics of the Patterns	Estimated Passwords	Estimation Success Rate
1	1234	horizontal	1234, 4560, 7890	100
2	2580	vertical	1470, 2580, 3690	100
3	1333	horizontal, overlapping	1222, 1333, 4555, 4666, 7888, 7999, 0000	100
4	2000	vertical, overlapping	1444, 1777, 1000, 2555, 2888, 2000, 3666, 3999	100
5	1399	↵-shaped, overlapping	1255, 1288, 1366, 1399	100
6	1357	horizontal, diagonal	1357, 1350, 4680	100
7	1733	vertical, diagonal	1733, 1766, 4033, 4066	100
8	7597	triangle	4264, 7297, 7597	100
9	9054	random	6821, 6021, 9054	100
10	8642	random	0975, 0972, 8642	100
11	75920	5-digits	75920	100
12	39547	5-digits	39547, 39540	100
13	13333	5-digits	13333, 46666, 79999,	100
14	10000	5-digits	14444, 17777, 10000, 25555, 28888, 20000 3666, 39999	100
15	79831	5-digits	46531, 79831, 79864	100
16	976154	6-digits	976154	100
17	391736	6-digits	281714, 391736, 392825	100
18	798105	6-digits	798105	100
19	800000	6-digits	144444, 177777, 100000, 200000, 255555, 288888, 366666, 399999 400000, 477777, 500000, 588888, 699999, 700000, 800000	100
20	139712	6-digits	136412, 139012, 139712, 469745	100

4. Verification

The reduction rate of the number of cases was calculated by Formula (2), and on reviewing the reduction rates along with the characteristics by pattern in Table 7, the following characteristics of decreases in reduction rates were found.

$$1 - \frac{\text{the number of estimated passwords}}{\text{total number of estimated}} \quad (2)$$

Table 7. Reduction rate by test case.

Test Case	Password	No. of Digits	Characteristics of the Patterns	Total Number of Cases of Passwords	Number of Estimated Password	Number of Cases Reduction Rate
1	1234	4	horizontal	1000	3	99.700
2	2580	4	vertical	1000	3	99.700
3	1333	4	horizontal, overlapping	1000	7	99.300
4	2000	4	vertical, overlapping	1000	8	99.200
5	1399	4	↵-shaped, overlapping	1000	4	99.600
6	1357	4	horizontal, diagonal	1000	3	99.700
7	1733	4	vertical, diagonal	1000	4	99.600
8	7597	4	triangle	1000	3	99.700
9	9054	4	random	1000	3	99.700
10	8642	4	random	1000	3	99.700
11	75920	5	random	10,000	1	99.990
12	39547	5	random	10,000	2	99.980
13	13333	5	horizontal, overlapping	10,000	3	99.970
14	10000	5	vertical, overlapping	10,000	8	99.920
15	79831	5	Random	10,000	3	99.970
16	976154	6	Random	100,000	1	99.999
17	391736	6	Random	100,000	3	99.997
18	798105	6	Random	100,000	1	99.999
19	800000	6	vertical, overlapping	100,000	15	99.985
20	139712	6	random	100,000	4	99.996

4.1. Reduction Rates for Number of Cases by the Number of Digits of Passwords

Figure 15 shows reduction rates according to the numbers of digits in the passwords.

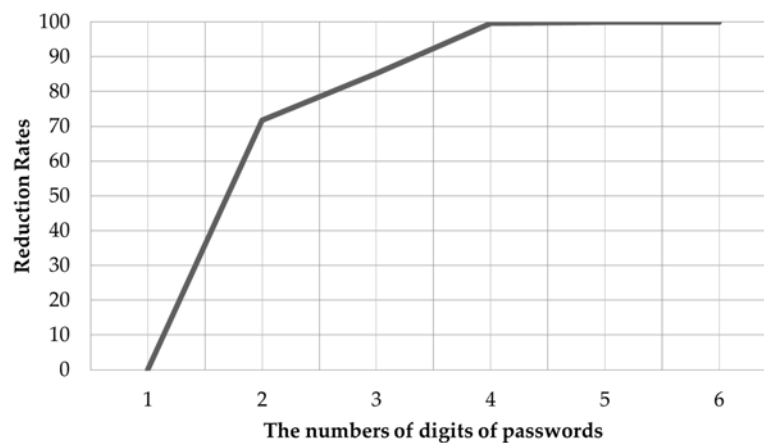


Figure 15. Reduction rates according to the numbers of digits of passwords.

If the number of digits of the passwords were one, the total number of cases of passwords would be 10. However, the reduction rate would be zero because the user took only one action for each password, and the number of estimated passwords would also be 10. Even when the number of digits of passwords was only increased to two, the reduction rates would increase drastically because the

total number of cases increases by a power of 10, but the number of estimated passwords in the present paper was not large enough to the extent that the number exceeded 10.

4.2. Reduction Rates for Number of Cases by the Number of Overlapping Digits

Figure 16 shows the rates of reduction of the numbers of cases according to the numbers of overlapping digits calculated on the basis of four-digit passwords. It can be seen that as the number of overlapping digits increased, the reduction rate decreased. This is because, if all the numbers in four digits were assumed to be the same, the user would take pressing actions at the same location, leading to a wider range of passwords that could be estimated. On the contrary, when the number of overlapping digits decreases, the range of movements of pattern increases and the range of locations of pressing actions would also increase, leading to narrower ranges of estimation.

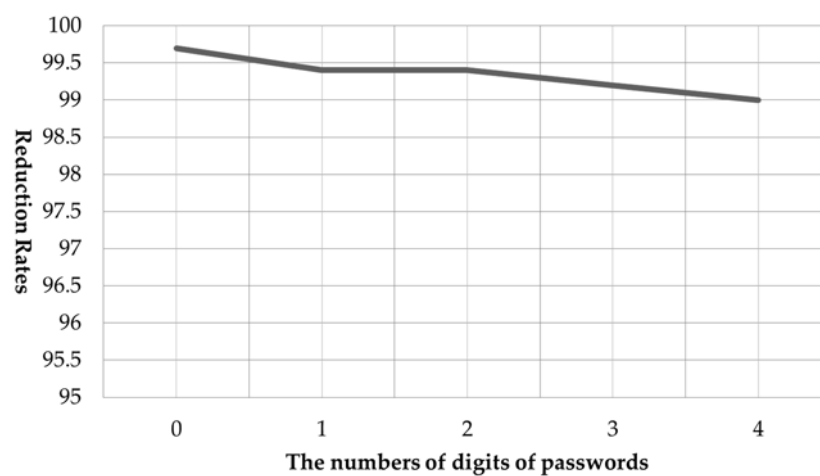


Figure 16. Reduction rates according to the numbers of overlapping digits (on the basis of four-digit passwords).

4.3. Reduction Rates for the Number of Cases According to Pattern Complexity

On reviewing Figures 15 and 16 once again, it can be seen that the rate of reduction of the number of cases increased as the number of digits of passwords increased and the number of overlapping digits decreased. This means that the rate of reduction of the number of cases decreased when the motions taken by the user to input passwords were wider and more complex and the locations where the motions were taken were not overlapping and were more complicated. Organized according to the number of digits, the reduction rates according to the complexity of user's password patterns can be explained with Figure 17. It was shown that when the actions taken by the user to input the password were more complicated, the reduction rate was higher.

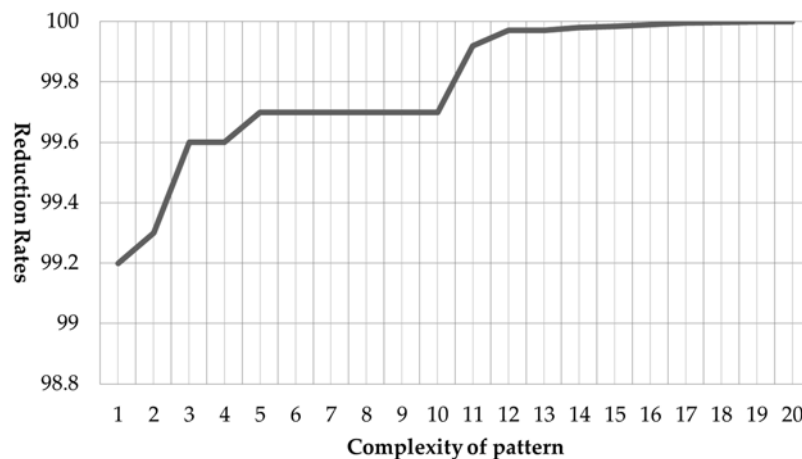


Figure 17. Reduction rates according to the complexity of patterns.

4.4. Binary Classification Result

The precision, recall factors, and *F*-scores calculated in 20 test cases are as shown in Table 8.

Table 8. Binary classification result.

Test Case	Password	Predicted Passwords	Numbers of Predicted Passwords	Precision	Recall Factor	F-Score
1	1234	1234, 4560, 7890	3	0.333	1.000	0.500
2	2580	1470, 2580, 3690	3	0.333	1.000	0.500
3	1333	1222, 1333, 4555, 4666, 7888, 7999, 0000	7	0.143	1.000	0.250
4	2000	1444, 1777, 1000, 2555, 2888, 2000, 3666, 3999	8	0.125	1.000	0.222
5	1399	1255, 1288, 1366, 1399	4	0.250	1.000	0.400
6	1357	1357, 1350, 4680	3	0.333	1.000	0.500
7	1733	1733, 1766, 4033, 4066	4	0.250	1.000	0.400
8	7597	4264, 7297, 7597	3	0.333	1.000	0.500
9	9054	6821, 6021, 9054	3	0.333	1.000	0.500
10	8642	0975, 0972, 8642	3	0.333	1.000	0.500
11	75920	75920	1	1.000	1.000	1.000
12	39547	39547, 39540	2	0.500	1.000	0.667
13	13333	13333, 46666, 79999	3	0.333	1.000	0.500
14	10000	14444, 17777, 10000, 25555, 28888, 20000 36666, 39999	8	0.125	1.000	0.222
15	79831	46531, 79831, 79864	3	0.333	1.000	0.500
16	976154	976154	1	1.000	1.000	1.000
17	391736	281714, 391736, 392825	3	0.333	1.000	0.500
18	798105	798105	1	1.000	1.000	1.000
19	800000	144444, 177777, 100000, 200000, 255555, 288888, 366666, 399,999 400,000, 4777777, 500000, 588888, 699999, 700000, 800000	15	0.067	1.000	0.125
20	139712	136412, 139012, 139712, 469745	4	0.250	1.000	0.400

The precision is the probability for the actual password to be included in the predicted passwords, the recall rate is the probability for predicted passwords to be included in the actual passwords, and the *f*-score is a score obtained by the formula; $f\text{-score} = 2 \times (\text{precision} \times \text{recall} / (\text{precision} + \text{recall}))$ [24]. The precision was identified to be low through calculations with values not exceeding 33% in most cases because although the number of cases of passwords that could be 1000 in the case of four digit passwords was reduced to 1~7, the actual number of passwords was fixed to 1. However, since all the groups of passwords predicted using the method proposed in the present paper included actual passwords, the recall factors were identified as 100% in all cases.

4.5. Energy Efficient

We have also set forth the energy efficiency of the smartwatch and smartphone with regard to password prediction.

Figure 18 shows a graph of the amounts of energy consumed in the experiment described in the present paper. The upper side shows the energy consumed when one test case is experimented. One test case took approximately 5 s of experimental time and both the smartwatch and smartphone showed a charge amount of 99.8%. The bottom side is a report on the amount of energy consumed when all the 20 test cases were experimented. Approximately 120 s of experimental time was spent when the 20 test cases were experimented. The smartwatch showed a charge amount of 96.8% with an energy consumption of 3.2%, while the smartphone showed a charge amount of approximately 98% with a battery energy consumption of approximately 2%. The reason why the battery consumption of the smartwatch was higher was that the smartwatch was loaded with a battery with lower specification than that of the smartphone, considering the size and specification of the smartwatch [12,13]. The fact that the period of use of the smartwatch was longer than that of smartphone was also a reason for this effect.

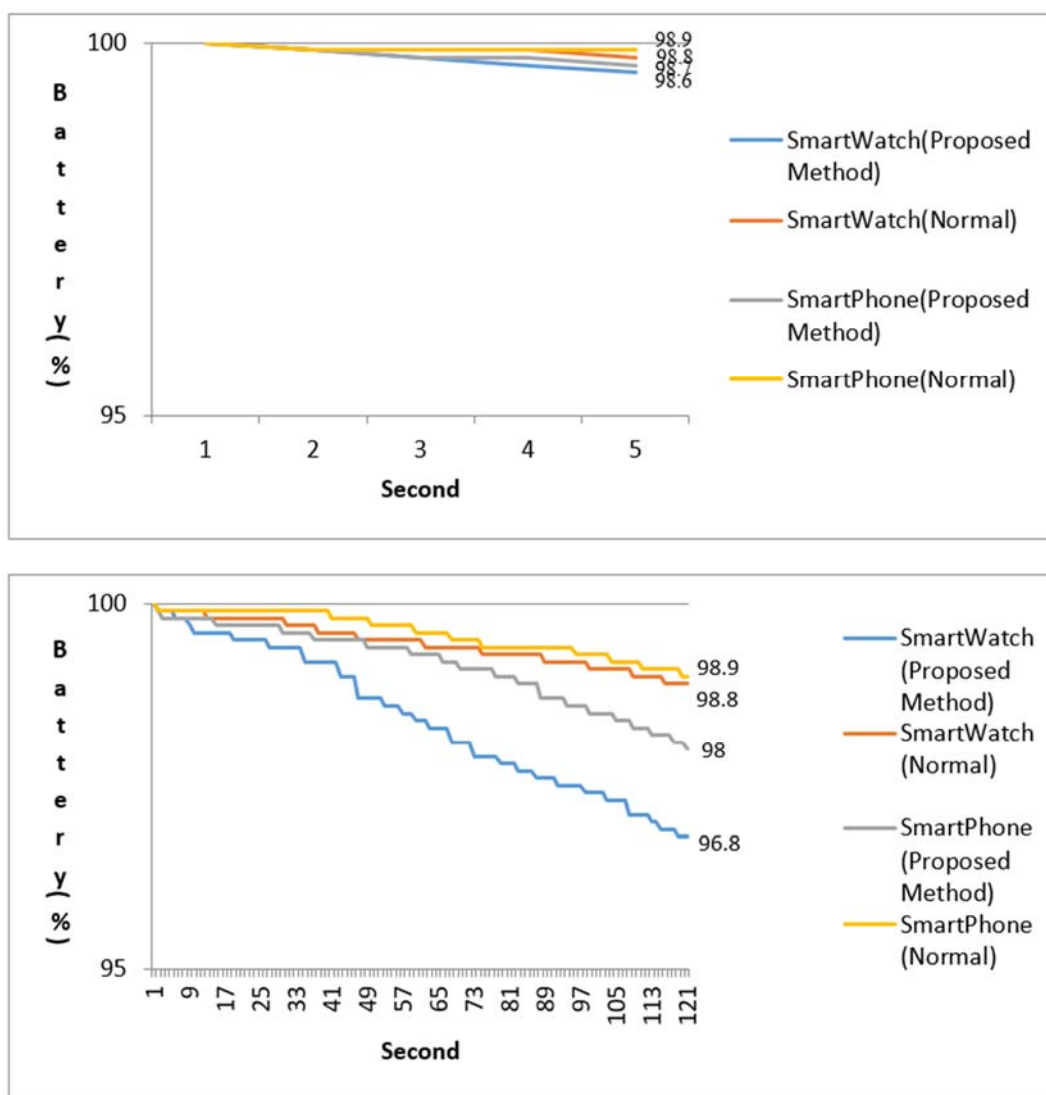


Figure 18. Energy efficiency (upper side: Experiment 1 test case, bottom side: Experiment 20 test case).

5. Related Work

Studies of attacks on components of smart devices such as sensors have mainly dealt with threats that may arise from using smart device sensors, rather than from the weaknesses of algorithms that can occur within the code of the application that runs the sensor [25,26]. Most smart devices are installed not with only motion sensors, but with other sensors such as various cameras, global positioning system (GPS), and microphones. Previous studies have been conducted focusing on privacy infringement using information from these sensors. For instance, [27] designed a Driver Detection System (DDS) that calculates the change values of the motion sensor of the smartphone to detect the vehicle driving direction. This system first detects the NFC (Near Field Communication) and audio of the firmware installed in the vehicle with the smartphone to detect the presence of the driver in the driver's seat nearby, and thereafter calculates the change values of motion sensors such as the accelerometer and gyroscope sensor to detect the driving speed and direction. In addition, the author of [28] injected malware that operates sensors into the smartphone to expose the privacy of user-based information leaked from sensors other than the motion sensor, that is, the microphone, GPS data, and camera.

One of the interesting and sensitive pieces of information attackers aim to obtain in the field of security threats is information on passwords or pin codes. Such pieces of information can be predicted by expanding keystroke threats that can predict acts of typing on the smartphone screen.

Studies conducted before the commercialization of smartwatches first used motion sensors to confirm the keystrokes on smartphones. Both studies [29,30] utilized motion sensors to predict motions for typing on the virtual keyboard of a touch screen and used the degree of change from the gyroscope sensor and accelerometer sensors. The authors of [29] have particularly conducted experiments where the users did not type at a fixed location but did type on handheld smart devices, and additionally mentioned the relationship between vibration state and keystrokes in such cases, and the author of [30] compared results from gyroscope sensors with those from accelerometer sensors to show that gyroscope sensors were superior to accelerometer sensors in terms of precision.

Studies on keystrokes as such have been expanded to the prediction of passwords or pin codes.

In [31], the movements of motion sensors inside the smartphones were monitored by installing a Trojan application. The affected sensors were the gyroscope and accelerometer sensors, and the application learned behaviors such as the touch events of the user, and predicted the actions conducted by the user on the touch screen based on the learning. Password stealing was one of the experiments in the current study. The current study conducted the experiment while expanding PIN codes consisting only of numbers to four, six, and eight digits, and showed a prediction rate of 80%. The author of [32] uses only accelerometer sensors and predicts passwords with character strings rather pin codes consisting of numbers. The author predicted the passwords by dividing smartphone screens into certain rectangles in proportion to the sizes of the screens and calculating the distances to coordinate values being touched.

After smartwatches were commercialized, the threats of various keystrokes were demonstrated based on the movements of the smartwatch [33–36]. For instance, studies that predicted the movements of the smartwatch to predict keyboard typing logs [33] or smartphone pin codes [34] were conducted. The author of [33] predicted English words typed on the keyboard of a desktop or laptop computer based on signals from motion sensors such as the smartwatch's accelerometer sensors and gyroscope sensors. The position of the wrist changed according to the position of alphabets on the keyboard and the degree of change, which was measured by the smart sensor's motion sensor, were used to predict the words being typed. Similarly, the author of [34] predicted PINs using motion sensors such as the accelerometer and gyroscope sensor, based on the movements of the smartwatch when the user entered the pin number of the smartphone after wearing a smartwatch. The pin number prediction of the relevant study adopted the random forest learning method, and the signals of the x-, y-, z-axes of the gyroscope and the accelerometer were used as features of the random forest learning. Similarly, the author of [35] also predicted pin numbers wearing a smartwatch. In the relevant study, the author

made a 12-key number input device for pin number input by himself and predicted the pressed pin numbers through machine learning (deep learning). Our study was most similar to studies [34,35] in that the purpose of the study was to predict passwords such as PINs pressed while wearing a smartwatch. However, studies [34,35] predicted pin numbers based on machine learning. This means that the sensor values recorded in the smartwatch could be used again in learning, and the features used in learning could be also collected. Such processes mean that quite some effort and time should be spent in deriving predictable results. On the contrary, we predicted the passwords only through a series of calculation processes using only algorithms, without learning or feature collection, which naturally led to a reduction in the time and costs of prediction.

6. Conclusion

In the present paper, the threat of sufficient leakage of user's password patterns through the motion recognition sensors embedded in smartwatches that are prominent in wearable markets, was proved. Most smartwatches are provided with motion recognition sensors to expand the functionality and to overcome the limitations of hardware in smartwatches. However, users' passwords can be sufficiently leaked through these motion recognition sensors. Therefore, it can be said that, ironically, wearable devices such as smartwatches released for increasing speed and convenience, may be subject to security threats such as password pattern leakage, due to that fact that those wearable devices are worn by the users. In the present paper, passwords were predicted by collecting the patterns of passwords entered by users wearing a smartwatch using accelerometer sensors, which are motion recognition sensors. Basically, if the number of digits of passwords was assumed to be four, the number of cases of possible passwords is $10^4 = 1000$. However, according to the method proposed in the present paper, three to eight passwords were predicted for each of the four-digit passwords depending on the overlapping numbers, showing a reduction rate for the number of cases, of 99%, and the predicted passwords showed high accuracy. In the current study, the experiment was expanded to predict passwords with more than four digits. In the results of this experiment, the reduction rate for the number of cases decreased as the number of digits of the passwords increased, or as the number of overlapping numbers of passwords decreased. This means that the information for the prediction of passwords increased as the number of numbers not overlapping increased. On the contrary, the method proposed in the present paper showed a limitation in that the number of cases did not decrease at all in the case of passwords consisting of only one number of one digit passwords. However, the above limitation could be overcome because bank users do not set their important passwords as a single number or a one-digit password, pursuant to the password protection policy [37].

We plan to carry out future works with more extended scenarios. The password prediction system proposed in the present paper simply transmits the sensor values from the smartwatch to the connected smartphone, and the transmitted sensor values are again transmitted to the server connected to the smartphone. First, this may involve a weak point because it can be subject to spatial restriction in security threat scenarios, and we plan to overcome this weak point, because attackers wish to capture target information without being subject to spatial restriction. Therefore, their first goal is usually to steal the sensor values from the smartwatch within the smartphone, and secretly retransmit the sensor values from the smartphone to the cloud environment. Second, the user's act of transmitting sensor values may be a limitation. In the present paper, sensor values were transmitted assuming that the act of inputting passwords was a prototype, and the point of transmitting sensor values was set to the point of completion of transmission. However, the act of transmitting sensor values can be a limitation because such behaviors can sufficiently occur in everyday life. To overcome the foregoing, we plan to approach the issue with a reinforced scenario such as enabling the user to obtain sensor values only when the user conducts the act of entering the password near the relevant GPS address after storing the GPS values of the coordinates of the bank and ATM.

Acknowledgments: This work was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2016-R2718-16-0035) supervised by the IITP (National IT Industry Promotion Agency), the Basic Science Research Program through the NRF funded by the Ministry of Education (NRF-2015R1C1A1A02037561) and the 2016 Yeungnam University Research Grant.

Author Contributions: Jihun Kim and Jonghee M. Youn conceived, designed and performed the experiments; Jihun Kim analyzed the data; Jihun Kim and Jonghee M. Youn wrote the paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Rawassizadeh, R.; Price, B.A.; Petre, M. Wearables: Has the age of smartwatches finally arrived? *Commun. ACM* **2015**, *58*, 45–47. [CrossRef]
2. Chernbumroong, S.; Atkins, S.A.; Yu, H. Activity classification using a single wrist-worn accelerometer. In Proceedings of the 5th International Conference on Software, Knowledge Information, Industrial Management and Applications (SKIMA), Benevento, Italy, 8–11 September 2011.
3. Hinckley, K.; Pierce, J.; Sinclair, M.; Horvitz, E. Sensing techniques for mobile interaction. In Proceedings of the 13th Annual ACM Symposium on User Interface Software and Technology, San Diego, CA, USA, 6–8 November 2000.
4. Rawassizadeh, R.; Tomitsch, M.; Nourizadeh, M.; Momeni, E.; Peery, A.; Ulanova, L.; Pazzani, M. Energy-Efficient Integration of Continuous Context Sensing and Prediction into Smartwatches. *Sensors* **2015**, *15*, 22616–22645. [CrossRef] [PubMed]
5. Udoh, E.S.; Alkharashi, A. Privacy risk awareness and the behavior of smartwatch users: A case study of Indiana University students. In Proceedings of the Future Technologies Conference (FTC), San Francisco, CA, USA, 6–7 December 2016.
6. A PowerPoint Presentation by Paul E. Tippens, Professor of Physics Southern Polytechnic State University, 2017. Technical Paper. Available online: https://www.stcharlesprep.org/01_parents/vandermeer_s/Useful%20Links/Honors%20Physics/pdf%20lectures/Acceleration.pdf (accessed on 29 June 2017).
7. Dadafshar, M. *Accelerometer and Gyroscopes Sensors: Operation, Sensing, and Applications*; Maxim Integrated: San Jose, CA, USA, 2014.
8. The Earth's Gravitational Field. Technical Paper. Available online: http://www.gpsg.mit.edu/12.201_12.501/BOOK/chapter2.pdf (accessed on 29 June 2017).
9. Takeda, R.; Tadano, S.; Todoh, M.; Morikawa, M.; Nakayasu, M.; Yoshinari, S. Gait analysis using gravitational acceleration measured by wearable sensors. *J. Biomech.* **2009**, *42*, 223–233. [CrossRef] [PubMed]
10. Liu, M. A study of mobile sensing using smartphones. *Int. J. Distrib. Sens. Netw.* **2013**. [CrossRef]
11. Furutani, K.; Kato, M.; Tsuru, T. Low-Pass Filter. U.S. Patent 5,668,511, 16 September 1997.
12. Welch, G.; Bishop, G. *An Introduction to the Kalman Filter*; University of North Carolina: Chapel Hill, NC, USA, 1995.
13. LG Urbane. Available online: http://www.gsmarena.com/lg_watch_urbane_w150-7680.php (accessed on 29 June 2017).
14. Samsung Galaxy S6. Available online: http://www.gsmarena.com/samsung_galaxy_s6-6849.php (accessed on 29 June 2017).
15. Hardyck, C.; Petrinovich, L.F. Left-handedness. *Psychol. Bull.* **1977**, *84*, 385. [CrossRef] [PubMed]
16. Watch Handedness. Available online: <https://en.wikipedia.org/wiki/Watch#Handedness> (accessed on 29 June 2017).
17. Is It Acceptable to Wear a Watch on the Right Wrist? Available online: <http://www.askandyaboutclothes.com/forum/showthread.php?116570-Is-it-acceptable-to-wear-a-watch-on-the-right-wrist> (accessed on 29 June 2017).
18. Why Wear a Watch on the Wrist Where You're Hand Dominant? Available online: http://www.reddit.com/r/Watches/comments/1wzub5/question_why_wear_a_watch_on_the_wrist_where/ (accessed on 29 June 2017).
19. Annett, M. *Handedness and Brain Asymmetry: The Right Shift Theory*; Psychology Press: Leicester, UK, 2002.
20. Yan, S.; Soh, P.J.; Vandenbosch, G.A.E. Wearable dual-band composite right/left-handed waveguide textile antenna for WLAN applications. *Electron. Lett.* **2014**, *50*, 424–426. [CrossRef]

21. Why Don't Apple Have Left Handed Watches? Available online: <https://www.iphonetricks.org/5-reasons-to-wear-the-apple-watch-on-your-left-hand/> (accessed on 29 June 2017).
22. Android Wear Left Handed Mode? Available online: https://www.reddit.com/r/AndroidWear/comments/3f77fs/left_handed_mode/ (accessed on 29 June 2017).
23. How to Set Up the Apple Watch for Left-Handed Use. Available online: <http://www.imore.com/how-set-apple-watch-left-handed-use> (accessed on 29 June 2017).
24. Goutte, C.; Gaussier, E. A probabilistic interpretation of precision, recall and F-score, with implication for evaluation. In Proceedings of the European Conference on Information Retrieval, Santiago de Compostela, Spain, 21–23 March 2005.
25. Nahapetian, A. Side-Channel Attacks on Mobile and Wearable Systems. In Proceedings of the 13th IEEE Annual Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2016.
26. Spreitzer, R.; Moonsamy, V.; Korak, T.; Mangard, S. Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *arXiv* **2010**, arXiv:1611.03748.
27. Chu, H.; Raman, V.; Shen, J.; Kansal, A.; Bahl, V.; Choudhury, R.R. I am a smartphone and I know my user is driving. In Proceedings of the 2014 Sixth International Conference on Communication Systems and Networks (COMSNETS), Bangalore, India, 6–10 January 2014.
28. Cai, L.; Machiraju, S.; Chen, H. Defending against sensor-sniffing attacks on mobile phones. In Proceedings of the 1st ACM Workshop on Networking, Systems, and Applications for Mobile Handhelds, Barcelona, Spain, 17 August 2009.
29. Cai, L.; Chen, H. TouchLogger: Inferring Keystrokes on Touch Screen from Smartphone Motion. In Proceedings of the 6th USENIX conference on Hot topics in security, San Francisco, CA, USA, 8–12 August 2011.
30. Liang, C.; Chen, H. On the practicality of motion based keystroke inference attack. In Proceedings of the International Conference on Trust and Trustworthy Computing, Vienna, Austria, 13–15 June 2012.
31. Xu, Z.; Bai, K.; Zhu, S. Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors. In Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, Tucson, AZ, USA, 16–18 April 2012.
32. Owusu, E.; Han, J.; Das, S.; Perrig, A.; Zhang, J. ACCESSory: Password inference using accelerometers on smartphones. In Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications, San Diego, CA, USA, 28–29 February 2012.
33. Wang, H.; Lai, T.T.-T.; Choudhury, R.R. Mole: Motion leaks through smartwatch sensors. In Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, Paris, France, 7–11 September 2015.
34. Sarkisyan, A.; Debbiny, R.; Nahapetian, A. WristSnoop: Smartphone PINs prediction using smartwatch motion sensors. In Proceedings of the 2015 IEEE International Workshop on Information Forensics and Security (WIFS), Rome, Italy, 16–19 November 2015.
35. Beltramelli, T.; Risi, S. Deep-Spying: Spying Using Smartwatch and Deep Learning. Master's Thesis, IT University of Copenhagen, Copenhagen, Denmark, December 2015.
36. Liu, X.; Zhou, Z.; Diao, W.; Li, Z.; Zhang, K. When good becomes evil: Keystroke inference with smartwatch. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015.
37. SANS Technology Institute. Password policy. Available online: <https://www.sans.edu/student-files/projects/password-policy-updated.pdf> (accessed on 29 June 2017).

