*electronics*

*Article*

# Advanced Authentication Method by Geometric Data Analysis Based on User Behavior and Biometrics for IoT Device with Touchscreen

**Jiwoo Lee [1], Sohyeon Park [1], Young-Gon Kim [1,*], Eun-Kyu Lee [1,*] and Junghee Jo [2]**

[1] Department of Information and Telecommunication Engineering, Incheon National University, Incheon 22012, Korea; jw961129@inu.ac.kr (J.L.); shg5865@inu.ac.kr (S.P.)

[2] Department of Computer Education, Busan National University of Education, Busan 47503, Korea; dreamer@bnue.ac.kr

* Correspondence: hyper1003@inu.ac.kr (Y.-G.K.); eklee@inu.ac.kr (E.-K.L.)

**Abstract:** The Internet of Things (IoT) technology is rapidly being applied to real life, but the application of a corresponding secure and convenient authentication method is still in significant challenge. So far, pattern, password and fingerprint authentication are the most used methods, but it is important to address various security vulnerabilities and limitations of these approaches. In the case of fingerprint recognition, additional hardware such as a fingerprint scanner is required, which causes cost issues and could be vulnerable to fingerprint theft. To solve this problem, this paper proposes a model that uses both biometric and behavioral authentication at the same time. This method exploits the biometric authentication that measures the length of the contact region that occurs when three fingers are placed side by side on the touch screen or pad. In addition, it utilizes the behavioral authentication itself using three-finger L-shape touch, as well as secure geometric information generated by smart watch such as acceleration sensors. Therefore, this proposed model will be useful to implement more secure, rapid and user-friendly way of authentication in many practical busy and buzzling field where deal with sensitive private information.

**Keywords:** security; authentication; IoT; wearable device; machine learning

check for updates

**Citation:** Lee, J.; Park, S.; Kim, Y.-G.; Lee, E.-K.; Jo, J. Advanced Authentication Method by Geometric Data Analysis Based on User Behavior and Biometrics for IoT Device with Touchscreen. *Electronics* **2021**, *10*, 2583. https://doi.org/10.3390/electronics10212583

Academic Editor: Amir Mosavi

Received: 30 September 2021
Accepted: 20 October 2021
Published: 22 October 2021

## 1. Introduction

Recently the Internet of Things (IoT) is being used in many different fields as the cost issue is not as critical as before and therefore implementation of home IoT systems is also rapidly increasing day by day. In the case of the current home IoT system, wall pads which use a centralized way of controlling and managing devices connected to the home network is commonly used, and most of them use a touch screen to support a user interface. Some wall pads collect and use sensitive data from users without any proper secure processing by intentional neglect or ignorance of private data security. If access to these devices by non-family members is infrequent, significant issues may not arise, but when logging into a specific IoT device in a place frequented by unspecified people, blocking the access of unauthorized users should be considered a priority. In other words, IoT device access must be protected through authentication [1] which secure, fast and convenient. In principle, access by unauthorized users is not allowed, but it should not be overlooked that systems are exposed to numerous types of access attacks. This includes intentional tricky attacks as well as attempts out of simple curiosity.

The authentication methods most used in touch screen user interfaces are ones based on a password or PIN, but this method has several inconveniences and is currently used as a secondary authentication method because they may be difficult to remember because of the following reasons: a password of at least four to usually eight or more digits and characters is required and it is easy to forget over time. In addition, there is an inconvenience of having to change it frequently because there is a high possibility of exposure. These significant drawbacks cause similar problems in the next most common pattern recognition authentication. Pattern authentication is easy to use, but the one created is too simple, someone else can crack it simply using commonly used expected patterns. In addition, after user authentication, it is necessary to prepare for a smudge attack [2] that acquires authentication using the handprint remaining on the touch screen. It is also very vulnerable to shoulder-surfing attack [3], which observes the user's behavior using pattern authentication and then attacks by using the same authentication motion that is remembered later. Various behavior-based authentications used as an alternative to this pattern recognition method are inevitably vulnerable to both smudge and shoulder-surfing attacks. The most famous method of bio-based authentication used to compensate for this problem is the fingerprint recognition method because it is convenient to log in and of course each person has a unique fingerprint that is totally different from others, therefore identity authentication is possible. However, there are still many vulnerabilities and problems related to information security systems. Of note, an experiment that showed the loopholes of fingerprint recognition technology conducted at the University of Michigan in the United States pointed out that biometric information can't be changed once leaked therefore it is much more hazardous than the classical security system. Fingerprints are used as one of the means of authenticating not only IoT networks, but also in the community for other purposes, so it is an authentication method with a very high risk of exposure. For this reason, the fingerprint recognition systems applied to facilities where security is important are currently regarded as an auxiliary security medium [4]. In addition to these problems, not all IoT devices have a touchscreen capable of fingerprint authentication, because there are many restrictions such as mechanical space and cost for additionally installing hardware such as a fingerprint scanner.

Currently, the mainly used authentication models are vulnerable to various attacks. The most used password or pattern make it easy for malicious third parties to check and abuse the authentication process. Fingerprint authentication models are also dangerous because leakage can cause serious damage. Since finding a new way to replace this most easily used authentication method was a new challenge, more secure and upgraded model while taking advantage of the advantages of each currently used authentication model is proposed [2,3].

In this context, this paper proposes the following methods to integrate and solve these problems and explains the experimental results. The method exploits the biometric authentication that measures the length of the contact region that occurs when three fingers are placed side by side on the touch sensor pad. In addition, it utilizes the behavioral authentication itself using three-finger L-shape touch, as well as secure geometric information generated by smart watch sensors such as acceleration sensors. It can complement the disadvantages of existing behavior-based authentication such as PIN or password and biometric authentication such as fingerprint and use of the smart watch's sensor to reflect the user's behavioral characteristics enhance security.

## 2. Related Research

Recently, a lot of research has been done on how to integrate behavioral and biometric-based authentication and IoT authentication so that users can quickly access systems with high reliability.

### *2.1. Fingerprinting*

The most popular authentication model in recent years is fingerprint recognition. This method is easy, fast, and secure, but not all IoT devices have fingerprint scanners. To this end, attaching a fingerprint scanner implies an additional cost, and hardware other than the built-in fingerprint scanner also requires room for physical space. This problem makes attaching a fingerprint scanner to an IoT device undesirable. In addition, fingerprints are also used in important parts of real life, such as background checks for criminal history and immigration history and in banking. This means that if fingerprint data is exposed at least once to a malicious attacker, it can be subsequently used for a dangerous crime. and it should also be noted that once exposed, it is impossible to change fingerprints as easily as PINs or passwords for life, rendering fingerprint authentication services unusable again if exposed.

### *2.2. Behavior and Biometric Authentication*

Authentication methods such as PINs passwords and patterns are now popular, but vulnerable to smudging attacks or shoulder-surfing attacks. The most studied alternative method authentication is behavior and biometric authentication, an authentication method using users' unique behavior and biometric characteristics. These include recognizing and checking the user's walk with a camera to open the door [5], keystroke authentication that measures the user's keyboard input speed or habits [6], and gesture-based authentication that uses the user's own gestures [7]. Various behavioral and biometric authentication schemes are being studied, but the biggest problem with these certification methods is time, as the behavioral characteristics of users change slightly over time, therefore, computers trained with existing data will not allow successful authentication without re-entering the changed characteristics.

### *2.3. IoT Certicication*

Most IoT devices cannot use typical authentication methods. There are many IoT devices that do not have a keypad or display, so it is difficult to use authentication methods such as passwords, patterns and fingerprints. To use these authentication methods, installing fingerprint scanners or wireless communications devices for communication authentication is limited for reasons such as cost and space. Nowadays, home IoT systems typically use a centralized management method employing touchscreens. This allows IoT devices with various authentication methods to be integrated and managed via the touchscreen. Currently, the types and uses of IoT devices are very broad. For these many IoTs, each authentication method should have low dependency on a specific interface or sensor, require no hardware modification of existing products, impose no restrictions on device size and installation, security, and provide reliable authentication results. The most ideal IoT authentication method must satisfy all the above conditions.

## 3. Model Overview

The proposed model uses both behavior-based authentication and biometric authentication and uses a smart watch to leverage behavioral capabilities. The proposed authentication method is completed by the act of wearing a smart watch, spreading three fingers and swiping in an L-shape.

The length between the three fingers is used as data to obtain data that is easier to use and more secure than the currently used authentication models [8]. Since the length between fingers varies from person to person, it can be used as a biological variable with unique characteristics. In addition, since all users also have different behavior patterns, their gestures are all different from the perspective of the starting point, acceleration, touch area, etc., so these characteristics can be used as behavior-based variables. To use these two properties, the touch of the L-shape that best represents them is used. It can clearly measure the distance between fingers and make use of all the various behavioral features of the gesture.

### *3.1. Threat Model*

The threat model used in the experiment is as follows: when a malicious attacker who is not registered in the proposed model performs authentication, the success rate of malicious attacks depends on how much the attacker knows how to authenticate the model. The attacker may peek at the user's authentication performance action and infer the authentication process from any fingerprint marks remaining on the touch screen. In addition, another user may be an attacker attacking another authenticated user. An attacker who is familiar with all authentication processes can be the most dangerous attacker, so we consider this case as the main threat model.

### *3.2. Behavior-Based Authentication*

The user swipes an L-shape to the touchscreen using three fingers on a screen. Such gesture authentication is simpler than PINs or passwords, as it does not require any memorization. However, there are many problems if authentication is done only with this motion. As previously stated, it is vulnerable to smudge attack and shoulder-surfing attacks, where an attacker peeks at the user's motion or marks left on the touchscreen. These behavior-based authentication methods also changes over time. Therefore, implementing highly secure authentication using only behavior-based authentication is not a good solution.

### *3.3. Biometric Authentication*

In behavior-based authentication, biometric authentication is used to solve the problem of attributes changing over time. This model uses the distance between the fingers rather than the fingerprints which have a high risk of abuse. This information is considered an authentication method with increased security because the length and thickness of the fingers differ from person to person when three fingers are spread out.

### *3.4. Smartwatch Motion Authentication*

When using an authentication method that combines behavior-based authentication and biometric authentication, the smart watch wearing method is used together to confirm whether the user is close or not [9]. The important point is that the user's behavioral characteristics are also reflected in the above authentication method. When these behavioral characteristics are applied, the main factors that can judge the user are increased, which results in an effective increase in security [10]. Because each user has different wrist movement and approach speed, it is possible to perform a geometrical analysis using the smart watch's accelerometer and gyroscope sensor [11].

### *3.5. Model Diagram and Authentication Process*

The proposed model consists of a touch screen used by IoT devices, a user's smart watch, and a computing server for machine learning data analysis as shown in the Figure 1.

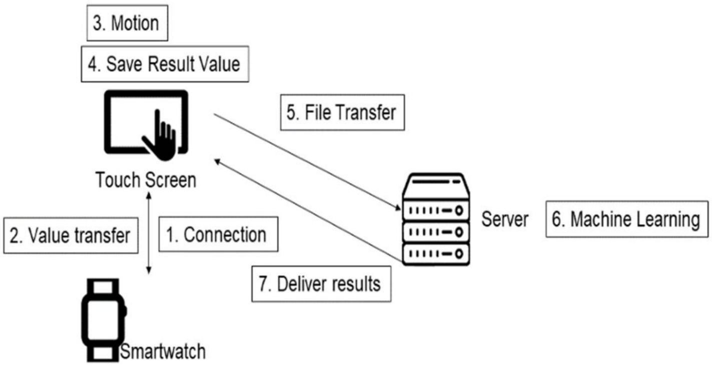


**Figure 1.** Model diagram and Data flow for authentication.

The order of operation of our authentication model is as follows:
Authentication Process:

(1) Connection: Connect the touchscreen to the smartwatch via Bluetooth.
(2) Transfer Behavior Data: The smartwatch continues to deliver accelerometer and gyroscope dataset until the end of operation.
(3) Perform Authentication: The user swipes the L-shape with three fingers on the touch screen. In the registration stage, this operation is performed 20 times, and after the

user's behavior feature is extracted, the actual use for an authentication process only needs to be done once.

(4) Save Result: Calculate the geometric distant when the actions entered by the user on the touchscreen with each feature and save the result and the smartwatch sensor interval result as a text file, respectively.

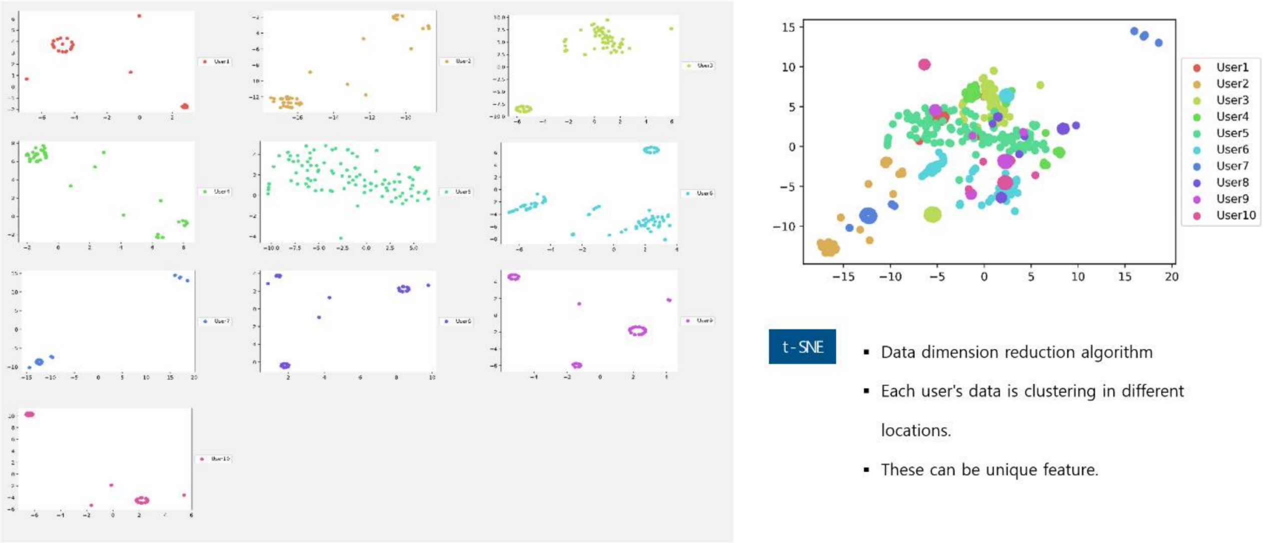
(5) File Transfer: Transfer the generated two text files to a specific storage space on the server.

(6) Machine Learning: The server performs machine learning using two files delivered. Isolation Forest method, which performs well among several classification models is used in this stage.

(7) Share Result: The server delivers machine learning result to the IoT device which has touchscreen.

### 3.6. Securing Unique Dataset with t-SNE (t-Distributed Stochastic Neighbor Embedding)

The t-SNE algorithm, a data dimension reduction algorithm, was exploited to check whether the collected data really represents the unique characteristics of an individual. Data from 10 users were used in this experiment. In the Figure 2, each user's data is in a different place. The user data are clearly different from each other. Therefore, it was confirmed that the collected user data had sufficiently unique characteristics.



- Data dimension reduction algorithm
- Each user's data is clustering in different locations.
- These can be unique feature.

**Figure 2.** Distribution of the user using t-SNE algorithm.

## 4. Description of the Model

In this section, the new authentication method using biometric data and behavioral data together will be described in detail by major components.

### 4.1. Touch Screen

On a touchscreen, when a user swipes L shape, the touchscreen uses input features to calculate behavior-based and biometric features, respectively. These calculated variables are stored as text files on the touchscreen and passed to the server.

#### 4.1.1. Behavior-Based Variables

The method uses two types of behavior data for authentication. First, it uses three fingers to make L-swiping gestures. This is the simplest gesture to ensure that the data to be used in the biometric authentication is fully available. Also, it's easy to remember because of its simplicity. For this, the method uses six features for gestures in behavior-based authentication as follows:

- Total distance: Total distance of movement ($\sum_{i=1}^{n} \overline{X_i X_{i-1}}$, $n$ is the length of the sequence, $X$ is the touch point)
- Displacement: distance between the start and end points ($\overline{X_0 X_n}$)
- Time: Time from touch start to end ($T_e - T_s$)
- Touch speed: average touch speed sequence ($\frac{1}{n} \sum_{i=1}^{n} \frac{\overline{X_i X_{i-1}}}{T_i - T_{i-1}}$)
- Touch area: mean of the touch area sequence ($\frac{1}{n} \sum_{i=0}^{n} M_i$)
- Angle: Mean of the angular sequence between the horizontal line and two points ($\frac{1}{n} \sum_{i=1}^{n} \left( \mathrm{atan}\left( \frac{\overline{Y_i Y_{i-1}}}{\overline{X_i X_{i-1}}} \right) \times \frac{180}{\pi} \right)$).

The behavior-based authentication variable is calculated using six variables and since this variable is the value of one finger, if three fingers are used, a total of 18 action-based authentication variables are used in the authentication method.

### 4.1.2. Biometric Variables

This method straightens three fingers of a user and measures the distance between each finger. The distance between fingers varies from person to person, so it can be used as a unique feature for authentication. It also has the strength that the value does not change over time. When the user performs authentication, our method performs authentication by straightening the three fingers as shown in Figure 3. It uses seven features for biometric-based authentication as follows.

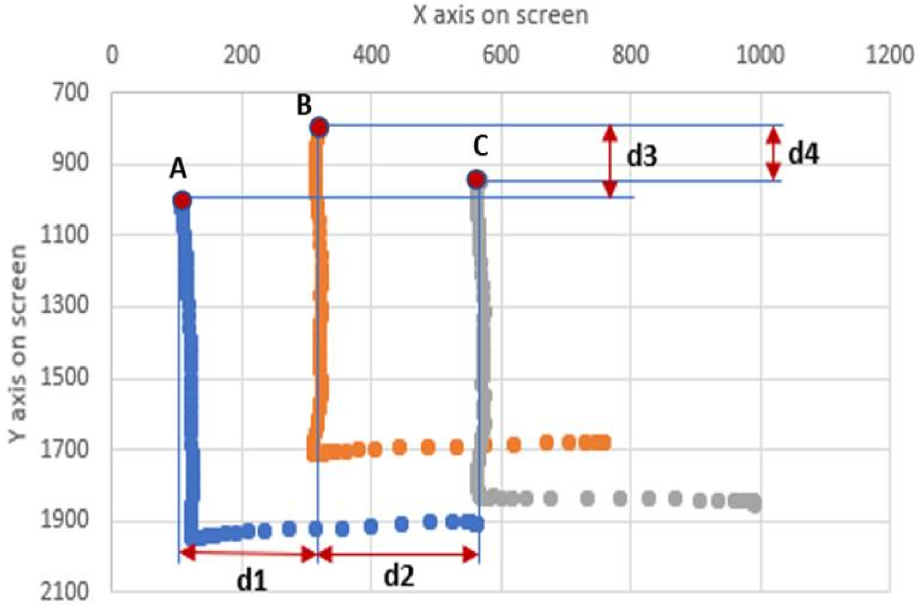


**Figure 3.** Example of L-swiping coordinates on a touchscreen.

- $\overline{\mathrm{AB}}$: Straight distance between A and B;
- $\overline{\mathrm{BC}}$: Straight distance between B and C;
- $\overline{\mathrm{CA}}$: Straight distance between C and A;
- d1: x distance between A and B;
- d2: x distance between B and C;
- d3: y distance between A and B;
- d4: y distance between B and C.

When using three fingers, the model calculates biometric variables using each distance of three fingers, resulting in a total of seven variables. Therefore, the total number of variables calculated on the touch screen is 25, and the calculated values of biometric variables vary according to the order of touch input on the touch screen. So, the input touch events must be sorted in the smallest order of x, and the swap function ensures that $x$ is stored in the array in the smallest order in each of the various touch sequences.

#### 4.1.3. Receiving Smartwatch Values

The smartwatch value is received by the touchscreen using a Bluetooth connection. The touchscreen continues to connect to the smartwatch until the user has completed authentication then terminates the connection when the user finishes typing. The smart watch calculates and sends the accelerometer and gyroscope values, and the touch screen averages the values of the smart watch parameters and uses them.

#### 4.1.4. Store Variables

The 25 behavioral and biometric variables calculated on the touchscreen and the sensor values received via the smartwatch are stored in the touchscreen internal storage as a text file. At this time, the values of the touchscreen and smartwatch variables are stored separately.

#### 4.1.5. File Transmission

In the touch screen, after saving the parameters of the touch screen and the smart watch as a file, it is necessary to perform the task of classifying the authorized users by using them. To implement this, machine learning is used, and because it requires a lot of computing power, touch screen sends the file to the server. At this point, we pass both files to POST at the same time.

### *4.2. Smart Watch*

The user must wear the smartwatch to use the behavioral features. L-swipe authentication provides information that can distinguish users because each user has different characteristics, such as the angle at which the wrist rotates and the speed at which the wrist moves. After the smart watch is connected to the touch screen using Bluetooth before the user performs authentication, the smart watch continuously transmits variables to the touch screen until the user completes the authentication action on the touch screen. Each variable is calculated before being transmitted from the smartwatch to the touch screen.

#### Calculate Variables

The model uses watches' accelerometer and gyroscope sensors to distinguish between users. This variable is passed to the touchscreen at a speed of 100 Hz. The touchscreen receives 100 $x$, $y$, and $z$ values of the sensors, a total of six features per second. We must process it to store a line of variables in a single action. In smartwatches, each variable is calculated as follows:

$$Mean_{acc,gyro} = \sqrt{x^2 + y^2 + z^2}$$

Each variable has a value from negative to positive, so we use the root mean square method for each element to find the magnitude of the accelerometer and gyroscope. Since tens to hundreds of variables need to be consolidated into one variable, the variables must be averaged on a touch screen.

### *4.3. Server*

In order to check whether the user who wishes to obtain authentication is a normal registered user, this model collects registration data 20 times in the initial registration procedure and extracts features by performing machine learning. After that, machine learning categorizes the extracted data during user authentication attempts to confirm whether this user is a registered user, and Gaussian mixture and isolation forest machine learning are used. We use 13 behaviors and biometric data per finger. Therefore, the proposed model using three fingers uses a total of 39 variables. A nonlinear classifier must be used to classify these high-dimensional data. The SVM model using a kernel, one of the representative classifiers, could not handle such high-dimensional data, so in order to reliably classify similar and completely different data, a clustering algorithm with several Gaussian distributions was used. This is because it is a way to sufficiently classify high-dimensional data because it uses a combination of multiple Gaussian distributions in a complex form.

Machine Learning

- Gaussian mixture is a clustering algorithm with multiple Gaussian distributions. Gaussian mixture does not have a class label, and similar patterns are clustered. This computes the probability of which data belong to a cluster and forms a cluster with a high probability of data distribution [12]. Among Gaussian mixture algorithms, 'covariance_type' and '$n$_components' parameters are specified. The 'covariance_type' is a string describing the type of covariance parameter used and be specified as 'spherical' because its non-linearity and '$n$_components' is a parameter that specifies how many mix components there are. The '$n$_components' as 2 because it is assigned as true or false.
- Isolation forest machine learning randomly selects dimensions to segment the space by any criterion. Space division can be expressed in dimensions and reference values, and multiple spatial divisions can be expressed in the form of decision trees. The more normal it is, the deeper it goes down the decision tree. Using these features, it is possible to separate normal and abnormal values based on how many times it is isolated by climbing down decision trees. The outliers are normalized from 0 to 1, so the larger than 0.5 and closer to 1 can be defined as outliers [13,14]. The 'contamination' is specified as the isolation forest parameter. This is the parameter used to define the threshold for the degree of contamination of the data set, i.e., the proportion of outliers in the data set and the sample score and specifies the condition as 0.08.
- Gaussian mixture and isolation forest together find the solution of classification with conflicting algorithms. These features are shown as accuracy differences. Thus, to compensate these shortcomings, the ensemble model is applied. Both Gaussian mixture and isolation forest use the same training dataset and test data with scale. This specifies that test data corresponding to false is returned as false in both the Gaussian mixture and isolation forest.

## 5. Experiments and Results

This section describes the contents of the experiment and evaluation of the proposed authentication method.

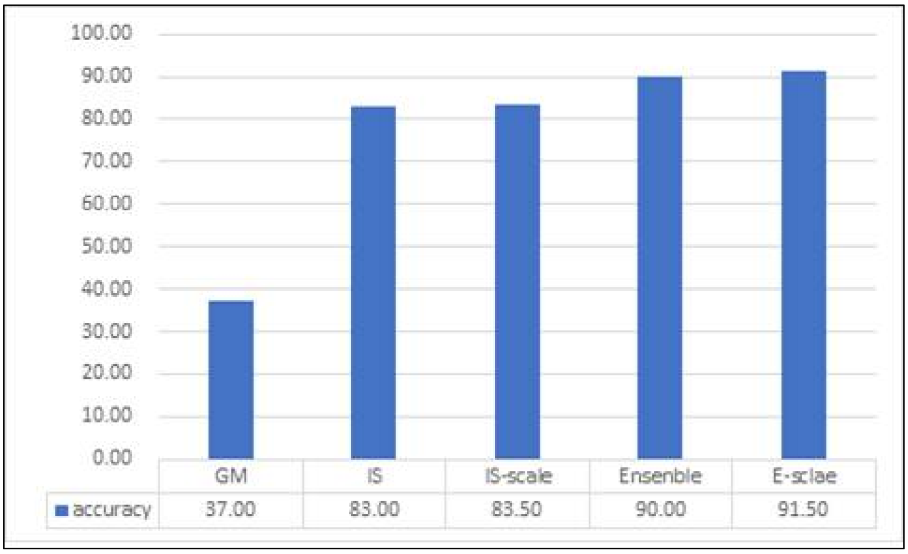
### *5.1. Experiments*

First, the experiment was conducted using a Samsung S10+ device as the touch screen and a Galaxy Watch 1 as the smart watch, and a personal PC was used as the server. Next, a total of 20 volunteers participated in the experiment. All subjects performed the three-finger L-shape swipe correctly in the proposed model and collected data. To collect sufficient data, 120 three-finger L-shape operations per person were performed. This collected data was used as a training set, and 100 out of 120 data were used as a test set, and the remaining 20 data were used. All experiments default on the training set of 100.

- Twenty volunteers provided their personal information [age (male/female)]: Ages: Teenager (3/0), 20's (7/4), 30's (1/0), 40's (2/3);
- The server PC specifications were as follows: CPU: AMD Ryzen 3 3200 G, RAM: 12 GB, SSD: 1 TB, OS: Windows 10;
- Touchscreen specifications were as follows: Samsung S10+, CPU: Exynos 9820, DRAM 8 GB, Touch Screen Dimension: 6.4 inches;
- Smart watch specifications were as follows: Samsung Galaxy Watch1, CPU: Exynos 9110, DRAM 1.5 GB.

### *5.2. Accuracy Evaluation*

In order to evaluate the accuracy of the proposed model, 100 datapoints were used for training and the test was performed by applying 20 data, and the accuracy was calculated by counting the number of times correctly judged out of the 20 tests. Accuracy was measured using Gaussian mixture and isolation forest algorithms, which are frequently used for data classification. Gaussian mixture shows an accuracy of 37% and isolation forest shows an accuracy of 83%. These results are not satisfactory, and the performance when applying Gaussian mixture is very poor as seen in Figure 4. A scaling method was used to improve the performance, and standardization method using mean-standard deviation was also used to unify the range of different data values for each variable. This method resulted in a performance improvement of about 5% in isolation forest. In the previous classification process, the data accurately classified by Gaussian mixture was often represented as misclassified in isolation forest. This is because machine learning finds solutions in different ways, so it is reasonable to utilize an ensemble model that combines the strengths of two machine learnings with different characteristics. This ensemble model shows an accuracy of 90%. It is clear that this is a model with sufficient accuracy. Finally, a model with an accuracy of 91.5% was obtained through an experiment through the scaling performed previously.



| | GM | IS | IS-scale | Ensenble | E-sclae |
|---|---|---|---|---|---|
| ■ accuracy | 37.00 | 83.00 | 83.50 | 90.00 | 91.50 |

**Figure 4.** Model accuracy evaluation [unit: %].

## 5.3. Evaluation by Training Dataset Size

In order to check the accuracy according to the size of the dataset, 20, 40, 60, 80, and 100 training data were collected, and the same test set was used. As shown in Figure 5, the accuracy according to the size of the training dataset does not show much difference between 20 and 100. On the contrary, it shows a result of a slight decrease in accuracy. The reason for these results seems to be that the presented model uses too many variables. Since the isolation forest uses the greedy algorithm to find a solution, if there are many variables or data, it is highly likely to fall into the optimal solution problem, but the ensemble model proposed in this paper offers some resistance to this problem.

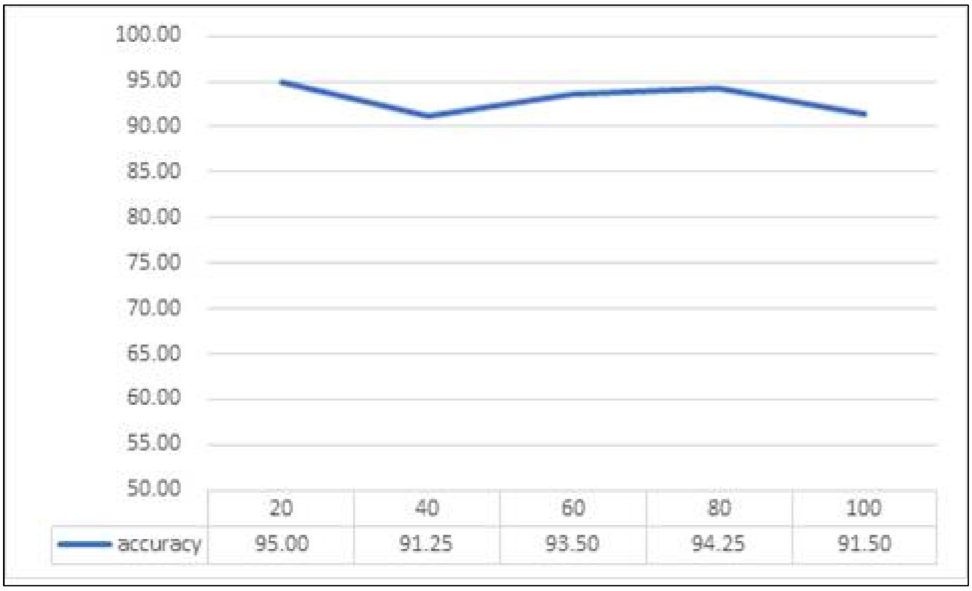


**Figure 5.** Accuracy according to training dataset size [unit: %].

### *5.4. Attack Resistance Assessment*

It is evaluated whether the proposed model is resistant to authentication-performing attacks. Most authentication processes are vulnerable to smudge attacks or shoulder surfing attacks as described in the previous section. In this experiment, it is determined that the user knows everything correctly, and each user's test set is used to measure the attack success rate. The experiment was conducted using data from 10 people with high accuracy, and the success rate was measured by training each data and performing an attack with the other nine test sets. The results are shown in Table 1 below, where it can be seen that most of the success rates in attack resistance range from 0% to 5%, which indicates strong security, and some data shows a success rate of less than 10%. As a result of these experiments, it is possible to know that the proposed model classifies by reflecting the unique data of individuals.

**Table 1.** Success rate for attacks with 100 training datasets [unit: %].

| User 1 | User 2 | User 3 | User 4 | User 5 | Average |
|---|---|---|---|---|---|
| 0 | 1.43 | 0 | 5.0 | 0 | |
| **User 6** | **User 7** | **User 8** | **User 9** | **User 10** | 2.47 |
| 0 | 2.86 | 9.29 | 5.0 | 1.11 | |

In the previous experiment, we were able to obtain sufficiently accurate results with a training dataset of 20. Therefore, it was tested whether the 20 training datasets could be sufficiently resistant to attack. The results are shown in Table 2. Most of the attack success rates were 1% to 7% higher. On average, the attack success rate is 6.39%. However, as the number of datasets increases, it is more helpful in judging an individual's unique information, so it seems to show a high attack success rate compared to the previous experiment. However, with only 20 datasets, the attack success rate is as low as 0% and on average, 6.39%, so this can be considered an authentication model with high security.

**Table 2.** Success rate for attacks with 20 training datasets [unit: %].

| User 1 | User 2 | User 3 | User 4 | User 5 | Average |
|---|---|---|---|---|---|
| 1.11 | 5.56 | 0 | 8.33 | 2.22 | |
| **User 6** | **User 7** | **User 8** | **User 9** | **User 10** | 6.39 |
| 5.0 | 7.78 | 13.89 | 12.78 | 7.22 | |

## 5.5. Accuracy Evaluation over Time

Most behavior-based authentication method lose accuracy over time because the authenticating behavioral factor is affected by time. In order to find out whether the proposed model is also affected by the passage of time, the change in accuracy of the model was measured for one month. Using three trial participants we measured whether there was any change in accuracy during the period. For the training dataset, the success rate was measured using the existing 100 datasets and 20 new datasets after a month had elapsed. The experimental results are shown in Figure 6. The accuracy of the three trial participants remained unchanged or slightly decreased. Therefore, we found that the accuracy of the model was not significantly affected over time. The slight drop in accuracy is due to the inclusion of behavior-based authentication variables. However, this too does not depend entirely on behavior-based authentication through biometric-based authentication variables, so it has resistance to decreasing accuracy over time.

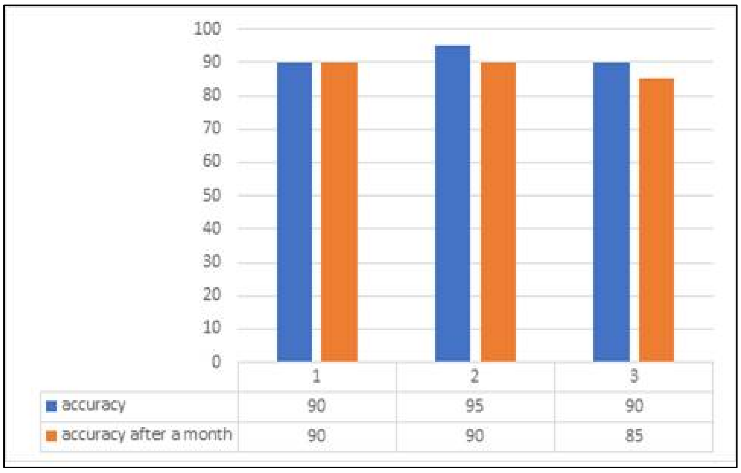


**Figure 6.** Accuracy over time of month [unit: %].

## 5.6. Evaluation with Performance Time

The execution time is measured as a criterion to determine whether the authentication process of the proposed model can quickly classify users in use. Execution time measurement is calculated by adding authentication operation time, data communication time, and machine learning execution time. Each process is performed five times and the result is calculated as an average. As shown in the results of Table 3, the authentication process is completed in 0.82 s or less than 1 s. The user hardly feels the inconvenience of authentication because the response is received in 0.29 s after the authentication operation is completed, and this time is very fast.

**Table 3.** Performance time [unit: s].

| Motion | Transmission | Machine Learning | Total Time |
|---|---|---|---|
| 0.53 | 0.02 | 0.27 | 0.82 |

### 5.7. *Comparison of Security and Functionality Features of Various Existing and Proposed Model*

The performance related to the security and functionality of the existing widely used authentication method and the proposed model is summarized, and the contents are shown in Table 4 below.

**Table 4.** Comparison of security and functionality features of various existing and proposed model.

| | PIN and Password | Pattern | Fingerprint | Proposed Model |
|---|---|---|---|---|
| **User Friendly** | Good | Good | Good | Good |
| **Too long password or complex pattern** | Easy to forget and inconvenient | Easy to forget and inconvenient | Not affected | Not affected |
| **Accuracy over Time** | Poor | Poor | Good | Good |
| **Security Performance** | Normal | Poor | High | High |
| **Influence of password leakage** | Critical | Critical | Critical | None |

## 6. Conclusions

The proposed authentication model, which is an easy, fast and reliable method implemented by integrating behavior-based and biometric authentication through smart watch is set up and tested successfully. The model shows a high accuracy of 91.5% on the 100 training datasets, and it was able to maintain high accuracy, even when the number of training datasets was reduced. The disadvantages of existing behavior-based authentication, which significantly affect accuracy over time, have also been addressed. In experiments conducted to find out if it is resistant to authentication attacks, this model showed average attack success rates of 2.47% and 6.39% on 20 training datasets, so it can be evaluated as a sufficiently secure model. The authentication process takes only 0.82 s, and a response can be received within 0.29 s after the user action is completed, so there is no inconvenience such as slow authentication. The Gaussian mixture and isolation forest methods find a solution in a different way, so we use the two together to reduce the opposite accuracy difference and increase the accuracy performance, so the ensemble model has the highest accuracy. In future work, we will measure performance, compare it with various machine learning methods, and expand this authentication approach through a variety of additional experiments.

**Author Contributions:** Conceptualization, E.-K.L.; Data curation, J.L.; Formal analysis, S.P. and J.J.; Investigation, J.J.; Project administration, E.-K.L.; Resources, J.L., Y.-G.K., E.-K.L. and J.J.; Software, J.L. and S.P.; Writing—review & editing, Y.-G.K. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by Incheon National University Research Grant in 2021.

**Informed Consent Statement:** Informed consent was obtained from all subjects involved in the study.

**Conflicts of Interest:** The authors declare no conflict of interests.

## References

1. He, W.; Golla, M.; Padhi, R.; Ofek, J.; Dürmuth, M.; Fernandes, E.; Ur, B. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In Proceedings of the 27th USENIX Security Symposium (USENIX Security), Baltimore, MD, USA, 15–17 August 2018; pp. 255–272.
2. Aviv, A.J.; Gibson, K.; Mossop, E.; Blaze, M.; Smith, J.M. Smudge attacks on smartphone touch screens. In Proceedings of the 4th USENIX Conference on Offensive Technologies, Washington, DC, USA, 9 August 2010.
3. Wiedenbeck, S.; Waters, J.; Sobrado, L.; Birget, J.-C. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proceedings of the Working Conference on Advanced Visual Interfaces, Venezia, Italy, 23–26 May 2006.

4. IPhone Fingerprint Sensor Hacked with a Finger Made of Clay at MWC. 2016. Available online: http://www.techworm.net/2016/02/iphone-fingerprint-sensor-hacked-finger-made-clay-mwc-2016.html (accessed on 6 January 2021).
5. Mantyjarvi, J.; Lindholm, M.; Vildjiounaite, E.; Makela, S.M.; Ailisto, H.A. Identifying users of portable devices from gait pattern with accelerometers, in Acoustics, Speech, and Signal Processing, 2005. In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'05), Philadelphia, PA, USA, 23 March 2005.
6. Giuffrida, C.; Majdanik, K.; Conti, M.; Bos, H. I sensed it was you: Authenticating mobile users with sensor-enhanced keystroke dynamics. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*; Springer: Cham, Swithzerland, 2014; pp. 92–111.
7. Shahzad, M.; Liu, A.X.; Samuel, A. Secure unlocking of mobile touch screen devices by simple gestures: You can see it but you can not do it. In Proceedings of the 19th Annual International Conference on Mobile Computing Networking (MobiCom), Miami, FL, USA, 30 September–4 October 2013.
8. Song, Y.; Cai, Z.; Zhang, Z. Multi-touch Authentication Using Hand Geometry and Behavioral Information. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017; pp. 357–372. [CrossRef]
9. Zhang, J.; Wang, Z.; Yang, Z.; Zhang, Q. Proximity Based IoT Device Authentication. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM 2017), Atlanta, GA, USA, 1–4 May 2017.
10. Yan, Z.; Song, Q.; Tan, R.; Li, Y.; Kong, A.W.K. Towards Touch-to-Access Device Authentication Using Induced Body Electric Potentials. 2019. Available online: https://dl.acm.org/doi/10.1145/3300061.3300118 (accessed on 30 September 2021).
11. Li, X.; Yan, F.; Zuo, F.; Zeng, Q.; Luo, L. Touch Well Before Use: Intuitive and Secure Authentication for IoT Devices. In Proceedings of the 25th Annual International Conference on Mobile Computing and Networking, Cabo San Lucas, Mexico, 21–25 October 2019; pp. 1–17. [CrossRef]
12. Moore, A.W. Very fast EM-based mixture model clustering using multiresolution kd-trees. *Adv. Neural Inf. Process. Syst.* **1999**, 543–549.
13. Liu, F.T.; Ting, K.M.; Zhou, Z.H. Isolation forest. In Proceedings of the 2008 Eighth IEEE International Conference on Data Mining, Pisa, Italy, 15–19 December 2008.
14. Liu, F.T.; Ting, K.M.; Zhou, Z.H. Isolation-based anomaly detection. *ACM Trans. Knowl. Discov. Data* **2012**, *6*, 1–39. [CrossRef]