Delivery of User Intentionality between Computer and Wearable for Proximity-based Bilateral Authentication

Jaeseong Jo[1], Eun-Kyu Lee[2]*, Junghee Jo[3]*
Department of Information and Telecommunication Engineering, Incheon National University, Incheon, Korea[1, 2]
Department of Computer Education, Busan National University of Education, Busan, Korea[3]

***Abstract*—Recent research discovers that delivering user intentionality for authentication resolves a random authentication problem in a proximity-based authentication. However, they still have limitations – energy issue, inaccurate data consistency, and vulnerability to shoulder surfing. To resolve them, this paper proposes a new method for user intent delivery and a new proximity-based bilateral authentication system by adopting it. The proposed system designs a protocol for authentication to reduce energy consumption in a power-constrained wearable, applies a Needleman-Wunsch algorithm to the matching of time values as well, and introduces randomness to a user behavior that a user must perform for authentication. We developed a prototype of our authentication system on which a list of experiments was conducted. Experimental results show that the proposed method results in more accurate data consistency than conventional methods for user authentication intent delivery. Eventually, our system reduces authentication failure rate by 66.7% compared to conventional ones.**

***Keywords*—Security; authentication; internet of things; user intentionality; proximity-based authentication; bilateral**

I. Introduction

An ID-password authentication has enjoyed a variety of applications for a long time. While it is simple to use, it requires mental efforts to remember IDs and passwords as well as physical efforts to input them directly. It is recommended to use different passwords for different IDs. However, people in real life use the same password for multiple IDs because it is easy to remember one password. Once the password is exposed, however, user's accounts can be exposed to security risks.

With advancement of Internet of Things (IoT) technologies and pervasive computing, recent proximity-based authentication performs without requiring both mental and physical from users. The proximity-based authentication initiates authentication when a wearable user approaches a certain distance from the authentication device (say, a computer). We note that once the user is within the distance, the authentication automatically proceeds regardless of the user's intention to authenticate. That is, the user proceeds with authentication that she does not know, named a random authentication problem. Moreover, the user's lack of understanding of authentication intent leads to the problem of continuing authentication; an authentication process starts whenever the user passes a certain distance of the computer that she wanted to authenticate.

A user authentication intent delivery solves the problems. It proceeds with authentication via a user's specific behavior, enabling proximity-based authentication to work with the sensor values in the wearable and data collected from the computer for this behavior. Conventional methods for user authentication intent delivery use a mouse in the computer to calculate acceleration values using mouse position values and distance traveled values to collect them with time values and use a keyboard to press the keyboard and time to press the time. The wearable collects acceleration sensor values and the time values and transmit them to the computer. The computer checks the consistency of these data to determine whether to authenticate.

However, the conventional methods have limitations as follow. First, they require the wearable device to keep running built-in sensors and recording data, which consumes energy faster in the small, power-constrained device. Next, they predefine the type of behavior that a user must perform for authentication and the number of actions that the user repeats the behavior, which could be vulnerable to external attackers. Last, the conventional methods do not make use of time values when checking data consistency, which may result in less accurate matching.

This paper proposes a new method that delivers user intentionality for authentication and resolves the limitations and eventually proposes a new proximity-based bilateral authentication system by adopting the new method. To address the energy concern, the proposed system designs a new protocol for authentication where an authentication process is initially detected by the wearable. The system resolves the second limitation by applying randomness to the number of actions; that is, it changes the number each time a user proceeds with authentication. Last, our system enhances accuracy of data consistency by applying a Needleman-Wunsch algorithm to the matching of time values as well as acceleration sensor data.

A prototype is developed where we use a Galaxy Watch as a wearable, and experiments are conducted to evaluate performance of the proposed system. Experimental results show that the proposed system reduces error in data consistency by 46.6% on average (from 0.3593 to 0.1918). The improved accuracy affects performance of authentication; our system reduces authentication failure rate by 66.7% compared to the conventional method.

*Corresponding Author.

The rest of the paper is composed as follows. Section II reviews two popular authentication methods and their limitations. Section III describes a conventional method for a user authentication intent delivery in detail. Section IV proposes a new proximity-based authentication system that delivers user's intentionality for authentication in an accurate manner. Experiments and performance evaluation of the proposed system are discussed in Section V. The last section concludes the paper.

II. Research Background

This section reviews a widely used authentication method, an ID-Password authentication, and discusses limitations. It also describes a proximity-based authentication method that can resolve the limitations.

A. ID-Password Authentication

The most popular user authentication method has been an ID-password authentication [1]. It determines whether these data are equivalent to the values stored in the database by the user entering their own ID and password. Recently, authentication security through secondary authentication has been strengthened. The security of authentication is increasing with the addition of various secondary authentication methods, including authentication methods using existing ID passwords [2], sending messages using smartphones to enter additional code of messages [3], and user verification methods using specific applications.

Limitations: The ID-Password authentication method has limitations; it requires mental and physical efforts from users. In the case of mental effort, it is likely to be resolved if the passwords and IDs of all accounts are unified, but if passwords and IDs are exposed, all accounts may be at risk. On the contrary, if all IDs and passwords are set differently, mental efforts are needed too much because one should remember the whole thing. In the case of physical effort, the process of entering an ID and password is more mobile than expected because it uses a mouse and keyboard to enter characters. Recently, additional authentication methods using secondary passwords and QR codes [5] have been utilized by utilizing smartphones [4] to increase security. This method is certainly highly reliable in security, but there is a hassle of unlocking a smartphone, using an application, or checking a message and entering it back into the computer.

B. Proximity-based Authentication

Proximity-based authentication is a technology that logs in or out users from applications, devices, websites, etc. using the distance between users and authentication devices as a key value [6]. To be successful in authentication, it is necessary to have auxiliary devices such as smartwatches and wearables near devices that users want to authenticate. Proximity-based authentication automatically initiates authentication when a user approaches a certain distance of the authentication device. At this time, authentication devices and users use wireless communications such as Bluetooth and Wi-Fi. The proximity-based authentication system is shown in Fig. 1. A computer and a user proceed with authentication by exchanging authentication tokens with each other [7] when the user is within a certain distance of the server.

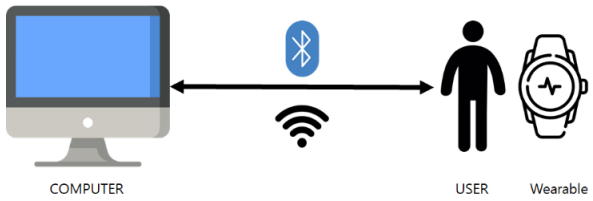

Fig. 1. Proximity-based Authentication Initiates as a user Approaches a Computer.

Limitations: Proximity-based authentication automatically begins a process when a user approaches a certain distance of the authentication device. The authentication that occurs at this time proceeds regardless of the user's intention to authenticate. In other words, authentication proceeds even if a user approaches a device within a certain distance without any intention of authentication, so the user proceeds with authentication that he or she does not know [8]. Authentication fails if the user deviates from the effective distance for authentication with the authentication device while the authentication is in progress. This is an important part of the authentication process that is irrelevant to the user's intentions described earlier. Authentication is attempted if the user passes the effective distance of the authentication device, at which point authentication attempts-authentication failures [9] are repeated because authentication fails if it is outside the effective distance. If this process is repeated, certain devices lock down the authentication and cause problems that prevent users from proceeding with authentication in the situation they want to authenticate. The following section describes how one can communicate users' authentication intent in proximity-based authentication in detail.

III. Delivery of User Intentionality for Authentication: Conventional Approach

In proximity-based authentication, a user authentication intent delivery allows accurate authentication to proceed by delivering authentication intention from assistive devices (e.g., wearables and smartwatches) or authentication devices (e.g., computers). Two typical technologies for user authentication intent delivery include wristband-based authentication for desktop computers (SAW) [10] and proximity-based user authentication on voice-powered Internet-of-Things devices (PIANO) [11]. This section describes a conventional approach that accurately conveys users' authentication intent in proximity-based authentication. Since our scenario sees authentication between a wearable and a computer, a review in this section is mainly based on the former.

A. User Authentication Intent Delivery

A user authentication intent delivery is generally based on near-field based authentication, where wearable users and computers are paired over wireless communication within a certain distance, then double-click a specific button on the computer keyboard to confirm the user's intention to authenticate. Afterwards, values for a user's specific behavior are collected from wearable and computer, and authentication is carried out by matching these data [12].

1) System architecture: After wearing a wearable device, the user double-taps the computer's keyboard to verify the computer's authentication intent. When the computer confirms the authentication intent, it requests data about the acceleration sensor of the wearable. Users take certain actions, using a mouse or keyboard. On wearable devices, the acceleration sensor value and the gravitational sensor value are calculated and sent to the server using a specific program to calculate the value of the mouse and keyboard movement. When transmitting, it is carried out through wireless connections such as Bluetooth and Wi-Fi. The matching of the sensor value of the wearable device sent to the server is verified using a mouse or keyboard, and user authentication is performed on the computer with an authentication completion message. Request to measure again if authentication fails.

Unlike traditional proximity-based authentication, the user authentication intent delivery conveys the user's authentication intent, which allows the user to approach within a certain distance, verify the authentication intent, and authenticate. Differences from proximity-based authentication methods are shown in Table I [13].

2) Operation: In a conventional method for user authentication intent delivery, a computer and a wearable is paired via Bluetooth communication [14]. After pairing, authentication starts by pressing the computer's keyboard specific key twice, and the computer requests acceleration sensor values and time data from the wearable. The worm transmits the requested acceleration sensor data [15] to the computer. When the data is transferred, the computer checks data consistency; it successfully authenticates upon successful data matching or fails to authenticate upon data matching failure. In the event of a data matching failure, the sensor data transfer request is re-requested. If the data is not sent within 5 seconds of pairing, the pairing is canceled and then the pairing is requested again.

3) Detection of user intent on computer: The computer uses data values for wrist movements of wearable users to check the consistency with acceleration sensor data of wearable [16]. To collect data on the user's wrist movement from a computer, conventional methods use a mouse-wiggle [17] and/or a TAP [18]. Fig. 2 illustrates these two ways.

TABLE I. DIFFERENCES BETWEEN TRADITIONAL AUTHENTICATION METHODS AND USER AUTHENTICATION INTENT DELIVERY BASED METHODS

Proximity-based authentication		***User authentication intent delivery***	
Advantages	Authentication system operation when user approaches within a certain distance	Characteristics	Complement the absence of a user authentication intent verification method of traditional proximity-based authentication by identifying the intent through specific actions.
Weakness	Continuously operates the authentication system when accessing within a certain distance without identifying the user's authentication intent.		

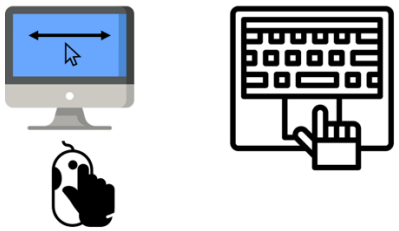

Fig. 2. Mouse-Wiggle (Left) and Keyboard Tab (Right) Methods.

When authentication begins, a user in the mouse-wiggle method moves the mouse from side to side on the screen, which is recorded. The computer measures the mouse's position values and time values with which it computes acceleration values. Finally, the acceleration value is calculated by dividing the time value by the distance traveled previously obtained. The TAP method makes use of the time value when the keyboard was pressed a certain number of times and difference between the current time value and the time value when the keyboard was first pressed. This value indicates the time when the user's hand presses and releases the keyboard. The computer uses this time value to verify that the value of the highest point of the acceleration sensor value in the wearable matches the recorded time.

4) Detection of user intent on wearable: After pairing with a computer, a wearable is asked to send sensor data. When a user performs a mouse-wiggle and keyboard-TAP method, the wearable transmits the value of the acceleration sensor of the device itself to the computer [19].

B. Limitations of User Authentication Intent Delivery

A delivery of explicit user intentionality for authentication solves the random authentication problem [20] that can occur in proximity-based authentication methods, thus enabling more accurate authentication. However, conventional methods for user authentication intent delivery have limitations that hinder optimal authentication operations. First, the methods make a computer to detect a user intent for authentication initially. Once detected, the computer tries to communicate with a wearable device on the user side to obtain sensor records. This implies that the device remains on a ready state all the time, which makes it hard to save energy consumption on the device. Next, conventional methods use fixed forms of user behaviors as intent. For instance, the TAP-5X method pushes a computer's keyboard five times to collect data for matching data between computers and wearables. Because TAP-5X performs exactly five actions by the user, it is possible for an external attacker to observe and analyze the user's behavior and authenticate by taking the same action [24]. Wearable devices may not be problematic because they are usually worn by the user, but if the user is away for a while or if the wearable is stolen 15 times, the computer cannot verify whether the user is a user or an attacker, making the TAP-5X vulnerable to external attackers. Last, conventional methods prioritize the matching of acceleration sensor values in data matching for authentication between computers and wearables for authentication. Data obtained from computers and wearables include time values and acceleration sensor values. A Needleman-Wunsch algorithm [21] has been used to match the

acceleration sensor values, increasing the accuracy of the acceleration sensor data values. However, algorithms for data matching were not used for time values while time values have been used as one of the most significant metrics in previous research on user authentication intent delivery [22, 23]. This can cause problems in the process of identifying data matching.

IV. Proposed System: User-Intended Proximity Authentication

This section proposes a new proximity-based authentication system that explicitly delivers user intentionality for authentication. To resolve the first limitation, an authentication process in the proposed system is initially detected on a user side instead of on a computer. To this end, the user is required to touch her wearable twice first. The next limitation is resolved by applying a one-time password concept that proposes a new criterion for the number of actions that a user must perform each time he or she proceeds with authentication. To resolve the last limitation, our system improves accuracy in the data matching process by applying the Needleman-Wunsch algorithm to time values as well.

A. System Architecture

The proposed system consists of two entities, a user and a computer, as shown in Fig. 3. The user is with a wearable that is paired with the computer via Bluetooth communication. The user starts behaving an intent action, and her behavior is detected both on the wearable and on the computer and processed. Fig. 4 helps us describe how accurately the system measures data on the behavior and determines that the measured values on both sides are matched.

The computer in Fig. 4 opens a Bluetooth server and connects it to Intelligent Unit that calculates data matching and Action Detector that is responsible for detecting the movement of a keyboard and a mouse on the computer and for measuring corresponding data. The wearable uses Bluetooth Server on the computer and a Bluetooth socket to make a UUID connection. Sensor Manager keeps monitoring values from built-in sensors. Once an authentication process is triggered, Sensor Manager transmits the sensor records to the computer via the Bluetooth communication. At the same time, Action Detector measures the movement of the computer's mouse and keyboard and records related data. Upon collecting data from both Sensor Manager and Action Detector, Intelligence Unit checks the match between the two data. Authentication is completed if the data is matched, or retransmission is requested if authentication fails due to data mismatch.

B. Protocol

The proposed system designs a protocol for authentication between the computer and the wearable, and Fig. 5 depicts flows and processes of the protocol.

The computer makes a pairing request to the wearable by transmitting its UUID. The wearable checks the validity of the UUID received and transmits its own UUID to the computer to proceed further with pairing. Once they are paired, a user is allowed to request authentication to the computer.

An authentication process in the proposed system is initially detected by the wearable unlike conventional methods for user authentication intent delivery. The user double-touches the wearable to communicate her authentication intent to the computer. Then, authentication begins when the computer confirms the intent. The computer requests the wearable to transmit sensor records. At the same time, it generates a random number (a nonce) and piggybacks the nonce on the request message.

Upon receiving the message, the user takes an action; she moves a mouse or pushes a key in a keyboard connected to the computer. The nonce received guides her behaviors; that is, she repeats the movement or the push multiple times corresponding to the nonce value. When the user performs an action, Sensor Manager in the wearable records acceleration values and corresponding time values and transmits them to the computer. After sending the request message to the wearable, Action Detector in the computer starts collecting data of mouse movement (changes of the pointer's positions and corresponding timestamps) and/or data of keyboard (numbers of key presses and timestamps of pressing and releasing).

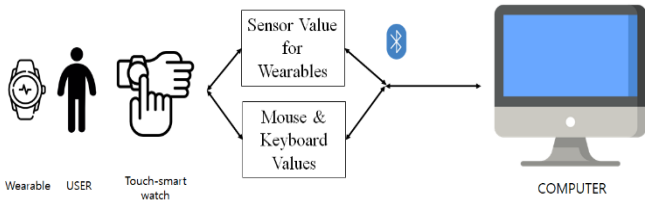

Fig. 3. The Proposed Authentication System Consists of Two Entities, a user and a Computer. They do Authentication by Delivering the user's Authentication Intent.

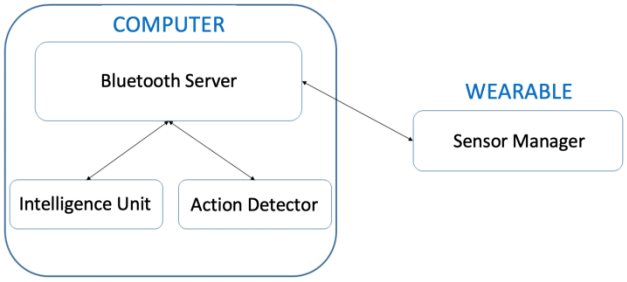

Fig. 4. Two Entities in the Proposed System Include a List of Components, and they are Responsible for Exchanging Data Regarding user's behavior and Processing it for Data Matching.

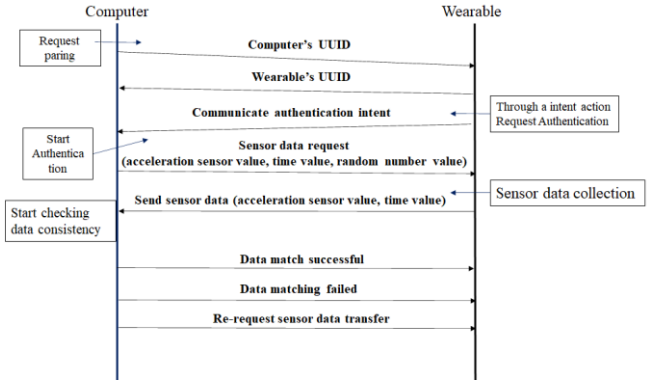

Fig. 5. The Proposed System Designs a Protocol for Authentication between Computer and user, where user's Intentionality for Authentication is Delivered Explicitly.

Intelligence Unit in the computer collects data from both Sensor Manager and Action Detector. These data are supposed to represent the user's behavior for authentication intent commonly but recorded by two different devices. It then checks the consistency of the data using the Needleman-Wunsch algorithm. If two data are matched, the user is authenticated. If they are not matched or the collected data is not received, the computer retransmits the request message. If there is no response within timeout period, authentication fails.

C. Accuracy of Data Consistency

Conventional methods for user authentication intent delivery, like our system, apply the Needleman-Wunsch algorithm to the data consistency check; it matches data from user-worn wearables with data measured on the computer. It is observed that the methods use the matching algorithm only to determine the matching of sensor values and do not care for corresponding time values. However, time values in general authentication have played an important role especially when computing data consistency and data matching [25]. Matching of sensor data may result in failure of authentication unless corresponding time values are matched. To resolve the limitation, this paper proposes applying the Needleman-Wunsch algorithm to the matching of time values as well as acceleration sensor data, enhancing accuracy of data consistency.

D. Randomness of user behavior

In a behavior-based authentication, data consistency is verified using data obtained by a user taking an action. Conventional methods for user authentication intent delivery define criteria in their specific behaviors [26]. This criterion is an essential part of users' behavior but can be abused for attacks. An external attacker can observe certain behaviors that a user performs when authenticating to a computer and then mimic the same action with a wearable device to carry out an authentication attack [27]. The criteria for users' behavior serve as fixed ID-Password values in a popular authentication. Thus, if data is leaked, constant data can be analyzed and attacked with authentication using fake data.

To tackle the challenge, the proposed system adopts the concept of OTP in the existing ID-Password authentication method [29]. The computer in our system sends a random number together when requesting data for authentication to a wearable [28]; this changes the required number of criteria for each authentication of a user's specific behavior. More technically, the computer sends two random values that are applied separately to the mouse and keyboard actions. To reduce the time required for certification as much as possible, a random number for the mouse is between 3 and 5 and that for the keyboard is between 3 and 7, which is based on numbers of existing authentication methods. This allows users to defend against authentication attacks because each authentication requires different numbers of certain behaviors. Even if external attackers observe and analyze users' behavior, they are inconsistent. We note that an optimal range of random values could be an interesting topic for further research.

V. Development and Performance Evaluation

This section develops a prototype of the proposed system, runs experiments, and evaluates its performance. To assess accuracy of data consistency, we compare error values both in a traditional (conventional) method reviewed in Section III and in the proposed system that applies the matching algorithm to the time values additionally. Regarding randomness of user behavior, we measure data on how much user behaviors are matched when using randomized criteria. The initial result is then used to see whether an external attacker is authenticated when he imitates a particular behavior in both systems.

A. Development

The test environment was modeled on the way that a user performs authentication at a personal computer, and a wearable was worn on the user's right wrist. We use a computer running Linux Ubuntu 16.04.04 LTS on a system of Intel® Core™ i5-9600KF CPU @ 3.70GHz and 16GB of memory. When recording mouse movements, the computer calculates the acceleration value using the position change value and the time change value [30]. When recording keyboard input, the time when the keyboard is inputted and the time when it is inputted is recorded. We use a Galaxy Watch (smartwatch) as a wearable, and Table II shows its technical specification. The smartwatch samples the accelerometer sensor at 200 Hz and transmits the data to the Bluetooth server in real time.

B. Experiments on Traditional Method

For traditional methods, we use a mouse and keyboard to collect data about a user's specific behavior. Participants wear smartwatches on their right wrist to conduct experiments. In the smartwatch, acceleration sensors are used to collect acceleration values for wrist movements, and in the computer, mouse and keyboard are selected sequentially from Python-based programs. When selecting a mouse, the mouse moves from side to side on the screen to collect the mouse's location data and time data and calculate the acceleration. We then collect the time when the keyboard button is pressed once the keyboard is selected, or the time when the keyboard button is pressed [31]. The computer uses the matching algorithm to determine the data match for the acceleration value of the collected data.

For accurate verification of consistency of the data collected via the mouse-keyboard method of the participants, the data values are graphically represented to confirm the consistency of the values directly. This section compares the two graphs with the largest error in the experimental results as representatives, and the overall experimental results are tabulated.

TABLE II. Specifications of Smartwatch

	Spec OF Galaxy Watch
O.S	Tizen-based wearable OS 4.0
CPU	Dual-core 1.15 GHz Cortex-A53
Memory	4GB 768MB RAM, 4GB 1.5GB RAM
SENSOR	Accelerometer, gyro, heart rate, barometer
BATTERY	Up to 72 h (mixed usage)

Fig. 6 shows the mouse experiment results of participant 1. The x-axis of the graph is the time in seconds, and the y-axis uses the acceleration value (m/s^2). The graph for acceleration values in computers and smartwatches shows a similar graph in the peak, but in the last peak in the computer, the computer shows an acceleration value of 0.47264 and 0.168671 in the smartwatch, with an error value of 0.303969. In the SAW paper, the criterion for the error value of the data is 0.3. Existing systems determine that certification failed for the current participant.

Fig. 7 shows the results of a keyboard experiment for the same participant. In the figure, the part marked in red squares takes time for the keyboard to press and hit. The data consistency check on the keyboard first determines whether the acceleration value on the smartwatch is the value of the peak point at the time the keyboard is pressed on the computer. The keyboard checks the pressed and hit time and determines that it is the same if there are no other pick points within this time interval. However, the above graph shows that the value is peak at the time the keyboard was pressed on the second computer, but the exact data matching was not achieved because another pick point was displayed in the red square section, which represents the interval where the keyboard was pressed and hit. For the first experimental participant, neither mouse-keyboard nor mouse-keyboard matched the data.

Fig. 8 shows a graph of the mouse results of participant 6. The graph on the mouse results of the 6th experimental participant shows significantly similar appearance and matching values in computers and smartwatches than the graph of the first participant in the preceding one. However, the maximum value on a computer at 2.5 seconds in the graph is 1.62745, and the minimum value for a smartwatch is 1.10937. In this experiment, the error value at the peak point has a maximum value of 0.51808. This value is also determined to be an authentication failure because it does not match the data with more than twice the error tolerance value of 0.3 in [10].

Fig. 9 shows the results of the same participant's keyboard experiment. By checking the graph above, the sixth experimental participant was able to see the matching of the data in the keyboard experiment because the time the keyboard was pressed on the computer was all peak value of the smartwatch's acceleration value and no other peak value was included in the red square section.

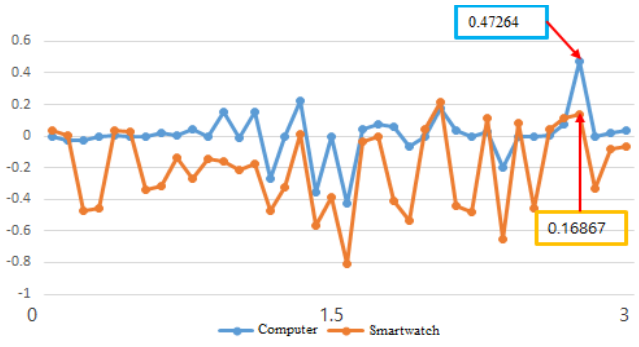

Fig. 6. An Experimental Result of Mouse Movement on Participant 1.

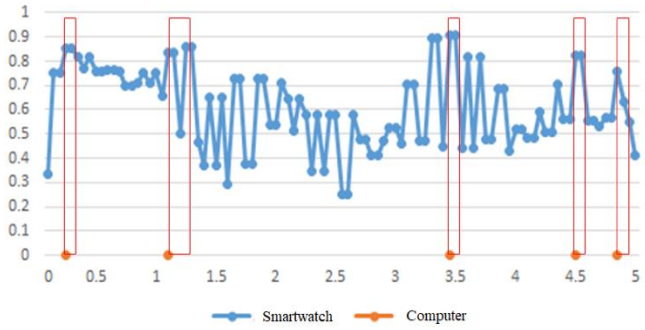

Fig. 7. An Experimental Result of Keyboard Press on Participant 1.

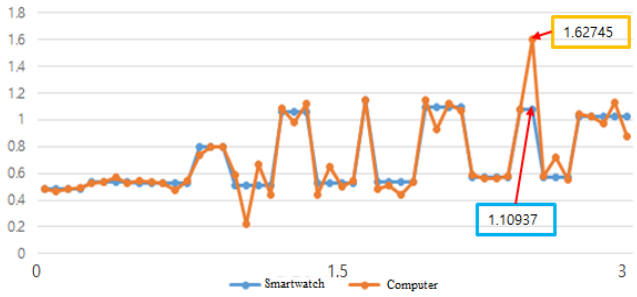

Fig. 8. An Experimental Result of Mouse Movement on Participant 6.

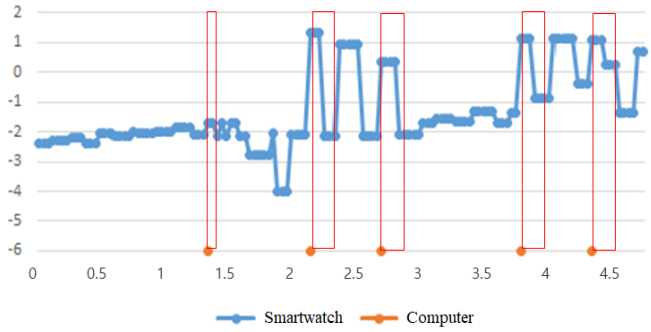

Fig. 9. An Experimental Result of Keyboard Press on Participant 6.

Table III summarizes mouse experiment results of a total of eight experimental participants in the traditional method. Five of the eight participants in the experiment are close to the tolerance value of 0.3, of which three are accurately included in the tolerance value, with one exceeding some.

Table IV shows eight participants are certified through the results of a keyboard experiment. There were five successful participants in the experiment, and three unsuccessful participants. Authentication via keyboard rather than mouse is the main method. All participants matched the time the keyboard was pressed on the computer with the peak point of the acceleration value on the smartwatch, but three failed to authenticate, including the other peak value in the keyboard's pressing and hitting interval. These results confirm that when the matching algorithm for time values is not applied during the authentication process through the user authentication intent transfer method.

TABLE III. EXPERIMENTAL RESULTS OF EIGHT PARTICIPANTS USING TRADITIONAL METHODS

	Computer	***Smartwatch***	***Error value***
Participant 1	0.47264	0.16867	0.30396
Participant 2	0.25175	-0.18172	0.43347
Participant 3	0.84264	0.28839	0.55425
Participant 4	-0.02481	-0.39514	0.37033
Participant 5	0.64428	0.41439	0.22989
Participant 6	1.62745	1.10937	0.51808
Participant 7	0.75613	0.52571	0.23042
Participant 8	0.40917	0.17514	0.23403

TABLE IV. KEYBOARD EXPERIMENT RESULTS FROM EIGHT PARTICIPANTS USING TRADITIONAL METHODS

	Authentication success	**Authentication failed**
Participant Number	2, 3, 6, 7, 8	1, 4, 5

C. Experiments on Proposed System

Unlike traditional methods, a smartwatch in the proposed system verifies the user's authentication intent, sends it to the computer, and verifies this intention on the computer to proceed with authentication. In this case, random values are transferred to the smartwatch together to provide a baseline for a specific behavior for the user's authentication, and experimental participants take a specific behavior through the mouse and keyboard according to this number.

With these data values, the computer applies the Needleman-Wunsch algorithm to verify the consistency of the data, and then applies the algorithm to the time value to perform authentication with more accurate data matching. Experiments conducted by experiment participants are the same as previous experiments, and only new parts are added that initiate authentication by touching the smartwatch twice. The graph also displayed the results of the experimenter with the largest error value and the experimenter with the smallest error value, just like the previous experiment, and the results for the entire experiment were tabulated.

Fig. 10 shows a graph of the acceleration sensor values of participant 5. The random number of mouse experiments occurred was 4, and the user moved the mouse left and right for 4 seconds to measure acceleration sensor data, time data, and acceleration and time values through the computer's mouse movement. In the above graph, the graphs for acceleration values of computers and smartwatches are not completely consistent, but we can confirm that the two data are much more consistent than those of conventional methods. At this point, a peak value of 0.33762 was recorded on the 1.2-second computer, while the smartwatch recorded a value of 0.25983. At this point, the error of the two values is 0.07779, showing a significantly lower value than 0.3 which was represented by the error value in the existing user authentication scheme.

Fig. 11 shows the results of a keyboard experiment of the same participant. At this point, the displayed random numbers represent the same 5 as the existing experiments, and the user conducted an experiment of pressing the keyboard five times. In the graph above, the time when the keyboard was pressed on the computer and the peak point of the acceleration value of the smartwatch are the same, and the red section for the time when the keyboard was pressed and hit does not include other peak points. In the case of keyboard experiments, there was no problem with data matching, unlike previous conventional methods experiments among participants. In other words, authentication was carried out by applying the need only-one algorithm to the time value, matching the section where the keyboard was pressed and hit to the time when the peak point of the smartwatch was stamped.

Fig. 12 is a mouse experimental graph of participant 1 in the proposed method. Unlike the results of one previous experiment, graphs for acceleration values of smartwatches and computers show more consistency. The computer's acceleration value is 0.50388 and the smartwatch recorded acceleration sensor value is 0.28104. The error value for this is 0.22284, which is lower than the error range of 0.3. However, the values shown this time showed similar values in previous experiments.

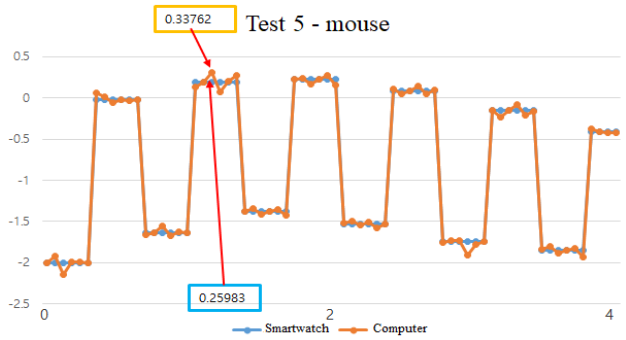

Fig. 10. An Experimental Result of Mouse Movement on Participant 5 in the Proposed Method.

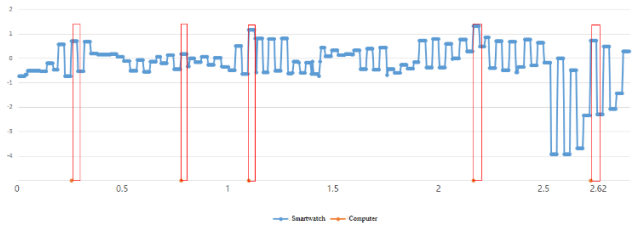

Fig. 11. An Experimental Result of Keyboard Press on Participant 5 in the Proposed Method.

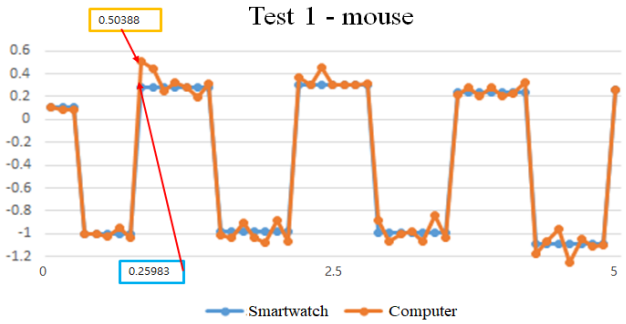

Fig. 12. An Experimental Result of Mouse Movement on Participant 1 in the Proposed Method.

The results of the overall participants in the proposed scheme are presented in Table V. There were seven participants who did not correspond to the error value of 0.3, and only one failed to authenticate beyond the error value. It shows higher accuracy than data matching experiments in which three people in the previous existing method succeeded and five failed. This is the result of applying the need-one-value algorithm to the time value, which makes the comparison between computers and smartwatch data more accurate. It shows a lower error value than the error value shown in the experiments of the existing method, and is reliably successful in data matching, enabling authentication.

TABLE V. EXPERIMENTAL RESULTS OF 8 PARTICIPANTS IN THE PROPOSED SYSTEM

	Computer	***Smartwatch***	***Error value***
Participant 1	0.50388	0.28104	0.22284
Participant 2	-0.02944	0.09978	0.12922
Participant 3	0.27756	0.23265	0.04491
Participant 4	0.98824	1.09113	0.10289
Participant 5	0.33762	0.25983	0.07779
Participant 6	0.8537	1.3054	0.4517
Participant 7	1.2084	0.98841	0.21999
Participant 8	0.74269	1.02772	0.28503

D. Performance of Data Consistency

We confirm the experimental results of the existing and proposed methods in the previous subsection. In mouse authentication, we show that the existing method succeeds in 3 out of 8 and 5 fails, and that the proposed method fails only 1 out of 7 people. Furthermore, we show that the error value of the proposed scheme is also significantly lower, and we can confirm that it is a more suitable method for data matching. This can be confirmed through the graph in Fig. 13.

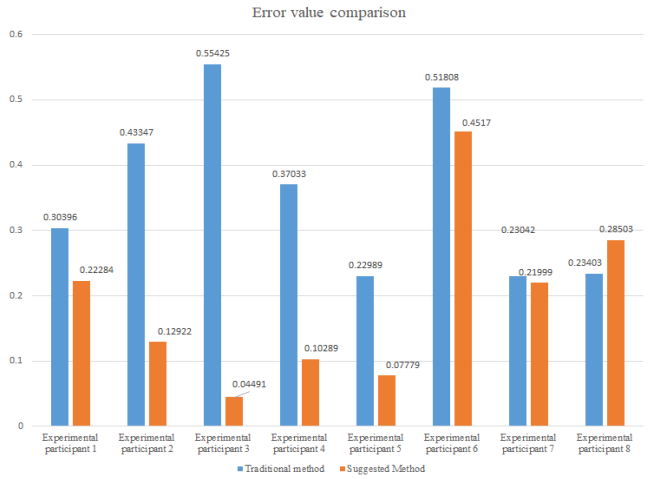

Fig. 13. Comparison of Error Values between Existing and Proposed Methods.

By checking the graph in the figure, the maximum value of the error in the existing scheme is 0.55425 and the minimum value is 0.21989 and the maximum value of the error in the proposed scheme is 0.4517, with a minimum value of 0.04491. The mean of each error value shows a significantly lower value of 0.359304 in the existing method, 0.191796 in the proposed method, and since the data error value for successful authentication must be less than 0.3 it is appropriate to use the proposed method focusing on matching time values over the existing method.

Keyboard-experiments also showed results of five successful and three unsuccessful using conventional methods, but the proposed method showed results of seven successful and one failure. However, because the proposed method can only authenticate when both the mouse and keyboard have a data match, one failed to authenticate through a match at the mouse value. Comparing only keyboard values, all eight showed accurate data matching.

E. Comparison of Behavioral Matching with Randomness

Traditional methods operate by setting criteria for specific behaviors of users. For instance, SAW in [10] used the TAP-5X, a five-press keyboard method. However, as previously stated, certain behaviors with these criteria can allow an external attacker to observe the user's movements and take the same action to make an authentication attack [32-34]. In this paper, random numbers are transferred from the computer to the smartwatch to perform the mouse-keyboard behavior at different times per authentication, rather than the criteria set for a particular number of actions. To confirm this, eight participants observed other people's experiments and examined whether they could perform the same behavior.

In experiments with existing methods, all eight participants answered that all users could do the same because they used the same authentication method of mouse movement and keyboard No. 5 tab. However, the experimental participants failed to take the same action because the proposed authentication method applied different random numbers to the mouse-keyboard method. Through this, authentication methods through randomness have an advantage in attacks through the observation of external attackers than when there is a set standard for a specific number of actions for authentication of existing users.

VI. CONCLUSION

This paper proposed a new proximity-based authentication system that delivered user's intentionality for authentication in an accurate manner. Conventional methods for user authentication intent delivery solve a random authentication problem that can occur in proximity-based authentication. But, they still have limitations; (i) a wearable device may consume energy much faster, (ii) conventional methods proceed based on the number of actions fixed to a specific behavior for user authentication, which could be vulnerable to external attackers, and (iii) the methods do not match time values, which results in less accurate data consistency process.

To overcome the limitations, the proposed system designs a new protocol for authentication where an authentication process is initially detected on a user side instead of on a computer. The system adopts a randomness that changes the number of actions that a user should perform each time she proceeds with authentication. It increases the accuracy of the matching of the data by applying a Needleman-Wunsch

algorithm to time values when verifying data consistency. Experimental results showed that authentication was succeeded 5 times and failed 3 times with conventional methods, but the proposed system showed 7 successes and 1 failure. Results in the mouse experiments showed that the maximum error value in the conventional methods was 0.55425 and the minimum value was 0.21989, while the proposed system showed the maximum of 0.4517 and the minimum of 0.04491, which was much lower.

A. Discussion

Verifying user intentionality is one of the most important goals in authentication process. In traditional patterns of authentication interaction (human-machine, human-human, and machine-human authentication), human beings have been involved directly in authentication and delivered authentication intent explicitly [35]. Examples include password-based methods and biometric-based methods. By touching on a finger scanner, a user presents her intent for authentication in a fingerprint authentication. With increasing development of IoT technologies and pervasive computing, however, a new pattern of a machine-machine authentication becomes popular [22, 36-37]. For instance, a user carrying a wireless authentication token approaches a target computer that authenticates the user whenever the token is within a certain distance. In such a new pattern of the proximity-based authentication, the user intentionality is often omitted or not verified explicitly.

Delivering the intent and verifying it on both sides of authentication entities may delay processing and degrade convenience of the machine-machine authentication [38]. That is, a new authentication method is on between accurate verification and user convenience. The proposed authentication system is somewhat intended to high accuracy and high protection level. It diminishes risks from external attackers by randomizing user behaviors in authentication, increases accuracy of data consistency process by handling time values, and takes care of energy consumption of a power-constrained IoT device by designing a new authentication protocol.

The proposed system may not provide an excellent benefit of user convenience. Our authentication may be recognized as an interruptive step in a user's normal workflow. That is, a user should start explicitly authentication after stopping what she is doing. Once authentication done, she gets back to her normal work that she was on before authentication. A future work may include development of an advance authentication that blends seamlessly into users' workflow. One possible approach is to make use of the workflow for authentication [26]. It would be optimal if she is being authenticated while she is doing her work; that is, seam between authentication and workflow are blurred.

Delivery of users' authentication intent is expected to enable faster and safer authentication through user behavior analysis if machine learning, which has recently been utilized in various fields, is applied. Furthermore, as the demand for wearable devices such as smartwatches is increasing, further research is required to analyze user behavior patterns in more detail and to quickly authenticate based on them.

REFERENCES

[1] L. Lamport, "Password authentication with insecure communication", Communications of the ACM, November 1981.

[2] T. Petsas, G. Tsirantonakis, E. Athanasopoulos, S. Ioannidis, "Two factor authentication: is the world ready?: quantifying 2FA adoption", European Workshop on System Security (EuroSec), Article No.:4, pp.1–7, 2015.

[3] S. Ma, R. Feng, J. Li, Y. Liu, S. Nepal, Diethelm, E. Bertino, R. Deng, Z. Ma, and S. Jha, An empirical study of SMS one-time password authentication in Android apps, ACM Annual Computer Security Applications Conference, Dec. 2019.

[4] B. Rodrigues, A. Chaudhari and S. More, "Two factor verification using QR-code: A unique authentication system for Android smartphone users," International Conference on Contemporary Computing and Informatics (IC3I), 2016.

[5] B. Zhou, J. Lohokare, R. Gao, and F. Ye, EchoPrint: Two-factor Authentication using Acoustics and Vision on Smartphones, ACM Annual International Conference on Mobile Computing and Networking, Oct. 2018.

[6] J. Zhang, Z. Wang, Z. Yang and Q. Zhang, "Proximity based IoT device authentication," IEEE Conference on Computer Communications (INFOCOM), 2017, pp. 1-9.

[7] A. Kalamandeen, A. Matthew Scannell, E. De Lara, Anmol Sheth, Anthony LaMarca, "Ensemble: cooperative proximity-based authentication", ACM International conference on Mobile systems, applications, and services (MobiSys), pp. 331–344, 2010.

[8] M Horton, 2016, "Proximity based device security", US Patent 9,443, 071, AT&T Intellectual Property I, L.P, Atlanta, GA (US).

[9] A. Varshavsky, A. Scannell, A. LaMarca, E. de Lara "Amigo: Proximity-Based Authentication of Mobile Devices", Ubiquitous Computing, pp 253-270, 2007.

[10] S. Mare, R. Rawassizadeh, R. Peterson, D. Kotz, "SAW: Wristband-based Authentication for Desktop Computers", ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2018, Article No:125.

[11] N. Z. Gong et al., "PIANO: Proximity-Based User Authentication on Voice-Powered Internet-of-Things Devices," IEEE International Conference on Distributed Computing Systems (ICDCS), 2017, pp. 2212-2219.

[12] D. E. Bernard, 2008, " Multimodal natural language query system and architecture for processing voice and proximity-based queries ", US Patent 7,376,645, The Intellection Group, Inc, Duluth GA (US).

[13] Li et al, Los Altos, CA (US), 2018, " Methods and Apparatus for User Authentication and Human Intent Verification in Mobile Devices ", US Patent 9,877,193, Apple Inc., Cupertino, CA(US).

[14] R. Bouhenguel, I. Mahgoub and M. Ilyas, "Bluetooth Security in Wearable Computing Applications," International Symposium on High Capacity Optical Networks and Enabling Technologies, 2008, pp. 182-186.

[15] J. Rekimoto, "GestureWrist and GesturePad: unobtrusive wearable interaction devices," International Symposium on Wearable Computers, 2001, pp. 21-27.

[16] S. Khan, S. Parkinson, L. Grant, N. Liu, S. Mcguire, "Biometric Systems Utilising Health Data from Wearable Devices: Applications and Future Challenges in Computer Security", ACM Computing Surveys , Article No:85, July 2020.

[17] R.Raya, J. Roa, E. Rocon, R. Ceres, J. Pons, "Wearable inertial mouse for children with physical and cognitive impairments", Sensors and Actuators A: Physical, Vol. 162, Issue 2, pp. 248-259, August 2010.

[18] N. Kern, B. Schiele, and A. Schmidt "Multi-Sensor Activity Context Detection for Wearable Computing", European Symposium on Ambient Intelligence, pp 220-232, 2003.

[19] S. Li, A. Ashok, Y. Zhang, C. Xu, J. Lindqvist and M. Gruteser, "Whose move is it anyway? Authenticating smart wearable devices using unique head movement patterns," IEEE International Conference on Pervasive Computing and Communications (PerCom), 2016, pp. 1-9.

[20] L. Xiao, Q. Yan, W. Lou, G. Chen and Y. T. Hou, "Proximity-Based Security Techniques for Mobile Users in Wireless Networks," IEEE Transactions on Information Forensics and Security, 8(12), pp. 2089-2100, Dec. 2013.

[21] Needleman, Saul B. & Wunsch, Christian D. (1970). "A general method applicable to the search for similarities in the amino acid sequence of two proteins". Journal of Molecular Biology. 48 (3): 443–53.

[22] X. Li, Q. Zeng, L Luo, T, Luo, "T2Pair: Secure and Usable Pairing for Heterogeneous IoT Devices", ACM Conference on Computer and Communications Security, pp. 309–323, 2020.

[23] S. Mare, R. Rawassizadeh, R. Peterson, D. Kotz, "Continuous Smartphone Authentication using Wristbands", Workshop on Usable Security, 2019.

[24] A. Bianchi, I. Oakley, "Wearable authentication: Trends and opportunities", 2016, it - Information Technology 58(5).

[25] F. De Arriba-Pérez, M. Caeiro-Rodríguez, J. Santos-Gago, "Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios", Sensors, 16(9), 1538, 2016.

[26] A. Huang, D. Wang, R. Zhao, Q. Zhang, Au-Id: Automatic User Identification and Authentication through the Motions Captured from Sequential Human Activities Using RFID, ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 3(2), Article No.: 48, June 2019.

[27] L. E. Boyd, X. Jiang, G. R. Hayes, "ProCom: Designing and Evaluating a Mobile and Wearable System to Support Proximity Awareness for People with Autism", Conference on Human Factors in Computing Systems (CHI), pp. 2865–2877, 2017.

[28] J. Jacob, K. Jha, P. Kotak and S. Puthran, "Mobile attendance using Near Field Communication and One-Time Password," International Conference on Green Computing and Internet of Things (ICGCIoT), pp. 1298-1303, 2015.

[29] C.-H. Ling, C.-C. Lee, C.-C. Yang, and M.-S. Hwang,"A Secure and Efficient One-time Password Authentication Scheme for WSN", International Journal of Network Security, Vol.19, No.2, PP.177-181, Mar. 2017.

[30] C. Shen, Z. Cai, X. Guan, Y. Du and R. A. Maxion, "User Authentication Through Mouse Dynamics," in IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 16-30, Jan. 2013.

[31] F. Ciuffo and G. M. Weiss, "Smartwatch-based transcription biometrics," IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), pp. 145-149, 2017.

[32] X. Li, "Smart Sensing Enabled Secure and Usable Pairing and Authentication. Doctoral dissertation, 2020. Retrieved from https://scholarcommons.sc.edu/etd/6068.

[33] X. Liu, Z. Zhou, W. Diao, Z. Li, K. Zhang, "When Good Becomes Evil: Keystroke Inference with Smartwatch", ACM Conference on Computer and Communications Security, October 2015.

[34] J. Voris, Y. Song, M. Salem, S. Hershkop, S. Stolfo, "Active authentication using file system decoys and user behavior modeling: results of a large scale study", Computers & Security, Volume 87, November 2019.

[35] S. Peisert, Ed Talbot, and T. Kroeger, Principles of Authentication. ACM Workshop on New Security Paradigms Workshop (NSPW), 2013.

[36] C. Li, X. Ji, B. Wang, K. Wang, and W, Xu, SenCS: Enabling Real-time Indoor Proximity Verification via Contextual Similarity, ACM Transactions on Sensor Networks, 17(2), pp 1–22, June 2021.

[37] W. He, M. Golla, R. Padhi, J. Ofek, M. Durmuth, E. Fernandes, and Blase Ur, Rethinking Access Control and Authentication for the Home Internet of Things (IoT), USENIX Security Symposium, Baltimore, MD, 2018.

[38] I. Chenchev, A. Aleksieva-Petrova, and M. Petrov, Authentication Mechanisms and Classification: A Literature Survey, Intelligent Computing, Lecture Notes in Networks and Systems, vol 285. pp 1051-1070, Springer, 2021.