IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 1, 2020, accepted March 31, 2020, date of publication April 28, 2020, date of current version May 13, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2990861

Design and Evaluation of an Authentication Framework for Wearable Devices

ABDULLAH ALHARBI[1] AND TALAL ALHARBI[2]

[1]Department of Computer Science, Community College, King Saud University, Riyadh 11437, Saudi Arabia
[2]Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al Majma'ah 11952, Saudi Arabia

Corresponding author: Abdullah Alharbi (arharbi@ksu.edu.sa)

This work was supported by the King Saud University, Deanship of Scientific Research, Community College Research Unit.

ABSTRACT The demand for wearable technology devices has changed in recent years, due to the fact that wearable devices (WDs) make our lives easier and more comfortable than ever before. WDs are often seen as an extension to mobile devices such as smartphones even thought the size, shape and physical specifications, i.e., the form factors are completely different. The core features of WDs are always accessible and available to users while sole input devices, e.g. keyboard does not exist. In this case, the traditional authentication methods in which users type in passwords on the system can not apply to authenticate WDs. Therefore, this paper introduces an Authentication Framework for Wearable Devices (AFWD) that basically includes an authentication model designed for WDs, capable of creating reliable and secure authentication techniques. Subjective and objective assessment of the AFWD showed that it provides usability, deployability, and security and that people are willing to use it if available. Such a framework is crucial for Intelligent Transportation Systems (ITS) as it provides reliability and trustworthiness of the data transmitted via WDs.

INDEX TERMS Wearable devices, authentication framework, usability, cybersecurity, intelligent transportation systems.

I. INTRODUCTION

One of the major issues in authentication research is that well-known and ''comfortable'' authentication means are co-opted for use on emerging devices, often without an examination of their fit. For instance, passwords and PINs made their way from desktop and laptop computers to mobile devices even though typing accurately on those devices is difficult [11]. Wearable devices (WDs) are an emerging technology that lacks authentication means because although WDs can be considered an extension of mobile devices (e.g., smartphones), the form factor for each is very different. Mobile devices are used in a ''bursty'' way, which means that people use them frequently but for short periods of time [9]. In contrast, WDs are always on, always accessible, and always expected to be connected to other devices and services such as smartphones, Intelligent Transportation Systems (ITS) or the Internet [3], [16]. Despite these differences, WDs are often used in conjunction with mobile devices for reasons such as improved processing power, capabilities such as keyboards, screens, and additional memory.

The associate editor coordinating the review of this manuscript and approving it for publication was Edith C.-H. Ngai.

As WD popularity grows, so does their access to apps and other functionalities that store private information such as email, banking information, and health information. Unauthorized access to the WD may cause interception, interruption, or modification to this private information. Mobile devices often use passwords, biometrics, and personal identification numbers (PINs) to control access to the device and its resources. These authentication methods are not viable on WDs because the input devices are completely different, and many WDs do not have keyboards so entering a password or PIN is more difficult. Therefore, in this paper, we develop an authentication framework that respects the limitations imposed by the WD's form factor rather than simply using possibly unsuitable traditional authentication methods. Since mobile device authentication needs be different from WDs authentication mechanisms, we redefine the authentication problem for WDs. The following list summarizes our considerations when designing a WD authentication mechanism:

1) The different types of WDs define the available authentication methods, such as hand-worn (e.g., smartwatches), head-mounted (e.g., smartglasses), foot-worn (e.g., smart shoes), or body-dressed

(e.g., smart clothing). Not all of them have access to the same data about the wearer [14].
2) For WDs to be effective and beneficial, the device needs to be always on and the data always accessible [3].
3) Many WDs lack input means such as a keyboard or screen, which limits implementing traditional authentication methods, i.e. passwords or PINs.
4) Users must be willing to use an authentication method to encourage adoption. Not protecting their device may put their data at risk.

Data integrity in WDs is significantly crucial for the operations of systems such as Intelligent Transportation Systems (ITS), which rely on the data generated from users to perform certain tasks, e.g. decsion traffic condition [18], [20]. The proposed framework is sufficient to exam the validity and accuracy of the data gathered toward building crowd-sourcing databases.

Our key scientific contributions can be summarized as follows:

- We introduce an Authentication Framework for Wearable Devices (AFWD), which is designed to provide a path to creating authentication methods specific to WDs keeping the four points mentioned above in mind.
- We explore the possibility of creating a secure and usable authentication method to identify whether or not the current WD's wearer is its owner in a transparent and continuous way.
- We investigate whether the proposed method minimizes the wearer's effort and respect the form factor, diversity, and limitations of the WD.

The remainder of our paper is structured as follows: Section II discusses the related work and Section III provides a brief overview of the AFWD. Section IV presents the subjective assessment of the AFWD and Section V presents the objective assessment. Section VI discusses the proposed framework and Section VII concludes the paper.

II. RELATED WORK

The way WDs designed limits the authentication schemes, which can be easily implemented in multiple options in mobile devices. The key advantage of WDs is built-in the sensors that can be used to passively gather authentication data. For this particular reason, we only consider behavioral biometrics research since plenty of this data exists in WDs, such as movement.

In [10], the authors initially attach Motion Recording Sensors (MRSs) to various parts of the participant's body, such as foot, hip, pocket, and arm, prior to the experiment and then collect gait recognition data. They investigate the acceleration signal received from these different body segments and the overall results are evaluated based on the value of the equal error rate (EER). The best EER values achieved are 5%, 7%, 10%, 13% for foot, pocket, arm and hip respectively. Even thought, the authors obtain a relatively less value of EER, i.e., (5%) for the footwear, the sample sizes involved in the study are small and not enough to generalize the results.

The paper [17] proposes a new approach that essentially relies on collected patterns of unconscious blinking and head-movements for user identification. Each user wears a head-mounted display (HMD) that communicates directly with an HMD sensor integrated in the system. The False Accept Rate (FAR) and the False Reject Rate (FRR) the proposed system obtained are 11.3% and 0.5% respectively. This has a negative impact on the confidentiality by unauthorized individuals access to the system.

Some behavioral biometrics, such as hand movements and gestures can be utilized for the authentication of WD. In [19], the authors explore how accelerometer and gyroscope data calculated at smartwatches can help in identifying user's hand, arm and finger gestures. Thus, they develop a unique classifier using the movements of tendons to recognize 37 gestures, in which the accuracy achieves 98%. The classifier is extend to recognize also the written characters, in which the accuracy achieves 95%. In this paper, MotionAuth is proposed using three different gestures, i.e., arm up, arm down and forearm rotation. The EER value MotionAuth achieved is 2.6% based on a sample of 30 participants.

In reality, it is useful to monitor the vital signs, i.e., the measurements of the body's function including body temperature, plus rate and breathing rate. In [15], the authors develop a biometrics authentication system using electrocardiogram (ECG) signals captured from WDs. The problem in this case is that the noise resulting from movement or acquisition can effect the ECG signals. Consequently, the authors use cross correlation between the authentication and registration stages, in which the system obtains 5.2% and 1.9% for FAR and FRR respectively. Similarly, in [8], the authors design BT-Authen, a new authentication technique used to extract body temperature data via smart watches. In their experiment, they consider the skin temperature data gathered from 30 different participants, and the EER value BT-Authen received for three days in row is 1.46%, 2.18%, 3.4% for the first, second and third day respectively.

The best approach to improve FAR and FRR values is via combining multiple biometric modalities. For instance, the paper [12] demonstrates how data extracted from eye blinking features and head movements by Google Glass sensors help identifying different activities, such as reading, chatting, analyzing and math problems. As a result of combining the two biometric modalities, i.e., the eye blinking features and head movements, the accuracy is increased from 67%, which was achieved when the eye blinking is used alone to 82%.

After going through the current state-of-the-art, we found that there is no existing authentication designed especially for WDs. Only a few papers proposed a relatively close solution but for mobile devices. In [5], the authors design a Non-Intrusive and Continuous Authentication (NICA) framework used to authenticate mobile devices based on biometric. The level of annoyance always associated with the authentication

is minimized in this framework because the confidence level is continuously measured during the user's identity processing. The key advantage of this framework is that sensitive information is only revealed when the confidence is set to high. The security level of the framework is evaluated based on the feedback received from 27 participants, where 92% of them realized how secure environment is compared to prior proposed solution.

The paper [6] introduces a mobile device framework for authentication purpose, with the aim to reduce users attempt normally happened in the authentication stage and improve the current issues with transitional authentication techniques. The framework mainly relies on behavioral biometrics mechanism to recognize the owner of the device. As a result, the device users successfully performed all required tasks 67% less when they are explicitly authenticated compared to transparently authenticated.

III. THE AUTHENTICATION FRAMEWORK FOR WEARABLE DEVICES

A. OVERVIEW

To address the WD authentication problem, the Authentication Framework for Wearable Devices (AFWD) was created. The AFWD provides a model to create transparent and continuous authentication methods for WDs. The AFWD exploits the current wearer of WD's biometric patterns (e.g, movement activity, heartbeats, and voice) which are gathered during normal WD use, to verify that the current wearer is also the WD's owner.

The AFWD's output is a security level tag (SLT). SLT represents the current security level in the WD and it shows how certain the AFWD is that the current WD's wearer is in fact its owner. The SLT is continuously calculated and periodically reported to the operating system. The SLT calculation is based on the biometric data that is gathered during the authentication process, and provides an authentication level (low, medium, or high) to other processes. By doing so, the authentication is centralized and does not have to be reinvented for each process. Each process has a minimum SLT level below which access to the process is denied.

B. DEVICE CLASSIFICATION METHOD

The work described here requires a method to determine what type of device we are working with. The types of devices we are considering are: mobile, wearable, or portable. A relevant literature review was done and it has not revealed a method to classify these devices. Therefore, we devised a taxonomy (see Figure 1) that can be used to classify devices into one of four groups: wearable (e.g., smartwatch and smartglasses), mobile (e.g., smartphones), portable (e.g., laptop), or other (those that fit into none of the previous categories).

Here, we list our assumptions:

1) The device that is under classification should have an operating system (OS) that has basic known OS features such as installing and running applications, performing, at minimum, simple computation tasks, and connecting with other devices or the Internet.
2) The primary use of the device must be considered. For example, it is uncommon to use laptop while in motion and it is not expected to be worn on the body. Examples include eBook readers (such as Kindle) and music players, which are all built for specific purposes and thus are not considered multipurpose. Devices such as tablet computers (e.g., iPads) are considered multipurpose since they were not designed only for reading books or playing games, but serve for other general purpose such as browsing and running apps.
3) The device can be easily moved from one place to another; the three categories (wearable, mobile, and portable) will, most of the time, fall under this class. One excluded example here is big servers.
4) The device should fit in a typical pocket such as jeans pockets, t-shirt pockets, or shirt pockets.

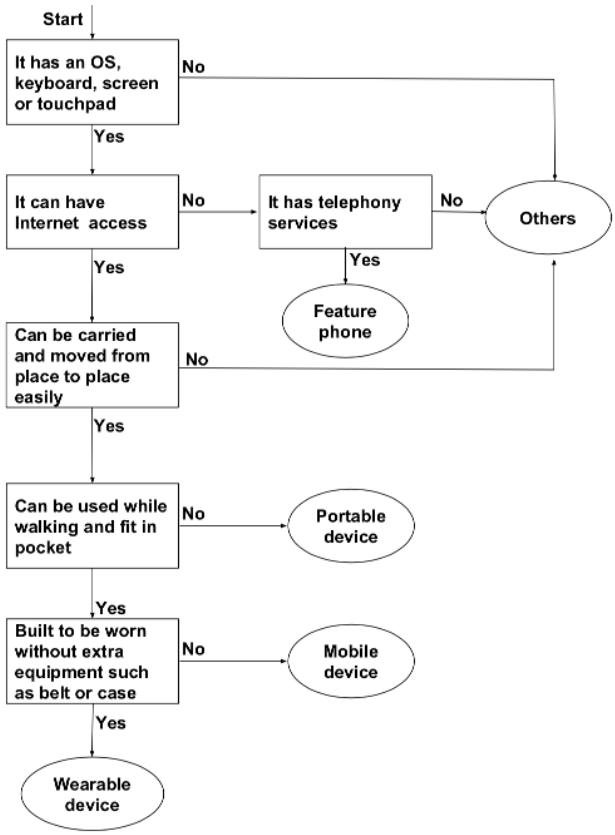

FIGURE 1. Device classification method.

As an example of how the device taxonomy in Figure 1 is used, we consider the example of a typical smartphone. Beginning at the top of Figure 1, we answer 'yes' to the queries as follows: a smartphone has an operating system, can have Internet connectivity, can be carried from place to place easily, can be used while walking and fit in a pocket, but is not built to be worn (not simply held in the hand) without extra equipment, leading to the classification of ''mobile device''.

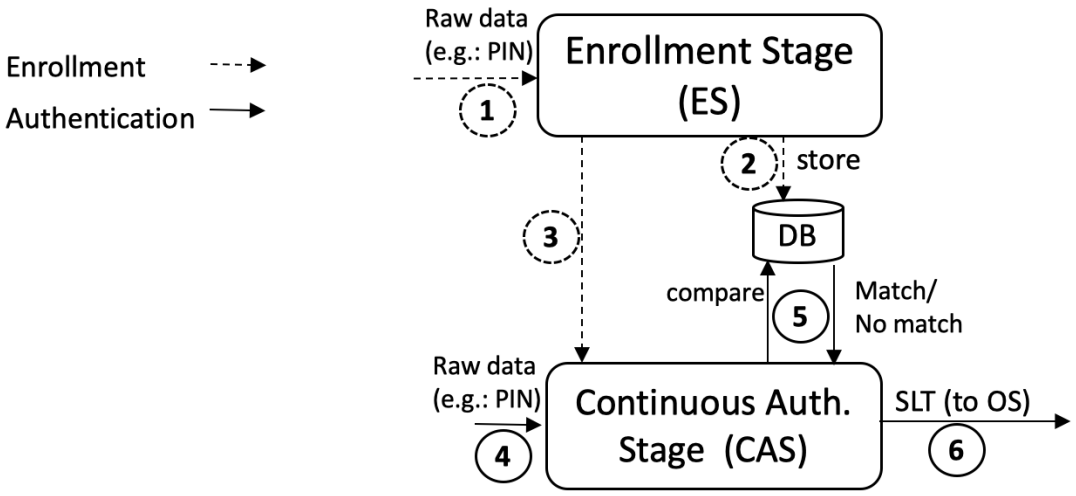

FIGURE 2. A high-level overview of AFWD.

When classifying a non-smart phone, we would answer 'no' to having Internet connectivity, and 'yes' to telephony services, thereby classifying it as a feature phone.

Similarly, for a smartwatch, we answer 'yes' to the queries as follows: a smartwatch has an operating system, has a touchpad, can have Internet connectivity, can be carried from place to place easily, can be used while walking and fit in a pocket, and (different from a smartphone) is built to be worn without extra equipment. Therefore, we classify a smartwatch as a ''wearable device''.

C. AFWD ASSUMPTIONS

The following assumptions must be considered to effectively implement an AFWD-based method:

1) **Biometrics must be valid:** the AFWD expects that the chosen biometric has the following seven factors: universality, uniqueness, permanence, measurability, performance, acceptability, and circumvention [2], [13, pp. 29]. The absence of one or more factor may affect the process of authentication. This is because if the chosen biometric does not have enough uniqueness to distinguish between individuals, it may lead to falsely allowing unauthorized access.
2) **A WD is a single-user device:** the AFWD assumes that the chosen authentication method will be implemented in a single-user WD in order to identify the device's wearer as its owner. The reason for this assumption is that the WD is a personal item that is unlikely to be shared.

D. AFWD DESIGN

The AFWD has two main stages: the *Enrollment Stage* (ES) and the *Continuous Authentication Stage* (CAS) since the AFWD distinguishes between two types of wearers: a first-time wearer (FTW) and a returning wearer (RW). The FTW is the wearer who must first enroll into the system by providing credentials that are used for comparison during the authentication process. In contrast, the RW is the wearer who has already enrolled into the system and has credentials that are already stored in the AFWD database.

An overview of the AFWD is shown in Figure 2. The path that FTW follows is represented by the dashed lines while the solid lines show the path a RW follows. The enrollment path is represented by the shapes with dashed lines and it starts with acquiring the raw data and then storing it in the AFWD database (step 1 and 2 in Figure 2). After the enrollment stage is done, the flow then moves to the CAS (step 3). The shapes with solid lines represent the authentication path. The authentication starts with acquiring the raw data (step 4), comparing it to the content of AFWD database (step 5), and finally calculating the SLT to eventually make the authentication decision (step 6).

E. THE AFWD DESIGNATED DATABASE

The AFWD database stores the credentials that the system and the user agreed upon during enrollment. The credentials can be any information about the device owner that represents any of the three authentication factors(e.g., something you have, something you know, something you are). For example, the database can contain the biometric template that is used in the authentication process. This database resides in the WD so the credentials are kept on the WD to protect its owner's privacy. Both stages (ES and CAS) interact with the AFWD database by inserting new credentials or comparing to those already stored in it.

F. ENROLLMENT STAGE (ES)

The framework starts with the ES, in which a wearer is asked to provide information such as a password, PIN, or biometric samples (which is used as credentials). The ES happens only once. After the ES is successfully completed, the type

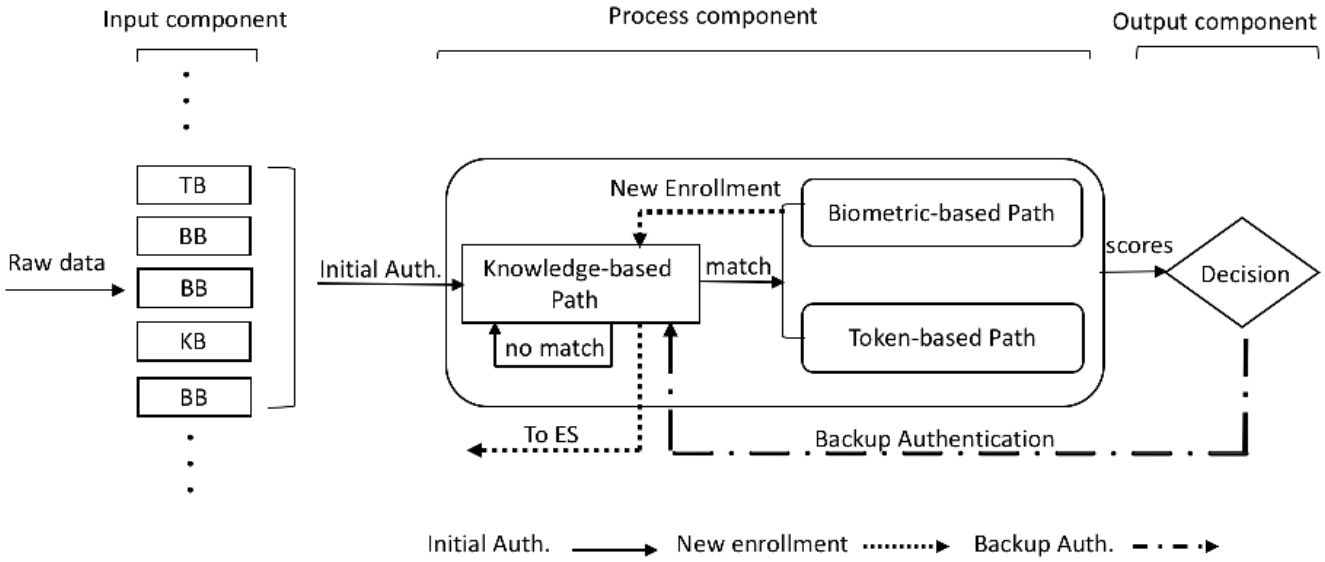

FIGURE 3. The three components of the continuous authentication stage. TB: token-based data, BB: biometric-based data, and KB: knowledge-based data. The rounded corner rectangles are continuous processes while the sharp corner rectangles are not. The solid arrows represent the initial authentication flow, the dotted arrows represent the new enrollment authentication flow, and the dashed arrows represent the backup authentication flow.

of wearer then becomes a RW because the credentials are already stored in the AFWD database.

G. CONTINUOUS AUTHENTICATION STAGE (CAS)

The CAS consists of three components: input, process, and output, as shown in Figure 3. The result of the CAS is the SLT, which represents the security level in the WD, and is periodically calculated and reported to its operating system to be used by other WD processes that require an authentication. The CAS is broken into several parts, as discussed in the following sections:

1) THE AFWD INPUT COMPONENT

The input component is comprised of information collected about the current WD wearer. It represents one or more of the three main authentication factors; knowledge-based factor (e.g., graphical password), token-based factor (e.g., tethered smartphone), and biometric-based factor (e.g., voice).

2) THE AFWD PROCESS COMPONENT

The process component consists of three paths, each of which represents one of the authentication factors. Each path interacts with the AFWD database that stores all credentials (PIN, biometric templates, or trusted device identifiers) that the wearer and the system agreed upon during the ES.

- **The knowledge-based path:** represents the ''something you know'' class. In this path the information provided by the wearer (e.g., PIN) is compared to the one stored in the AFWD database. The comparison result is either match (when the credentials provided by wearer matches the one stored in the database) or non-match (when the credentials provided by wearer does not match the one stored in the database).

Although the knowledge-based path is part of the CAS, it does not have to be continuous but is requested only when needed. It an explicit authentication that may be requested in several cases as follows:

1) Initial Authentication: If the wearer is a RW who is already enrolled into the system, takes off the WD and then puts it back on again, an explicit authentication is needed. The reason for requiring an explicit authentication is that the AFWD cannot guarantee that the WD is worn by its owner next time. This kind of explicit authentication happens infrequently because we assume people wear the WD for long periods of time (e.g., a whole day) which means a minimum of one explicit authentication per day.
2) Backup Authentication: Some sensitive tasks cannot be performed because there is not enough information available upon which to base the authentication decision. For this reason, the backup authentication is used to raise the SLT level which allows performing sensitive tasks. For example, if the SLT is at low level, the wearer is not able to perform some sensitive tasks such as banking. Therefore, the wearer must wait until sufficient data is collected in order to raise the SLT, or can raise it instantly by using this backup authentication.
3) New Enrollment Authentication: The knowledge provided explicitly authenticates the wearer before adding any new credentials such as biometric samples or tokens to the AFWD database. By doing so, the AFWD ensures that this addition is done by an authorized wearer.

- **The token-based path:** A token can be a physical object such as a tethered smartphone or the WD itself. For example, we could check if the smartphone that is tethered to the WD is nearby by checking if they are connected via Bluetooth. This path takes the input token data (e.g., connectivity status to known device) and compares it to the content stored in the AFWD database (e.g., list of known devices). Similar to we saw in the knowledge-based path, the comparison result in token-based path is also either match or non-match; the known device is nearby or its Bluetooth is on or off. Infrequently, WD's wearer may need to add a new token or delete others. For example, if a wearer sells a smartphone that is used as a token, the smartphone is no longer a trusted token and therefore should to be immediately deleted from the database. In order to add or delete a new token to or from the AFWD database, an explicit authentication is required. By doing so, we make sure that this process of addition or deletion is legitimate. If the result of this authentication is a match, then the AFWD goes to the enrollment stage (ES) to add the new token to the AFWD database.
- **The biometric-based path:** processes the ''something you are'' data, e.g., biometric traits such as gait, or voice. This path performs a *feature extraction phase* in which distinctive features are extracted, and a *comparison* phase where the extracted features from the newly entered biometric are compared to the ones stored in the AFWD database [13, pp. 7] [7, pp. 58].
  1) Feature Extraction Phase: salient and distinctive features of the biometric input are extracted and represented digitally. The extracted features are used in the comparison phase.
  2) Comparison Phase: extracted features are compared to those of its counterpart that is stored in the AFWD database. The result of the comparison process is a matching score; the higher the score, the higher the biometric similarity.
     Comparison is a verification process because the comparison is a one-to-one [13, pp. 9] [10] which requires a claim of identity. Thus, we are assuming that the person who is wearing the WD is the owner, and the act of wearing it is considered the claim of identity.

3) THE AFWD OUTPUT COMPONENT

In the AFWD output component, the result of the three paths is used to create the final output: the *Security Level Tag (SLT)*. The SLT represents to what level the WD is used only by its owner. It determines the security level of the WD based on the data gathered; the levels range from *low*, which means that the data gathered does not match that of the WD's owner, to *high* which means the data gathered closely matches that of the WD's owner. These levels are used to allow or disallow tasks, such as sending text messages and reading email. The SLT starts *low* and it changes based on the gathered data analysis results; it increases with matches and decreases with non-matches. After wearing the WD and performing an explicit authentication (e.g., entering the PIN), the SLT moves to *high* for a predefined period of time during which the SLT is recalculated based on the most recently gathered data and then reported to the operating system.

One way to improve the accuracy of biometric-based authentication is by using a fusion process to consolidate the results of several independent authentication methods into a multimodal or multifactor biometric [18]. Fusion methods include feature-level (e.g., feature vectors from similar methods are merged to create a single feature vector that represents multiple sources), score-level (e.g., accuracy scores from multiple sources are normalized to a single scale) and decision-level (e.g., the match/non-match decisions from multiple sources are combined, often using majority voting rules). We used decision-level fusion in the AFWD because it produces binary match/non-match decisions rather than accuracy or match scores. Furthermore, the authentication factors used in the AFWD are not all biometrics, thus feature-level fusion is not suitable since not all factors have feature vectors. Since decision-level fusion loses the granularity of score level fusion (e.g., scores of 60% and 99% accuracy would both result in a ''match'' decision assuming a 50% threshold), we used a weighted decision-level fusion: each decision is given a different weight based on how accurately it represents the owner. For example, if we have two biometrics, we would give the one that has high distinctiveness a higher weight than the one with lower distinctiveness. Further discussion and a worked example are presented in Section III-H5.

H. AFWD DATA STRUCTURES

1) SCORE OBJECT (SObj)

The AFWD output component calculates the SLT based on SObj. The SObj is a tuple as follows:

$$SObj = (s, w)$$

where s is the score representing the comparison results either match or non-match. w represents the input object's weight (0 to 1).

2) INPUT OBJECT

The input object represents one of the three types of raw data entered into the AFWD: biometric, knowledge, and token objects, as follows:

1) **Knowledge Object (KObj):** The input *KObj* is a tuple as follows:

$$KObj = (ID, t, tp, r)$$

where ID is a unique identifier for the object, t is the time the raw data was entered, tp is the type of knowledge-based authentication method used, such as password or PIN, and r refers to the raw data entered by the user.

2) **Token Object (TObj):** The input *TObj* is a tuple as follows:

$$TObj = (ID, t, dt, upd)$$

where *ID* is a unique identifier for the object, *t* represents the time that the token was added to the AFWD database, *dp* refers to the device type that is used as token such as smartphone, and *upd* represents the unique physical address of the token such as the International Mobile Equipment Identity (IMEI) [1].

3) **Biometric Object (BObj):** A *BObj* is a tuple as follows:

$$BObj = (ID, t, bt, fv, w)$$

where *ID* is a unique identifier for the object, *t* refers to the time the raw data was entered, and *bt* represents the type of biometric used, such as fingerprint, face, voice, or gait. *fv* represents the feature vector extracted from the raw data, and *w* represents the weight that is given to the biometric based on how distinctive it is in identifying the WD's owner. The more distinctive the biometric, the higher the weight assigned to it.

The algorithm for data collection is shown in Algorithm 1.

Algorithm 1 The AFWD data collection algorithm

```
set predefinedPeriod {How often data is collected}
set maxDataSize
set minDataSize
while timePassed < predefinedPeriod do
    collect data from sensor
    if maxDataSize > dataSize > minDataSize then
        create input object
        send object to input buffer
    end if
end while
```

3) OUTPUT BUFFER

The AFWD process component sends all SObjs to the AFWD output component where they are placed in an output buffer until needed for the SLT calculation.

4) OUTPUT OBJECT

The SLT is the only output of the AFWD and is a tuple as follows:

$$SLT = (t, l)$$

where *t* is the time the SLT was calculated and *l* is the value of the SLT: high, medium, or low.

5) SLT CALCULATION PROCESS

As previously discussed, the SLT is calculated periodically based on the objects available in the output buffer. To calculate the SLT, the AFWD gives points to each biometric and token object that represents the effect they have on the SLT value. The effect is determined by the weight in the case of the biometric objects, which can be low, medium, or high. Tokens are equally weighted since there is no difference between two different tokens in representing the WD's owner.

TABLE 1. The token and the biometric objects' weights that are used to calculate the SLT. B_h means *high* distinctiveness, B_m *medium* distinctiveness, and B_l means *low* distinctiveness. T represents the token object.

Objects	Point (score is match)	Point (score is non-match)
B_h	1	0
B_m	0.5	0
B_l	0.25	0
T	0.15	0

For example (see Table 1), if the result of the comparison in the process component (see Figure 3) is *match*, the biometric object is assigned the points 1, 0.50, and 0.25 to the biometrics that have high, medium, and low distinctiveness respectively. If it is *non-match*, the points given is zero. All token objects are given the same points (0.15) since they do not represent the owner (i.e., a token can be used by more than one person), but it could help in the authentication process. Similarly, if the comparison result of the token object in the process component is *non-match*, the points given is also zero.

The formula to calculate the SLT's level of security is as follows:

$$l = \frac{tp}{bw}$$

where *l* is the level of security, and *bw* is the balanced weight derived from all the objects' weights that are used in the SLT calculation. Objects' weights are added together and used to calculate the *bw* as follows:

$$bw = \begin{cases} 1, & \text{if } tw < 1 \\ tw, & \text{if } tw \geq 1 \end{cases}$$

where *tw* is the total of all objects' weights given during the objects' creation, and *tp* is the total points and is calculated using Table 1.

The following example explains how to calculate the SLT. Assume that we have three SObjs coming from the AFWD process component. One is the result of comparing a biometric object that has high distinctiveness (e.g., B_h) against its counterpart in the AFWD database and the comparison result was *match*. Another is the result of comparing a biometric object that has low distinctiveness (e.g., B_l) against its counterpart in the AFWD database and the comparison result was *non-match*. Last is a token object T and the comparison result was *match*. First, we need to calculate the *tp* using Table 1: $B_h = 1$, $B_l = 0$, and $T = 0.15$. Therefore, the *tp* is:

$$tp = 1 + 0 + 0.15 = 1.15$$

Next, we calculate *bw* using: $B_h = 1$, $B_l = 0.25$, and $T = 0.15$. Therefore, the *bw* is 1.4. Finally, the level of security is:

$$l = \frac{1.15}{1.4} = 0.82 = 82\%$$

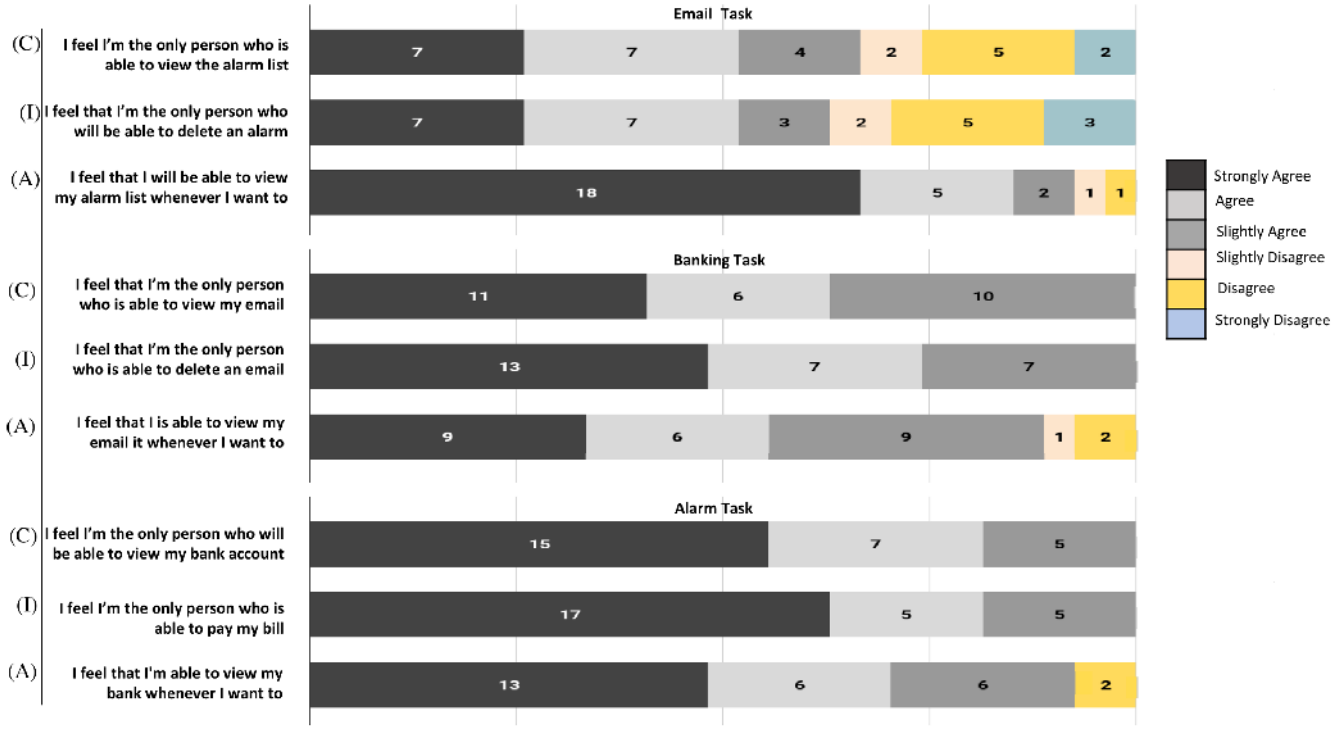

FIGURE 4. The participants' opinions toward per task AFWD assessment in terms of the CIA principles: (C) is confidentiality, (I) is integrity, and (A) is availability.

TABLE 2. An example of what tasks can be performed based on the SLT value.

SLT Value (%)	Reported Level	Allowed Tasks
SLT≥80	High	banking
80>SLT≥ 60	Medium	access photo
60>SLT ≥ 40	Low	weather info

This means that the WD is 82% certain that it is worn by the owner. Based on this, the developer can set a threshold for each security level and level needed for any function or task (see Table 2 for examples).

IV. THE AFWD SUBJECTIVE ASSESSMENT: USER PERCEPTIONS OF THE AFWD

One of the goals of the AFWD is to minimize user effort. In this section, we present a subjective assessment of the AFWD via a user study.

A. STUDY GOAL

In this study, the AFWD was assessed from the user's perspective. The goal is to determine whether or not the participants believe that the AFWD-based method provides trustworthy security, and whether or not users accept and would consider using the AFWD, if it was available on their WDs.

B. PARTICIPANTS

The 27 participants were 18 years old and above. They were recruited using convenience sampling strategies such as mailing lists, social media, word of mouth, and personal invitation. The percentage of people who were between the ages of 25 and 34 was 71%, 19% between 18 and 24, and 9% between 35 and 44. All participants were smartphone users, and 90% of them used an iPhone, while the rest used Android-based devices. The percentage of participants who own a WD was 33.3%; all of them are the hand-worn type such as smartwatch or fitness tracker. Our study was IRB-approved prior to its start.

C. EQUIPMENT AND METHODOLOGY

We used an LG-W100 smartwatch running Android Wear OS version 6.0.1 and a Bluetooth-connected LG Nexus 5 smartphone running Android OS version 6.0.1. We created an Android app for the smartwatch called `AFWDStudy` that imitates some of the AFWD's functionalities; it is not an AFWD prototype as it serves the purpose of this study only.

The `AFWDStudy` app background is either red, yellow, or green, which corresponds to Low, Medium, and High SLT levels. These levels were adjusted manually by another app installed on the smartphone and controlled by the experimenter during the study.

The investigator started by briefly explaining the AFWD's main features. The participants were asked to assume that they had already enrolled into the system, they were the owner of the smartwatch, an AFWD-based authentication method was already implemented, and that the device was able to collect and analyze their biometric data. Initially, the security

level was set to low (red background) and was switched gradually by the experimenter to medium (yellow background) and then high (green background). While the security level was low, the participants were asked to access the banking app or email. This access was rejected since both require a higher security level than low.

Next, the participants were asked to perform several tasks. First task is the Alarm Task which requires low SLT level and above and has two sub-tasks: Viewing the alarm list and deleting one from it. Second task is the Email Task which requires medium SLT level and above and has two sub-tasks: Reading and Deleting an email. Third task is Banking Task which requires high SLT level and has two sub-tasks: View the bank account and pay a current bill.

All participants successfully performed all tasks, after which they filled demographic questionnaire, followed by a questionnaire designed to assess the subjective AFWD security.

D. RESULTS

Participants were asked to rank each task in terms of what level of security that they felt it should require, regardless of what rank the experimenters gave it. We ranked all alarm tasks as requiring a low security level and the majority (80%) of the participants agreed with this ranking. It was unexpected to have 20% of the people ranking alarm higher than low because setting and deleting and alarm is not overly sensitive and can sometimes be accessible on a locked screen, such as in some smartphones. Those who ranked alarm as medium or high justified their choices by saying that a low security level might cause privacy issues such as unauthorized people viewing their schedule or deleting an alarm, causing them to miss an important meeting.

We ranked all email tasks as requiring a medium security level; nine participants (36%) agreed with our ranking. The 18 remaining participants felt that email should be ranked as a high security level task, which is understandable because the content of email may be personal.

In the banking task, participants were required to perform two sub-tasks: view their balance and pay a current bill. Most of the participants felt that this task should require a high security level, which was expected. However, two participants had a different opinion and ranked this task either as medium or low. This was not expected for a sensitive action like this which involves a financial transaction, but may be because the participants depend on the bank to protect them in cases of fraud.

Six-point Likert Scale questions were asked about the tasks with answers ranging from ''strongly disagree'' to ''strongly agree.'' and were grouped according to security principles (confidentiality, integrity, and availability). The results show that confidentiality is managed effectively in the AFWD in the medium and high security levels. This is supported by the fact that all participants agreed that they are the only owner who is able to view emails and bank balances. In the alarm task, 64% of the participants agreed that the owner is the only person who is able to view the alarm list, which suggests that the AFWD also manages confidentiality in such a task. It was not expected that the majority of participants would agree that only the owner is able to view the alarm list. Some participants may have created and inaccurate mental model that affected their responses. Also, they may think of security as a binary value in which it either allows or disallows (protecting all or nothing).

The users agreed that the integrity of the data in tasks that require medium and high level security is not affected, and data modification can only be performed by an authorized wearer. This is supported by our participants' opinions in which they felt that only the owner is able to delete an email or pay a bill. In the alarm task, the effect on integrity is evaluated by the ability to delete an alarm from the alarm list. Since the alarm task requires a low security level, it is not expected that deleting an alarm is restricted to those who are authorized. However, 64% of participants felt the opposite. This might also be related to an inaccurate mental model.

Our participants felt that the availability of their data in all tasks is not affected in the security measures applied by the AFWD. 93% of participants felt that they they are able to access information on their devices. In the email and banking tasks, 7% of the participants felt that access attempts would be rejected at some point, and that their data would not be available whenever needed. Those participants believed that behavioral biometrics might be affected by emotions or medical issues such as having a fast heartbeat or sore throat. Similarly, in the alarm task, participants also felt that availability is not affected by the AFWD security measures. This was expected since the alarm task requires only a low security level in which all people are able to perform the task successfully.

E. GENERAL AFWD ASSESSMENT

This assessment evaluates the perceived level of security produced by the AFWD in terms of security principles in which we see how users feel about the confidentiality, integrity, and availability of their data while using a WD with an AFWD-based authentication method implemented. We also present an assessment based on the comparison between their current authentication method and the AFWD-based authentication method. Finally, we test whether or not having multi-factor and transparent authentication as provided by the AFWD would encourage people to use it when it is available.

1) **Assessment Based on The CIA Triad:** The majority of the participants (96%) felt that the AFWD-based authentication manages confidentiality by preventing an unauthorized accesses to the owner data. Similarly, all participants felt that an AFWD-based authentication method preserves the integrity of the owner's data by preventing any data alteration by unauthorized people. The majority of the participants (81%) felt that availability is not affected in the AFWD-based authentication method.

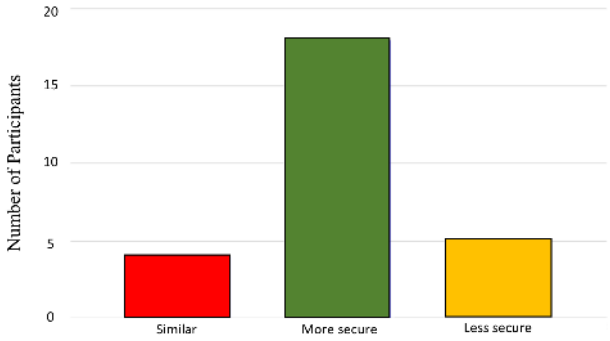

FIGURE 5. How participants compare the AFWD to their current authentication methods.

2) **Assessment Compared to Current Authentication Method:** Participants were asked to compare the proposed AFWD-based authentication method to their current method. Figure 5 shows that 66.7% (18 participants) felt that an authentication method based on AFWD is more secure than their current authentication method while 14.8% (four participants) felt it is similar. The remaining 18% (five participants) felt that the proposed framework will be less secure than their current authentication method. This might be affected by the lack of knowledge or trust in behavioral biometrics because they are not as familiar to users as other traditional authentication methods such as a password, PIN, or fingerprint. Those who saw the AFWD as less secure than their current authentication method still think it is secure or protected when they were asked how they would describe it.
3) **Multi-factor Authentication and Transparent Authentication Effect:** We asked participants whether having multi-factor authentication and transparent authentication features would encourage them to use the AFWD-based authentication. All participants but one believed these two features would encourage them to do so. This positively supports the acceptability of the AFWD when available since the prospective users felt that it provides some aspects of two important features: security and usability.
4) **How Do You Describe the AFWD?** We asked our participants to choose one or more words from a list of 14 positive and negative adjectives that they thought describe the AFWD. We used the concept of a Word Cloud to show participants choices as shown Figure 6. The responses show that our participants felt that the AFWD is both secure and usable, as supported by the fact that the three most important words chosen by our participants were *protected* and *secure*, which are related to security, and easy to use, which is related to usability.

V. THE AFWD OBJECTIVE ASSESSMENT

Usability-deployability-security (UDS) is a framework developed by Bonneau *et al.* [4] to analyze authentication methods that aim to replace traditional passwords. It evaluates authentication schemes in terms of usability, deployability, and security; the authentication scheme either ''offers the benefit'', ''almost offers the benefit,'' or ''does not offer the benefit'' [4]. In this section, we assess the AFWD from an objective point of view using UDS framework. Some benefits are not applicable in our scheme and if this is the case, we mark it not applicable (NA).

FIGURE 6. The adjectives chosen by our participants to describe the AFWD. Larger print represents words chosen more frequently.

TABLE 3. The usability assessment of the AFWD-based authentication method. $\surd$ means it offers the benefit, $\sim$ means it almost offers the benefit, χ means it does not offer the benefit.

Usability	
Benefits	**Assessment**
Memorywise-Effortless	$\sim$
Scalable-for-Users	$\surd$
Nothing-to-Carry	$\surd$
Physically-Effortless	$\surd$
Easy-to-Learn	$\surd$
Efficient-to-Use	$\surd$
Infrequent-Errors	$\sim$
Easy-Recovery-from-Loss	$\surd$

A. USABILITY ASSESSMENT

Our usability assessment based on the UDS framework shows that the AFWD-based authentication methods are usable since they offer almost all benefits (see Table 3). This also matches our participants' choices in the subjective assessment study in which the majority described the AFWD as ''easy to learn,'' and ''learnable'' which are two usability aspects.

1) **Memorywise-Effortless:** The AFWD has a knowledge-based backup authentication mechanism, which might require memorization. However, this process is not a fundamental feature in the AFWD since it depends mainly on session-based behavioral biometrics. This suggests that the AFWD needs nothing memorized during its core function since the authentication is continuous and transparent. However, we conservatively chose ''almost offers the benefits.''
2) **Scalable-for-Users:** The AFWD-based authentication method offers this benefit since it assumes that the WD

is for a single user and therefore if the wearer uses the AFWD on other WDs, it does not increase their load.

3) **Nothing-to-Carry:** Although a token is considered one of the factors that can be used in the authentication decision in the AFWD, it is only used upon availability (e.g., a tethered smartphone). Therefore, the AFWD offers this benefit since because it requires nothing to carry beyond the WD itself.
4) **Physically-Effortless:** Users are not required to make an effort because all needed data is gathered transparently.
5) **Easy-to-Learn:** The AFWD is easy to learn since users are not required to have specific skills in order to use it. Enrollment might require some learning but it should be straightforward since users are asked to provide behavioral biometrics that are part of their daily activities such as voice and walking. Therefore, the AFWD offers this benefit.
6) **Efficient-to-Use:** The AFWD offers this benefit since it is transparent; users do not spend time on each authentication. The enrollment may take some time that is longer than the authentication process but this is considered reasonable according to UDS framework since enrollment should happen only once.
7) **Infrequent-Errors:** Users are not required to perform specific tasks in order to authenticate themselves, therefore input errors are infrequent. Rather, the framework exploits what WD sensors can gather about users as they go about their regular tasks and uses data from this as the authentication mechanism's input. In general, being behavioral biometrics oriented, the AFWD-based authentication method may make errors. Therefore, the AFWD ''almost offers the benefit.''
8) **Easy-Recovery-from-Loss:** One of the AFWD features is that it has a backup authentication that is used when the WD does not have enough information to authenticate the current wearer. Also, this feature can be used to replace old biometric templates that are no longer valid for authentication. Therefore, the AFWD offers this benefit.

B. DEPLOYABILITY ASSESSMENT

As can be seen in Table 4, our deployability assessment shows that the AFWD is not yet mature. It also shows that there are some accessibility issues especially with biometrics, which the AFWD mostly depends on, since not all users can provide the required traits. In general, given that we ranked three benefits one of each kind, ''offer'', ''does not offer'', and ''almost offers'' the benefit, the AFWD is not yet mature enough to be fully deployed.

1) **Accessible:** AFWD-based authentication method is almost accessible where a user is not prevented from using it because it depends on what kind of method is used. For example, the authentication method based on heartbeat is accessible by all people. However, methods that depend on gait are not accessible by disabled people. Therefore, the AFWD almost offers this benefit.
2) **Negligible-Cost-per-User:** There is little cost in order to deploy an authentication method based on the AFWD. In fact, the AFWD aims to provide a strong authentication base that requires no extra equipment to authenticate users. Given that tokens are optional, the AFWD offers this benefit.
3) **Server-Compatible:** We chose ''NA'' because the authentication in the AFWD does not need an interaction with any server and it is only a client-side process.
4) **Browser-Compatible:** We chose ''NA'' because there is no web browser needed in the AFWD-based authentication methods.
5) **Mature:** the AFWD is still in the development process and has not been implemented on any scale. Therefore,the AFWD does not offer this benefit.
6) **Non-Proprietary:** The AFWD was developed to be hardware and software independent and therefore, the AFWD offers this benefit.

TABLE 4. The deployability assessment of the AFWD-based authentication method. $\surd$ means it offers the benefit, $\sim$ means it almost offers the benefit, χ means it does not offer the benefit.

Deployability	
Benefits	**Assessment**
Accessible	$\sim$
Negligible-Cost-per-User	$\surd$
Server-Compatible	NA
Browser-Compatible	NA
Mature	χ
Non-Proprietary	$\surd$

C. SECURITY ASSESSMENT

Our security assessment using the UDS framework shows that the AFWD offers almost all of the benefits, as can be seen in Table 5 and in the list below. Our assessment shows that the AFWD either offers or almost offers 10 security benefits out of 12 from the UDS framework. This indicates that the AFWD provides trustworthy security, which is in accordance with how the potential WD users feel toward the AFWD security as presented in our subjective assessment (Section IV) . The only benefit that the AFWD-based authentication method struggles to provides is the resilience to internal observation.

1) **Resilient-to-Physical-Observation:** is an example of a shoulder surfing attack, which is where an attacker observes the victim to get the secret key such as a password or PIN. Authentication in the AFWD happens transparently and the user has no explicit interaction that can be observed by an attacker. The only situation that can be observed is explicit authentication, which can be replayed by an attacker to gain access to high level tasks or possibly enroll their biometrics instead of those of the legitimate wearer. This, however, would require having physical possession of the WD and any companion device.

TABLE 5. The security assessment of the AFWD-based authentication method. $\surd$ = offers the benefit, $\sim$ = almost offers the benefit, χ does not offer the benefit, and NA not applicable.

Security	
Benefits	**Assessment**
Resilient-to-Physical-Observation	$\sim$
Resilient-to-Targeted-Impersonation	$\sim$
Resilient-to-Throttled-Guessing	$\surd$
Resilient-to-Unthrottled-Guessing	$\surd$
Resilient-to-Internal-Observation	χ
Resilient-to-Leaks-from-Other-Verifiers	$\surd$
Resilient-to-Phishing	$\surd$
Resilient-to-Theft	$\surd$
No-Trusted-Third-Party	$\surd$
Requiring-Explicit-Consent	$\surd$
Unlinkable	$\surd$

2) **Resilient-to-Targeted-Impersonation:** It depends on the type of biometric being used in the AFWD-based authentication. For example, it is hard for an acquaintance to impersonate users when using an authentication method that depends on heartbeats or body temperature. However, it is possible when using an authentication method based on gait or voice, as an acquaintance may be able to imitate how people walk or talk which means it is vulnerable to a replay attack. We conservatively chose ''almost offer the benefit.''
3) **Resilient-to-Throttled-Guessing:** Although we say that the AFWD offers this benefit, the explicit authentication method may not be resilient to guessing. Also, it depends more on the security measures on the device in which the explicit authentication is performed. For example, if the explicit authentication is applied in a companion smartphone, the risk varies whether it is a password, PIN, or fingerprint. UDS framework suggests that this benefit might be granted if an attacker is limited to around 10 guesses per account per day. Many smartphones lock out the user after a small number of failed attempts to enter.
4) **Resilient-to-Unthrottled-Guessing:** The risk comes from the explicit authentication which is vulnerability to guessing attacks. However, having a limited number of guesses per account per day is widely available in smart devices, so the AFWD offers this benefit.
5) **Resilient-to-Internal-Observation:** There are no user inputs in the AFWD core authentication process, which lowers the chance of successfully impersonating a user by intercepting their inputs. However, a biometric template attack is possible in which the attacker steals the biometric template and then replays it against the one stored in the database. The AFWD depends on multimodal biometrics, which makes this attack harder since it would require an attacker to steal all current biometric templates to increase the SLT level and therefore gain the access to the sensitive resources.
6) **Resilient-to-Leaks-from-Other-Verifiers:** The authentication is performed locally in the WD, which suggests there are no other verifiers such as a remote server. The data collected are stored, analyzed, and classified on the WD. Therefore, the AFWD offers this benefit.
7) **Resilient-to-Phishing:** The authentication happens locally so the probability of simulating a valid verifier is missing and therefore no credentials can be stolen. Therefore, this benefit is offered in the AFWD.
8) **Resilient-to-Theft:** The possession of the WD by itself imposes little risk since the attacker would be locked out after a short time when the security level goes down as a result of the AFWD's low confidence that the current wearer is the owner of the device. If a companion smartphone is used for backup authentication, the possession of it does not guarantee unauthorized access. It depends on whether a security measure is used and whether or not these measures control the access well. This criterion suggests that the modest strength of a PIN would be enough to mark this as ''offers benefit.''
9) **No-Trusted-Third-Party:** The AFWD does not rely on any third party. Therefore, we say that it offers the benefit.
10) **Requiring-Explicit-Consent:** The AFWD requires that the wearer use explicit authentication every time they put on the WD. Users are asked to provide credentials before using the AFWD which can be skipped and therefore they are not enforced to use the AFWD without their consent.
11) **Unlinkable:** This benefit states that ''colluding verifiers cannot determine, from the authenticator alone, whether the same user is authenticating to both'' [4]. However, authentication happens locally and there is no interaction with any verifier that might be affected by any colluding.

VI. DISCUSSION

The AFWD overcomes the WD authentication problem as follows:

- The AFWD supports creating an effective and trustworthy security mechanism for WDs based on sensor data. It is trustworthy because it uses multi-factor and multimodal biometric authentication in which the security is improved and as evidenced by our subjective and objective assessments results. Also, the authentication in the AFWD is continuous which provides the ability to repeatedly check the owner's identity.
- The AFWD respects the unique form factor of WDs considering that they should be always available and always on by using behavioral biometrics to authenticate wearers transparently as the wearer goes about their regular tasks.Transparency is satisfied by the ability to collect the authentication data in the background.
- The AFWD respects the limitations of WDs such as the absences of input means by using factors such as behavioral biometrics.

- The AFDW-based authentication is acceptable by WD's owners' methods because it depends on factors such as behavioral biometrics that require little effort from the wearer compared to entering a password or a PIN.
- By using factors that do not require explicit user interaction, such as behavioral biometrics, the AFWD minimizes the wearer's interaction and effort to authenticate them. This is satisfied by the ability to collect the authentication data transparently.
- AFWD is hardware and software independent. This means the AFWD-based authentication method should work in any WD no matter what kind of hardware or software is installed.

VII. CONCLUSION

WDs are an immature technology that lacks a viable authentication mechanism that is capable of protecting its sensitive data. Solving such a problem is constrained by limitations such the unique form factor of WDs, which requires the device to always be on, and the lack of input methods that might be used in a traditional authentication methods, such as a passwords or PINs. This research aims to solve this problem by developing a unique AFWD, a framework works as a basis to build a transparent and continuous authentication method for a WD to protect its sensitive data and respects its limitations at the same time.

ACKNOWLEDGMENT

This project was supported by King Saud University, Deanship of Scientific Research, Community College Research Unit and Abdullah Alharbi would like to thank them for this support.

REFERENCES

[1] *IMEI Status Check*. Accessed: Feb. 29, 2020. [Online]. Available: https://www.t-mobile.com/verifyIMEI.aspx and https://www.t-mobile.com/verifyIMEI.aspx

[2] C. Ashby, A. Bhatia, F. Tenore, and J. Vogelstein, "Low-cost electroencephalogram (EEG) based authentication," in *Proc. 5th Int. IEEE/EMBS Conf. Neural Eng.*, Apr. 2011, pp. 442–445. [Online]. Available: http://ieeexplore.ieee.org.zorac.aub.aau.dk/ielx5/5773344/5910465/05910%581.pdf?tp=&arnumber=5910581&isnumber=5910465

[3] L. Bass and B. E. John, "Linking usability to software architecture patterns through general scenarios," *J. Syst. Softw.*, vol. 66, no. 3, pp. 187–197, Jun. 2003.

[4] J. Bonneau, C. Herley, P. C. V. Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes," in *Proc. IEEE Symp. Secur. Privacy*, May 2012, pp. 553–567.

[5] N. Clarke, S. Karatzouni, and S. Furnell, "Flexible and transparent user authentication for mobile devices," in *Proc. IFIP Int. Inf. Secur. Conf.* Springer, 2009, pp. 1–12.

[6] H. Crawford, K. Renaud, and T. Storer, "A framework for continuous, transparent mobile device authentication," *Comput. Secur.*, vol. 39, pp. 127–136, Nov. 2013.

[7] R. Das, *Biometric Technology: Authentication, Biocryptography, and Cloud-Based Architecture*. Boca Raton, FL, USA: Taylor & Francis, 2014, ch. 1–2.

[8] T. S. Enamamu, N. Clarke, P. Haskell-Dowland, and F. Li, "Smart watch based body-temperature authentication," in *Proc. Int. Conf. Comput. Netw. Informat. (ICCNI)*, Oct. 2017, pp. 1–7.

[9] H. Falaki, R. Mahajan, S. Kandula, D. Lymberopoulos, R. Govindan, and D. Estrin, "Diversity in smartphone usage," in *Proc. 8th Int. Conf. Mobile Syst., Appl., Services (MobiSys)*, New York, NY, USA, 2010, pp. 179–194, doi: 10.1145/1814433.1814453.

[10] D. Gafurov and E. Snekkenes, "Gait recognition using wearable motion recording sensors," *EURASIP J. Adv. Signal Process.*, vol. 2009, no. 1, pp. 7:1–7:16, Dec. 2009, doi: 10.1155/2009/415817.

[11] K. K. Greene, M. A. Gallagher, B. C. Stanton, and P. Y. Lee, "I Can't Type That! P@$$w0rd entry on mobile devices," in *Proc. Hum. Aspects Inf. Secur., Privacy Trust (HCI)*, in Lecture Notes in Computer Science, vol. 8533, 2014, pp. 160–171.

[12] S. Ishimaru, K. Kunze, K. Kise, J. Weppner, A. Dengel, P. Lukowicz, and A. Bulling, "In the blink of an eye: Combining head motion and eye blink frequency for activity recognition with Google glass," in *Proc. 5th Augmented Human Int. Conf. (AH)*, 2014, p. 15.

[13] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to Biometrics*. New York, NY, USA: Springer, 2011.

[14] H. Jiang, X. Chen, S. Zhang, X. Zhang, W. Kong, and T. Zhang, "Software for wearable devices: Challenges and opportunities," in *Proc. IEEE 39th Annu. Comput. Softw. Appl. Conf.*, Jul. 2015, pp. 592–597.

[15] S. J. Kang, S. Y. Lee, H. I. Cho, and H. Park, "ECG authentication system design based on signal analysis in mobile and wearable devices," *IEEE Signal Process. Lett.*, vol. 23, no. 6, pp. 805–808, Jun. 2016.

[16] S. Mann, "Wearable computing: Toward humanistic intelligence," *IEEE Intell. Syst.*, vol. 16, no. 3, pp. 10–15, May 2001.

[17] C. E. Rogers, A. W. Witt, A. D. Solomon, and K. K. Venkatasubramanian, "An approach for user identification for head-mounted displays," in *Proc. ACM Int. Symp. Wearable Comput. (ISWC)*, New York, NY, USA, 2015, pp. 143–146, doi: 10.1145/2802083.2808391.

[18] S. Seneviratne, Y. Hu, T. Nguyen, G. Lan, S. Khalifa, K. Thilakarathna, M. Hassan, and A. Seneviratne, "A survey of wearable devices and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2573–2620, 4th Quart., 2017.

[19] C. Xu, P. H. Pathak, and P. Mohapatra, "Finger-writing with smartwatch: A case for finger and hand gesture recognition using smartwatch," in *Proc. 16th Int. Workshop Mobile Comput. Syst. Appl.*, 2015, pp. 9–14.

[20] X. Zheng, W. Chen, P. Wang, D. Shen, S. Chen, X. Wang, Q. Zhang, and L. Yang, "Big data for social transportation," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 3, pp. 620–630, Mar. 2016.

ABDULLAH ALHARBI received the master's degree in information assurance and cybersecurity and the Ph.D. degree in computer science from the Florida Institute of Technology, Melbourne, FL, USA, and the second Master of Science degree in information technology from the Rochester Institute of Technology, Rochester, NY, USA. He is currently an Assistant Professor of computer science with King Saud University, Riyadh, Saudi Arabia. He is also a Research Fellow with the Center of Excellence for Information Assurance, King Saud University. His research interests are wearable devices security, transparent and continuous security, alternative authentication, usable security, and behavioral biometrics. He received the Information Assurance and Cybersecurity Graduate Certificate from the Florida Institute of Technology.

TALAL ALHARBI received the master's degree in network security and system administration from the Rochester Institute of Technology (RIT), Rochester, NY, USA, and the Ph.D. degree in security of software defined networks from The University of Queensland (UQ), Brisbane, QLD, Australia. He is currently an Assistant Professor and the Vice Dean for Academic Affairs with the College of Computer and Information Sciences, Majmaah University, Al Majmaah, Saudi Arabia. Prior to this, he was the Vice Dean for Systems and E-Services with the IT Deanship. His research interests include computer networks, networks security, software defined networks, cyber security, and blockchain technology. He received two advanced certificates from RIT focused on network planning and design and information assurance.