Novel user authentication method based on body composition analysis

Pawel Laka 1 · Zbigniew Korzeb 2 · Wojciech Mazurczyk 1

Received: 17 January 2020 / Accepted: 16 June 2020 / Published online: 24 July 2020
© The Author(s) 2020

Abstract
Authentication is the process of confirming one’s identity. There is a steadily growing need to protect confidential, especially financial, data, as banks provide their services online through their ubiquitous systems. This paper presents a novel authentication method based on the analysis of body composition. A trusted system that relies on the biometric authentication has been designed, implemented, and evaluated, showing a false accept rate (FAR) of 0%, while its false reject rate (FRR) is 2.65%. As the proposed solution requires virtually no special action from the user during the authentication process, it can be seen as suitable for incorporation into existing multifactor authentication solutions.

Keywords User authentication · Body analysis · Bioelectrical impedance · Biometry · Security

1 Introduction

The Payment Service Directive 2 2015/2366 (PSD2) of the European Parliament and of the Council (EU), implemented since 25 November 2015 for strong customer authentication (SCA), forces the banking sector to use system solutions necessary for proper authentication of customers and authorization of their operations [1]. Authentication is mandatory to verify the identity of a user and restrict illegitimate access the system. It is different from identification, which is a preliminary process to confirm the identity of users by requesting their credentials [2]. Under Article 97(1) of the Directive, a service provider is required to use a method consisting of at least two independent factors from the following categories: knowledge (something known only to the user, e.g., a password, a PIN code, etc.), possession (something known only to the user, e.g., a token, a microprocessor card, etc.), and customer characteristics (elements that distinguish the user from other individuals—his/her unique physiological and behavioral biometric features). Ensuring security is essential in the dynamically changing environment of banking operations. Existing counterfeiting techniques can already imitate biometric security features such as fingerprints, facial features, speech, handwritten signature or blood vessel system, the last one for a long time perceived as relatively safe [3]. Other limitations to biometry were also quickly identified [4]. Therefore, the main challenge for the banking sector is to find a rational compromise between ensuring secure authentication and authorization of customers on one hand and proposing functional, intuitive solutions on the other. The implemented changes may face initial reluctance from the customers, as this may in many cases prolong the process of logging in and accepting operations. Proposing original concepts in this area may increasingly determine the competitive advantage in the sector.

With biometrics, companies can be sure that they know not only that the login data are correct but also who entered them: biometric data such as the face or fingerprints cannot be easily shared, lost, or deleted. Furthermore, the use of biometrics based on a unique identifier makes it impossible for multiple users to share a single identifier, a practice which violates many corporate audit and security policies [5].

Verification of biometric data, taken into account in this paper, is a strategy that aligns the hereditary or behavioral characteristics of an individual with information that has
already been learned, specified in an arrangement and organized in a framework or a token database. Biometric verification can also be characterized as an idea of self-diagnosis by something you know, something you have, or something you are. Note that the biometric data can be essentially characterized as an assessment of human characteristics. Biometric identifiers are indicated as features that can be measured beyond doubt and used for naming and representing humans, suitable for use in modern authentication methods [6].

This paper proposes a novel authentication system with a new method for biometric authentication, based on new physiological biometric identifier. For this solution, we define biometric attributes listed in Section 3. They form a value vector called a biometric identifier, used in the novel authentication method. Note that for a parameter to be classified as a biometric identifier, it must have certain properties, such as [7]:

- **Universality**, defined as possession of particular characteristics by all humans (analyzed in Section 4.3).
- **Distinctiveness/Uniqueness**, describing how it varies across individuals (analyzed in Section 4.2 and evaluated in Section 4.5 using FRR; matching experimental results have been shown in Section 4.6).
- **Permanence**, demonstrating that the chosen features do not change in time (analyzed in Section 4.1 and evaluated in Section 4.4 using FRR; matching experimental results have been included in Section 4.6).
- **Collectability**, defining the ability to collect all the attributes (described in Section 3, where the proposed system is characterized).
- **Performance**, taking into account recognition accuracy, calculation time, error rates, etc. (characterized in Section 4; the results are presented in Section 4.6).
- **Acceptability**, described as ease of assimilation (analyzed in Section 4.3).
- **Circumvention**, expressing the risk of deception (analyzed in Section 4.3).

The extracted end-user features are verified by appropriate tools and fed into the system using a decision threshold strategy. To sum up, the main contributions of this paper are to:

- Design a new biometric authentication method based on body composition
- Analyze an innovative biometric identifier as part of the proposed method
- Examine the new solution using the example of the proposed identifier
- Analyze the threshold of the developed authentication system
- Compare the method with existing biometric authentication techniques

The rest of the paper is organized as follows: Section 2 describes the previous work in the area of biometric-based authentication. Then, Section 3 provides information about the proposed biometric system to prove the collectability of data therein. Next, Section 4 presents the obtained experimental results and compares the new method with existing ones. Finally, Section 5 concludes this paper and provides perspective on future work.

### 2 Related work

Many authentication systems can be compromised today if they are used as a single-factor authentication solution [8]. Nowadays, in systems responsible for storing sensitive data, a multifactor authentication (MFA) is typically the preferred choice. MFA is a secure authentication process which requires more than one authentication technique chosen from independent categories of credentials [2]. Many existing authentication methods are biometric [2], both in terms of behavior and physicality [9].

Behavioral features are those describing the personality and behavior of an individual, e.g., gait, keystroke, signature, handwriting, speech, GUI (graphical user interface) interaction, haptics, programming style, mouse dynamics, etc. [9, 10]. When it comes to physicality, physiological features are anatomical and biological properties of an individual. These are identifiers such as fingerprint, hand geometry, outer ear and facial pattern, DNA (deoxyribonucleic acid), retina, veins, voice, ECG, or iris [11, 12]. These features are widely accepted for their collectiveness, uniqueness, persistence, and cost-effectiveness to achieve verification and identification [9]. In the paper, we focused mainly on physical authentication methods. We considered the human body analysis as a new and unexplored identifier that can be used for the end-user authentication.

Few studies have been conducted considering body composition, specifically weight, in the process of confirming identity. In paper [13], biometrics of the sole and foot pressure were chosen as a method of authentication due to diversity and uniqueness of each individual. Several existing works refer to body analysis in the context of authentication. In [14], the authors present a system for authentication which scans users’ body parts, such as ears, fingers, fists, and palms, in a manner analogous to fingerprints, i.e., by pressing them against the display. In this case, 99.98% accuracy was demonstrated. Several body composition attributes, e.g., body fat, have been analyzed in medicine, for purposes such as statistics [15] or diagnosing diseases (e.g., body water, body fat, muscle mass, etc.) [16]. Nevertheless, none of these have been analyzed before as to be included in the authentication process.

Table 1 summarizes the work done so far in the field of authentication with methods related to this paper.
Nowadays, various techniques of assessing body composition parameters are known. These include densitometry, plethysmography, isotope dilution, whole-body K counting, anthropometric, bioelectrical impedance analysis, ultrasound, DEXA (dual-energy X-ray absorptiometry), CT (computerized axial tomography), and thermal imaging [17]. Bioelectrical impedance analysis (BIA), which we have used in this paper, was carried out by the body scale analyzer using the bioelectrical impedance method. Validity of BIA is also influenced by body size, gender, age, medical conditions, and ethnicity [17]. BIA is a portable, noninvasive, inexpensive, and easy-to-use method which is independent of patient cooperation [15].

Although there exist several papers analyzing the human body, currently, no works have been proposed pertaining to full-body composition analysis for authentication. There are tools and commercial solutions, like body scales, handheld monitors, or whole-body analysis equipment that allow exploring BIA. However, their functionality only allows up to 10 family members to be identified, so most probably, these devices only rely on body weight [18]. Note that the authentication method presented in this paper is able to support a much larger set of users, based on more than one body attribute.

The proposed authentication method has been developed based on more than one user’s body attributes, defined as a biometric identifier, such as

- Weight
- Body fat
- Visceral fat level
- Muscle mass
- Protein level
- Body water

The envisioned system has been presented in the next section.

### 3 Proposed trusted system

Note that each authentication system has to be insensitive by design to lighting conditions, changes, or aging. The method proposed in this paper is a novel solution which creates the biometric identifier taking into account the following user’s attributes:

- **Weight**—the total weight of the end user (in kilograms)
- **Body fat**—the percentage of body fat. This indicator represents the total body fat content (in percentage)
- **Visceral fat level**—this indicator shows the level of visceral fat in the abdominal cavity (in kilograms). It represents the fat surrounding the internal organs, which, unlike the subcutaneous fat, is not located under the skin,
- **Muscle mass**—the total size of muscles (in percentage)
- **Protein level**—the reflection of the protein contained in the body muscles (in percentage)
- **Body water**—the total water content is the total liquid content in the body (in percentage)

All the above mentioned attributes, with the exception of the weight [13], represent a novel approach to biometric authentication. The device is able to collect more parameters, such as bone mineral content. However, BIA is not currently recognized as a bone mineral measuring method [19]. The idea of this method is to use the device in a place where the user will not move. This can be a scale built into the floor, such as in this project, or a handheld device like in [20] mounted on a desk, keyboard etc. In this approach, the method is completely invisible to the user, who may not even be aware of its existence.

Figure 1 illustrates the proposed system architecture, which consists of the following components:

- **Body scale device**—Huawei AH-100 with Bluetooth 4.0 connectivity was used to collect the attributes. While widely available medical scale technology is not as accurate as high-end instruments, its ability to record readings allows us to see changes over time, which in itself is a very reliable metric. Huawei scale has been chosen due to its built-in Bluetooth connectivity, heat-resistant tempered glass casing, compatibility with Android and iOS systems, and the load capacity up to 150 kg. The scale works in such a way that when someone steps on the scale, a small electric current flows through the individual’s leg and

| Table 1 Summary of the related authentication methods |
|-------------------------------------------------------|
| **Related authentication** | **Proposed method** |
| Behavioral | Gait, keystroke, signature, handwriting, speech, GUI (graphical user interface) interaction, haptics, programming style, mouse dynamics |
| Physicality | Fingerprint, hand geometry, outer ear and facial pattern, DNA (deoxyribonucleic acid), retina, veins, voice, ECG or iris |
| Physicality–body analysis | Sole and foot pressure analysis, scans body parts scanning |
pelvis, measuring the resistance of a tissue, such as fat. Then, the scale sensors measure the level of resistance that the current has encountered returning through the other leg. The chosen scale is fitted with a high precision BIA chip, 4 pressure sensors, and 360° adjustable scale feet to achieve accurate and convenient measurement [21].

- The integrated application—it communicates with the device and retrieves all necessary attributes; the Huawei Body Fat Scale application made by Huawei is used to manage the body scale. The application connects to the scale and provides the measurement figures. The application was installed on a Samsung Galaxy A3 2016 SM-A310F mobile device with version v4.1 LE built-in Bluetooth sensor.
- The database—all the data for profile vectors and from surveys provided by the application have been stored in Google Cloud.
- The authentication system—decides whether the user has been correctly recognized based on the application data. The decision system was written using the formulas of VBA (Visual Basic for Applications), the programming language of Excel and other Microsoft Office programs.

This design enables the system to collect all the information needed to authenticate the end user. The proposed architecture has the smallest number of components required for the safe and efficient operation of such a system. The listed components communicate one with another to confirm the identity of the end user. The diagram of resulting sequences is shown in Fig. 2.

In Fig. 2, the proposed authentication process can be observed. It consists of the following steps:

1. The user to be weighted has to stand on the body scale.
2. The body scale takes measurements.
3. The scale is integrated with the Huawei module installed on a mobile device with an additional built-in Bluetooth sensor. The collected data are sent via Bluetooth.
4. The gathered data are first sent to the integrated application and then to the authentication system.
5. The body composition value of the individual being measured is compared to the reference value (related to the created profile). This way, the system decides whether the user really is who he/she claims to be. After comparing the current end-user vector with the profile vector, the authentication process is completed.
6. The data are simultaneously sent to the database.

The data were collected as vectors in the Google cloud for additional studies. Example data are presented in Table 2.

As seen in Table 2, the resulting measurements form a vector of values of successive body attributes. The method consists in studying the end user, whose vector is compared with the value defined for the given user (profile reference values). When the user is authenticated, the current vector is compared with the previous one. This has been implemented using a normalized squared Euclidean distance. The normalized squared Euclidean distance has been chosen due to its low complexity and simplicity in implementation. The normalized Euclidean distance \(d_{ne}(A, B)\) between vectors \(A\) and \(B\) in \(X = \{x_1, x_2, \ldots, x_n\}\) can be calculated using the formula [22]:

\[
d_{ne}(A, B) = \frac{1}{n} \left( \sum_{i=1}^{n} |\mu_A(x_i) - \mu_B(x_i)|^2 \right)^{1/2}
\]

In Google sheets, it has been implemented as \(\text{=SQRT(SUMXMY2(A1:B1,X2:Y2))}\) where in row 1 and columns A to B, there were values of particular attributes of the first vector, while in row 2 and columns X to Y, there were values of particular attributes of the second vector to compare. The result of such formula, whether or not the evaluated user is who he/she claims to be, is then verified within the authentication system. If the result of the algorithm is under the predefined threshold, the user is authenticated. It implies that the vector being measured is very similar to the profile one.

Taking into account the example data from Table 2, it is possible to define a profile vector from which the individual
Euclidean distance values can be calculated. The Euclidean distance examples are presented in Table 3.

The profile vector has been defined in row 2, while results from the two consecutive measurements have been recorded in rows 4 and 5. Column I contains the calculated Euclidean distances. The formula in I4 is \(\text{SQRT}(\text{SUMXMY2}(C2:H2,C4:H4))\), while in I5, it is \(\text{SQRT}(\text{SUMXMY2}(C2:H2,C5:H5))\).

### 4 Experimental methodology and results

This section describes the methodology of the experimental evaluation performed within the proposed authentication method. Different performance metrics are typically used to evaluate the efficacy of biometric systems, such as false accept rate (FAR, a.k.a. false match rate), false reject rate (FRR, a.k.a. false non-match Rate), relative operating characteristic (ROC) and crossover error rate (CER), and failure to enroll rate (FER) [23].

The following parameters are used in this paper as a measure of the biometric systems efficiency:

- **FAR**—the ratio of the number of attack cases incorrectly marked as authentic to the total number of attack instances. The FAR value must be as low as possible.

  \[
  \text{FAR} (\mu) = \frac{\text{Number of successful false attempts made in authenticating users}}{\text{Total number of attempts made in authenticating users}}
  \]

  where \(\mu\) is the security level [2].

- **FRR**—the ratio of the number of authentic interactions that have been incorrectly classified as attacks and the total number of authentic, significant instances. It measures the percentage of authentic interactions that are incorrectly classified as intrusive.

  \[
  \text{FRR} (\mu) = \frac{\text{Number of false rejects made in authenticating genuine users}}{\text{Total number of attempts made in authenticating users}}
  \]

  where \(\mu\) is the security level [2].

- **ROC**—the curve drawn between the false accept rate vs. the false reject rate. The shape of the curve depends on the

### Table 2  Example measurements of the body composition in the experiment

| What | Who | When | Weight (kg) | Body Fat (%) | Visceral fat level | Muscle mass (kg) | Protein (%) | Body water (%) |
|------|-----|------|-------------|--------------|-------------------|-----------------|------------|----------------|
| 1st data for user 1 | User | 2019 May 07 22:21 | 73 | 14.8 | 5 | 58.6 | 23.7 | 56.5 |
| 2nd data for user 1 | User | 2019 May 08 8:49 | 71.9 | 13.9 | 4.5 | 58.3 | 24.2 | 56.9 |
threshold value set for acceptance of the authentication event.

- **CER**—the rate at which both the false accept rate and false reject rate errors are equal.

### 4.1 Permanence analysis

The persistence of the biometric identifier was measured by daily testing of one participant from 7 May 2019 to 19 July 2019. Note that the initial measurement for the profile vector was performed on 19 March 2019. The end user is a male aged 28. The study was conducted under different conditions, including work time, weekends, occasional short trips, and climate changes, especially temperatures. During the study, throughout the changing seasons of the year, the air temperature varied by 30 °C, which could affect the metabolism of the participant. The study and experiments did not affect daily routines of the participant, including commuting, work, vacation, etc.

First of all, a reference measurement was performed and a profile was created. After 2 months, daily measurements started, comparing the ongoing daily values with the profile value.

The measurement results were compared with the previously defined values to obtain the appropriate data for the authentication system to make decisions. We considered three alternative variants to determine the Euclidean distance:

- **Variant 1**: where the vector parameters are compared with the initially measured ones. First of all, a reference measurement was performed on 19 March 2019 and a profile vector was established. During the experimental evaluation, daily measurements were performed and compared with the profile value.

- **Variant 2**: where the parameters of the biometric vector are compared with the previously measured ones. The current vector is no longer compared to the initial profile vector but to the last one which has been considered correct. Each new measurement that the system finds to be correct overwrites the last profile vector and sets a more up-to-date profile for the next comparison. Each daily measurement is compared with the last measured vector.

- **Variant 3**: where the vector parameters are compared with the averaged values from three consecutive previous measurements. Thus, with each new measurement, a new vector with an average value is created and compared with the current vector.

Several thresholds have been also evaluated for which the system should agree on a correct authentication. The obtained FAR values were tested for different threshold values. The results are shown in Section 4.6.

### 4.2 Uniqueness analysis

Another study has been performed to evaluate the uniqueness of the proposed biometric identifier. In this experiment, 27 end users differing by gender, age, and physique were studied: 15 men and 12 women aged 23 to 55 years took part in the survey. Each respondent had to stand on a scale that passed the results to the database. The measurement values of each user were compared with the measurements of any other user. By defining the threshold value for which the system should agree to authenticate correctly, the FAR value was obtained. Similarly to the last subsection of the FRR, the FAR was also tested for different threshold values. Additionally, ROC has been drawn and CER has been calculated. All the relevant results have been presented in Section 4.6.

### 4.3 Parameter analysis

The proposed novel biometric identifier has been investigated for suitability to become a new authentication method.

- **Universality**—the human body obviously consists of muscles, water, fat, and bones

- **Acceptability**—considering the short time needed to perform a measurement for a single user, the method is comfortable. Note that the user is not required to perform any additional authentication processes/actions.

| A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|
| 1 | Who | When | Weight [kg] | Body fat [%] | Visceral fat level | Muscle mass [kg] | Protein [%] | Body water [%] | Euclidean distance |
| 2 | Profile vector | 19 Mar | 74.4 | 15.3 | 5.0 | 59.5 | 23.5 | 56.5 |  |
| 3 | Who | When | Weight [kg] | Body fat [%] | Visceral fat level | Muscle mass [kg] | Protein [%] | Body water [%] | Euclidean distance |
| 4 | 1 user vector | 7 May | 73.0 | 14.8 | 5.0 | 58.6 | 23.7 | 56.5 | 1.75 |
| 5 | 2 user vector | 8 May | 71.9 | 13.9 | 4.5 | 58.3 | 24.2 | 56.9 | 3.25 |
Circumvention—using an object with different impedances at the sensors but whose composition similar to that of the human body is very unlikely. The potential attacker would have to use a decoy characterized by impedances of bone, water, fat, etc. at the same time. The object would also have to have the mass of a person whom the attacker would like to impersonate. Therefore, the proposed solution makes it very challenging to impersonate a human: this would require putting on the scale something of a similar weight that contains substances of impedance resembling muscles or water.

4.3.1 Permanence results

The main objective of this subsection is to verify the new method in terms of persistence, using the proposed biometric identifier. The vector constructed from the values of successive body attributes and defined in Section 3 has been investigated. The current biometric vector is compared to the initial reference profile vector, which has been described in Section 4.1 as a Euclidean distance (calculated using Variant 1). The results of the algorithm operation for this variant are presented in Fig. 3.

As it is seen in Fig. 3, the values are in the range from 0 to 5. It is visible that the body composition does not change much over time. The Euclidean distance did not start to increase as the measurements continued from the date of the profile vector. It can be observed that it still oscillates around 2 and 3.

However, in order to improve this result, the operation of the decision-making system has been changed. The static profile vector calculation has been changed to a...
dynamic one, which has been described in Section 4.1 (Variant 2). After changing the algorithm of the decision-making system, the results of the currently tested vector were compared to the last correct one. The results obtained are presented in Fig. 4.

The dynamic profile is shown in Fig. 4 to yield better results. Although the data vary in time, the values are distributed in a smaller range, from 0 to 3.

Finally, the third variant, described in Section 4.1, was also evaluated, and the results obtained are illustrated in Fig. 5. In this case, the current vector is compared with the average values of attributes. This scenario provides visibly better results than Variant 1. This may mean that the human body changes slightly over time.

Based on the results presented in this subsection, FRR values have been calculated for each considered variant. The obtained results are presented in Section 4.6.

### 4.4 Uniqueness results

In this subsection, we present results proving that the biometric identifier used in the proposed authentication method can be successfully used to provide uniqueness. All the users participating in the experimental evaluation and their similarities to one another are shown in Fig. 6. The results of the applied algorithm, described in Section 3, are presented in Table 5.

Conditional formatting has been added to the results for the sake of clarity and highlighting the differences. The lowest Euclidean distance values represent the closest matches, while the highest Euclidean values, reflecting the most distant vectors, are marked gradually from green to red. According to the scale used, values above 20 have been colored red and those below 5 are green. The intermediate values have been colored yellow.

| Table 4 | Uniqueness results for all users participating in the experimental evaluation, and similarities among the users numbered as shaded cells |
|---------|--------------------------------------------------------------------------------------------------|
| User    | Weight (kg) | Body fat (%) | Visceral fat level | Muscle mass (kg) | Protein level (%) | Body water (%) | Euclidean distance |
| 1       | 74.4        | 15.3         | 5.0                | 59.5             | 23.5             | 56.5           | –                  |
| user    | 74.9        | 19.7         | 11.5               | 56.5             | 20.0             | 55.3           | 9.20               |
| other   | 74.9        | 19.7         | 11.5               | 56.5             | 20.0             | 55.3           | 9.20               |
| 2       | 64.7        | 27.8         | 5.0                | 43.4             | 17.0             | 50.2           | –                  |
| user    | 64.7        | 32.9         | 5.0                | 39.6             | 13.9             | 47.4           | 7.61               |
| other   | 64.7        | 32.9         | 5.0                | 39.6             | 13.9             | 47.4           | 7.61               |
Based on the presented results, a gender-specific similarity relationship was observed in line with expectations [24]. Therefore, the table was divided by gender. When comparing users with numbers 1–12 and 13–27, the resultant Euclidean distance values are visibly high. This is because users 1–12 are females and 13–27 are males.

Additionally, it is worth noting the presence of green fields in Table 4, which means that the system would incorrectly identify different people as the same person. However, there have been users (e.g., no. 15) who are significantly different from all other users, i.e., they have a completely different body composition, so the system would not have a problem recognizing him/her. However, no case was identified as similar to many others and the green fields are generally in the minority.

It would seem that the weight alone is not a value granular enough to achieve full uniqueness. But as the results have shown, by taking more extensive attributes into account, e.g., the six attributes used in this study, one can observe distinctness.

In conclusion, it can be inferred that equal weight attribute does not by any means ensure the same decision of the authentication decision system. Below, we present 3 cases for users with a very similar weight. Although the values are very close to each other, the rest of the parameters allow the system to ensure full distinctiveness. Table 5 presents our distinct users, two of whom have almost the same weight.

As the first two lines of Table 5 demonstrate, despite the weight of these individuals being virtually the same, the system will properly recognize them as different people, taking into account all their attributes. In addition, a comparison of the same user on different days is shown in Table 6: even though the user’s weight was slightly different, he/she was correctly recognized by the system.

The results obtained visibly confirm the hypothesis that the proposed identifier, constructed from six independent attributes, is sufficient to achieve uniqueness. It has also been confirmed that it is possible to use such a biometric identifier as an input to the authentication method. Tables 5 and 6 show that the authentication system with a low threshold value would have no problem distinguishing end users. The threshold value analysis is presented in Section 4.6.

### 4.5 Performance results

In this subsection, different results by threshold selection have been presented. In relation to [23], if the threshold value is too small, the FAR will be low, but the FRR will be high. On the other hand, if the chosen threshold value is too high, then the FAR will be high, but the FRR will be low.

The experimental evaluation of FAR and FRR was performed in relation to the threshold/fresh grain in the range from 1.5 to 4. The threshold selected in this way shows the difference in FRR from 80 to 0% and increasing FAR values from 0.5% to almost 6%. Three Euclidean distance calculation variants as described in Section 4.1 have been included, and the obtained results are presented in Fig. 6.

As it can be seen, the change in the threshold value shows a decrease in the FRR as well as an increase in the FAR. The first variant for determining the Euclidean distance provided the worst results, which means that the composition of the body structure changes slightly over time. Note, however, that the results for variants 2 and 3 are not substantially different. Comparison of the current vector with the previous one (variant 2) initially yields a higher FRR but drops faster to 0 than comparison with averages (variant 3). The CER is the point at which it is optimally calculated. It has been found for variant

| Method based on biometric identifier | Universality | Distinctiveness | Permanence | Collectability | Performance | Acceptability | Circumvention |
|-------------------------------------|--------------|-----------------|------------|----------------|-------------|---------------|---------------|
| Face [2]                            | High         | High            | Medium     | High           | Low         | High          | Low           |
| Finger print [2]                    | Medium       | High            | High       | High           | Medium      | Medium        | Medium        |
| Hand geometry [2]                   | Medium       | Medium          | Medium     | Medium         | Medium      | Medium        | Medium        |
| Iris [2]                            | High         | High            | High       | Medium         | High        | Low           | High          |
| Signature [2]                       | Low          | Low             | Low        | Low            | High        | High          | Low           |
| Voice [2]                           | Medium       | Low             | Low        | Medium         | Low         | High          | Low           |
| Proposed method: body composition   | High         | Low             | Low        | Medium         | Medium      | Medium        | High          |

---

**Table 6**  Body composition for the same user with not exactly the same weight

| Who        | Weight (kg) | Body fat (%) | Visceral fat level | Muscle mass (kg) | Protein level (%) | Body water (%) | Euclidean distance |
|------------|-------------|--------------|--------------------|------------------|-------------------|----------------|--------------------|
| User 3     | 73.3        | 14.6         | 4.5                | 59.1             | 23.9              | 56.8           | –                  |
| The same user 3 | 72.8      | 14.2         | 4.5                | 59.0             | 24                | 56.9           | 0.66               |

---

**Table 7**  Biometric methods comparison

| Method based on biometric identifier | Universality | Distinctiveness | Permanence | Collectability | Performance | Acceptability | Circumvention |
|-------------------------------------|--------------|-----------------|------------|----------------|-------------|---------------|---------------|
| Face [2]                            | High         | High            | Medium     | High           | Low         | High          | Low           |
| Finger print [2]                    | Medium       | High            | High       | High           | Medium      | Medium        | Medium        |
| Hand geometry [2]                   | Medium       | Medium          | Medium     | Medium         | Medium      | Medium        | Medium        |
| Iris [2]                            | High         | High            | High       | Medium         | High        | Low           | High          |
| Signature [2]                       | Low          | Low             | Low        | Low            | High        | High          | Low           |
| Voice [2]                           | Medium       | Low             | Low        | Medium         | Low         | High          | Low           |
| Proposed method: body composition   | High         | Low             | Low        | Medium         | Medium      | Medium        | High          |
2. For the threshold equal to 2.9, the resulting FRR is 0% and FAR is 2.65%.

### 4.6 Comparison with existing biometric methods

In Section 1, the definitions of parameters (universality, distinctiveness, permanence, collectability, performance, acceptability, circumvention) have been explained, while in this subsection, all parameters are analyzed and compared with other existing biometric authentication methods. In Section 4, they have been analyzed in the context of the proposed solution. However, in this subsection, we try to compare the new method with other known techniques. Taking into account the abovementioned parameters, an attempt was made to assess each of them in a three-stage scale (high, medium, low). The values adopted, based on the research and analyses presented in this paper for the introduced authentication method, are as follows:

- Universality—everyone has a body to measure—high
- Distinctiveness/uniqueness—at age 25 participants show occasional similarities—low
- Permanence—the results presented in this paper show that the method is suitable for use, but the values vary over time—low
- Collectability—it is easy to collect the required data but the end user has to stop for a while to have a measurement taken—medium
- Performance—FRR level remains low—medium
- Acceptability—the end user has to stop for a while to have a measurement taken but no additional authentication activities appear necessary—high
- Circumvention—as described in Section 4.3, it is very challenging to compromise the system using this method—high

Based on the results incorporated in [2] showing a comparison of several biometric methods (face, finger print, hand geometry, iris, signature, voice), the current method was added, and the results are presented in Table 7.

The new method is visibly competitive, performing not worse than the other state-of-the-art solutions. It should be admitted, however, that the scheme is weaker when it comes to distinctiveness and permanence. This could be improved by using more accurate measuring devices or adding more body composition values. At the same time, the proposed method could surpass other approaches when it comes to universality and circumvention. It is very common and each one of us has different values that are very hard to deceive. Building high-quality equipment into the infrastructure would increase the value of collectivity and acceptability, becoming invisible to the user.

In addition, the proposed method: the body composition has been compared with other methods described in [13] with regard to FAR and FRR. Table 8 shows FAR and FRR values for the methods mentioned in Section 2.

It must be noted that compared to the existing solutions, the results of the proposed method are promising. Apart from ear shape and ECG, it performs better than the rest of the methods in terms of FAR and FRR. At the same time, the proposed method is much more user-friendly than ECG or ear shape testing.

### 5 Conclusions and future work

This paper introduced a novel method for authentication based on biometrics. We have developed a trusted system that collects information about the users and verifies their identity. The method was analyzed on the basis of well-known criteria such as universality, distinctiveness, permanence, collectability, performance, acceptability, and circumvention. It has been proven that the new method meets all the criteria just as successfully as other biometric methods. Body composition turns out to be a promising biometric identifier with all its desirable properties. FAR and FRR results were obtained at the FRR = 0.00% and FAR = 2.65%.

In addition, it should be mentioned that this method can be used with virtually no action from the end user. It can certainly improve the current recognition systems in an economical way, as well as provide improved security and privacy. The new proposed method can be used as an additional factor of user authentication. The proposed solutions can be applied broadly by commercial banks to improve the stability and security of the banking sector and to protect the interests of participants of the financial market. It can also be added as an extra authentication method in public institutions or in the insurance sector.

In the future, the method can be improved by using other, new BIA-measuring devices so that it can confirm identity in office work in an unnoticeable manner. The method can be completed with more attributes, which should further improve its uniqueness.
Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. European Commission. (2015). Payment services (PSD 2) - Directive (EU) 2015/2366. https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en. Accessed 23 April 2020

2. Dasgupta D, Arunava R, Nag A (2017) Advances in user authentication. Springer International Publishing Ag, Cham. https://doi.org/10.1007/978-3-319-58808-7

3. Tassabehj, R., & Kamala, M.A. (2012). Evaluating biometrics for online banking: the case of usability. *International Journal of Information Management*. https://doi.org/10.1016/j.ijinfomgt.2012.07.001

4. Lumin A, Nanni L (2017) Overview of the combination of biometric matchers. *Information Fusion* 33:71–85. https://doi.org/10.1016/j.inffus.2016.05.003

5. Gioeli A (2015) Biometrics and the future of enterprise ID management. *Biometric Technology Today* 2015:8–10. https://doi.org/10.1016/S0969-4765(15)30037-0

6. Gemalto. (2019). Biometrics: authentication & identification (definition, trends, use cases, laws and latest news) - 2020 review. https://www.gemalto.com/govt/inspired/biometrics Accessed 23 April 2020

7. Oak, R. (2018). A literature survey on authentication using Behavioural biometric techniques. *Intelligent Computing and Information and Communication* pp.173–181. Singapore: Springer

8. Mishbahuddin M, Bindhumadhava BS, Dheeptha B (2017) Design of a risk based authentication system using machine learning techniques, 2017 IEEE SmartWorld, pp.1-6

9. Dargan S, Kumar M (2020) A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert Syst Appl* 143:113114. https://doi.org/10.1016/j.eswa.2019.113114

10. Riera A, Soria-Frisch A, Caparrini M, Cester I, Ruffini G (2010) Multimodal physiological biometrics authentication. Theory, Methods, and Applications, *Biometrics*. https://doi.org/10.1002/9780470522336.ch18

11. Ramadán G, Mohamed T, El-Latif A, Zorkany M, El-Sayed A, El-Fishawy N, Ghulam M (2018) Iris recognition using multi-algorithmic approaches for cognitive Internet of things (CIoT). *Futur Gener Comput Syst* 89:178–191. https://doi.org/10.1016/j.future.2018.06.020

12. Wang N, Li Q, El-Latif A, Peng J, Xuejuan N (2013) Multibiometrics fusion for identity identification: dual iris, visible and thermal face imagery. *International Journal of Security and its Applications* 7:33–44

13. Yeh K, Su C, Chiu W, Zhou L (2018) I walk, therefore i am: continuous user authentication with plantar biometrics. *IEEE Communications Magazine*. 56:150–157. https://doi.org/10.1109/MCOM.2018.1700339

14. Holz C, Barthipitaya S, Knaust M (2015) Bodyprint: biometric user identification on mobile devices using the capacitive touchscreen to scan body parts *CHI ’15 Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. doi: https://doi.org/10.1145/2702123.2702518

15. Schmidt S, Bosy-Westphal A, Niessnera C, Wolla A (2019) Representative body composition percentiles from bioelectrical impedance analyses among children and adolescents. The MoMo study. *Clinical Nutrition*. https://doi.org/10.1016/j.clnu.2018.11.026

16. Junga GH, Kimb JH, Chunge MS (2020) Changes in weight, body composition, and physical activity among patients with breast cancer under adjuvant chemotherapy. *Eur J Oncol Nurs* 44:101680. https://doi.org/10.1016/j.ejon.2019.10.1680

17. Rashmi R, Snekhala U (2019) Evaluation of body composition parameters using various diagnostic methods: a meta analysis study. *Obesity Medicine* 16:100150. https://doi.org/10.1016/j.obmed.2019.100150

18. The newspaper. (2020) 10 of the best bathroom scales, including smart scales and body fat monitors. https://www.telegraph.co.uk/health-fitness/body/best-bathroom-scales/. Accessed 23 April 2020

19. WenLee L, SanLiao Y, KuanLu H, ChangHsieh K, ChiChi C (2012) Performance of bioelectrical impedance analysis in the estimation of bone mineral content in healthy children aged 6–12 years. *J Clin Densitom*. https://doi.org/10.1016/j.jcld.2019.03.002

20. Omron Healthcare. (2020). Body fat monitor HBF-306. https://www.omronhealthcare-ap.com/ap/product/68-hbf-306/1. Accessed 23 April 2020

21. HUAWEI (2020). HUAWEI smart scale. https://consumerhuaweicom/en/accessories/smartscale/. Accessed 23 April 2020

22. Xu Z, Xia M (2018) Distance and similarity measures for hesitant fuzzy sets *Information Sciences*. https://doi.org/10.1016/j.ins.2011.02.028

23. Meghana N (2018) Biometric systems for user authentication. *Computer and Network Security Essentials*. Springer, Cham

24. Ashby N, Gallagher B (2018) Body composition. In *Eating disorders and obesity, third edition: a comprehensive handbook* (pp. 57–62). London: The Guilford Press

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.