Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

ActID: An efficient framework for activity sensor based user identification

*Sai Ram Vallam Sudhakar, Namrata Kayastha, Kewei Sha**

Department of Computing Sciences, University of Houston-Clear Lake, Houston TX 77058, USA

ARTICLE INFO

Article history:
Received 19 February 2021
Revised 28 April 2021
Accepted 3 May 2021
Available online 19 May 2021

Keywords:
Wearables
Sensors
Biometric
Identification
Classification

ABSTRACT

Identification is the core of any authentication protocol design as the purpose of the authentication is to verify the user's identity. The efficient establishment and verification of identity remain a big challenge. Recently, biometrics-based identification algorithms gained popularity as a means of identifying individuals using their unique biological characteristics. In this paper, we propose a novel and efficient identification framework, ActID, which can identify a user based on his/her hand motion while walking. ActID not only selects a set of high-quality features based on Optimal Feature Evaluation and Selection and Correlation-based Feature Selection algorithms but also includes a novel sliding window based voting classifier. Therefore, it achieves several important design goals for gait authentication based on resource-constrained devices, including lightweight and real-time classification, high identification accuracy, a minimum number of sensors, and a minimum amount of data collected. Performance evaluation shows that ActID is cost-effective and easily deployable, satisfies real-time requirements, and achieves a high identification accuracy of 100%.

1. Introduction

User authentication is an effective mechanism to protect malicious access to sensitive resources. Identification is a crucial component in the authentication protocol design as the purpose of the authentication is to verify the identity of the user (Ailisto et al., 2005; Gafurov et al., 2006; Mantyjarvi et al., 2005; Nickel et al., 2012). Over the past few decades, several types of identification technologies have been developed that can uniquely identify users and prevent impersonation. These identification solutions aim to provide a practical and cost-effective approach to easily identify the user as well as offer a smooth user experience, but challenges remain. Username/password-based identity is widely adopted in the digital world (Lin and Hwang, 2003), yet they are susceptible to hacking, theft, and fraud. A digital signature based on cryptographic algorithms is another popular approach for building a verifiable identity (Merkle, 1988). It is an effective solution, but it requires a powerful processor to generate digital signatures; therefore, resource-constrained devices have difficulty in creating such an identity. Recently, a hardware-based solution, Physical Unclonable Function (PUF) (Suh and Devadas, 2007), has evolved to identify users, and many authentication protocols are built based on it. PUF provides a strong identity solution but it requires extra hardware support. Similarly, tokens and access cards (Tan et al., 2001) provide a hardware-based solution for identity.

Biometrics-based identity solutions are the next frontier of identification and verification (Alizadeh et al., 2016). They are considered more effective than the aforementioned digital identities because of the following reasons. First, biometrics are a natural part of the user. Unlike other traditional means of identity verification such as usernames/passwords, PINs, tokens, etc., biometrics cannot be forgotten, lost, or

* Corresponding author.
E-mail addresses: vallamsudhaks0325@uhcl.edu (S.R.V. Sudhakar), kayasthan3411@uhcl.edu (N. Kayastha), sha@uhcl.edu (K. Sha).
https://doi.org/10.1016/j.cose.2021.102319

stolen (Derawi et al., 2010). Second, biometrics are unique for everyone, therefore they are hard to be forged. Third, the biometrics-based identities are easily verifiable by measuring the biometric characteristics (Sha and Kumari, 2018).

Many biometrics-based identities have been developed and applied in modern computing systems. For example, iPhone X and later versions, and Microsoft Surface Pro use facial recognition techniques to identify legitimate users app (2017); mic (2017). The fingerprint is the most widely adopted biometrics-based identity used in smartphones and PCs (Ohana et al., 2013). ECG/EEG patterns (Chatra, 2014; Dey et al., 2014), Iris patterns (Wildes, 1997), and palm vein patterns (Zhang and Hu, 2010) are other popular biometrics-based identities. All these solutions require special hardware to measure the biometrics. This can be expensive, inconvenient as well as very intrusive to the user's experience. The recent solutions of behavioral biometrics are inexpensive, more appropriate than conventional biometrics and/or they can be used in combination with traditional biometrics such as multi-factor authentication to improve security and usability (Gafurov and Snekkenes, 2009). However, some biometrics-based authentication systems necessitate user interaction, which is inconvenient for the user. Typing the password, lifting the phone for face id, and pressing the fingerprint sensor are just a few examples. This would be much more difficult for the user during continuous authentication, as the user must authenticate several times (Crawford et al., 2013; Saevanee et al., 2015; Syed Idrus et al., 2014). This problem can be solved by activity sensor based identity solutions such as wearable sensor based gait recognition (Kumar et al., 2016), touch gestures based recognition (Mondal and Bours, 2015), keystroke based recognition, etc., since the biometric patterns are captured implicitly while the user interacts with the device (Abuhamad et al., 2021). These approaches address the privacy (Chen et al., 2012) and power consumption (Gafurov and Snekkenes, 2009) issues better than traditional vision based activity recognition.

Based on the data collected by activity sensors, such as accelerometers and gyroscopes, researchers have analyzed the activity patterns of humans and have found unique traits that can be used as the identity. In literature, activity sensors have been used in identifying users based on their keystroke dynamics (Lee et al., 2018), hand movements (Casanova et al., 2012; Garcia et al., 2016), and gait patterns (Ailisto et al., 2005; Al Kork et al., 2017; Blasco et al., 2016; Chen, 2014; Damaševičius et al., 2016a; Damaševičius et al., 2016b; Derawi et al., 2010; Gafurov et al., 2006; Guan et al., 2011; Johnston and Weiss, 2015; Kwapisz et al., 2010; Liu et al., 2017; Mantyjarvi et al., 2005; Marsico and Mecca, 2019; Nickel et al., 2012; Primo et al., 2014; Rong et al., 2007; Su et al., 2014; Sugimori et al., 2011; Sun and Yuao, 2012; Thang et al., 2012; Xu et al., 2016; Yang et al., 2016). These existing approaches produce promising results, but most of them either use several sensors deployed around the body, which is not practical in real-life scenarios or employ computation-heavy algorithms based on a large number of features. The limitations of these approaches in the real-world applications include willingness to use wearable sensors, ability to wear them, success rate, scalability, ease of use, battery life, and the approach's usefulness (Chen et al., 2012).

As smartwatches and wristbands become pervasively available, many sensors, such as accelerometers and gyroscopes embedded on these devices can be used as measuring devices for biometrics. Therefore, we can design solutions that construct and verify digital identity for users by using these sensors to measure biometrics in a cost-effective and convenient way. In addition, this approach is not expensive and can be used in continuous authentication since it does not require any user interaction with the device.

In this paper, we propose ActID, an efficient framework for activity sensor based user identification, to efficiently identify users based on sensors deployed at the wrist. The main goal of our classification algorithm design is to overcome challenges resulting from the authentication application requirements and resource-constrained devices used in the application. We aim to design an efficient framework that identifies users with high accuracy in real-time, based on a minimal number of sensors, a minimal amount of data, as well as using only lightweight classification algorithms. The novelty of our proposed method is four-fold. First, we employ the Optimal Feature Evaluation and Selection method (OFES) (Kayastha, 2019; Kayastha and Sha, 2019; Sai Ram et al., 2020) and Correlation-based Feature Subset Selection (CFSS) (Hall, 1999) algorithms to evaluate the extracted features and select a set of high-quality features that can distinctly identify individuals. Therefore, we can keep the size of the feature set as small as possible. It also reduces the algorithm complexity. Second, we define a novel classification algorithm, Sliding Window based Voting classifier for gait authentication which reuses the data to reduce the amount of data and adapts voting to improve the identification accuracy. Third, we provide a smooth user experience with our proposed framework. Unlike other research methods, where the users must wear multiple sensors on different parts of the body, our experiment only requires the users to wear one wrist sensor and walk normally as they do on a plain surface for less than a minute to train the classifier. Fourth, we reduce the number of sensors by using only an accelerometer sensor and improve the cost efficiency of user classification based on activity sensor data. The performance evaluation based on a simple prototype with a multi-class classifier shows that the proposed framework can achieve high accuracy of 100% when applied to a 30 user dataset, which is better than the similar approaches including the efforts presented in (Al Kork et al., 2017; Damaševičius et al., 2016a; Gafurov et al., 2006; Johnston and Weiss, 2015; Kumar et al., 2016; Kwapisz et al., 2010; Liu et al., 2017; Nickel et al., 2012; Yang et al., 2016).

The contribution of the paper is three-fold. First, we analyzed challenges in the activity sensor based user identification. Second, we proposed a novel classification algorithm that features sliding window technique and voting method. Third, we built a prototype for activity sensor based user identification and carried out an extensive performance evaluation.

The rest of the paper is organized as follows. Section 2 discusses the motivation behind this study. Section 3 details the design of the ActID framework. Section 4 presents the performance evaluation based on a simple prototype implementation. Section 5 lists a set of related work. Finally, we conclude the paper and discuss future work in Section 6.

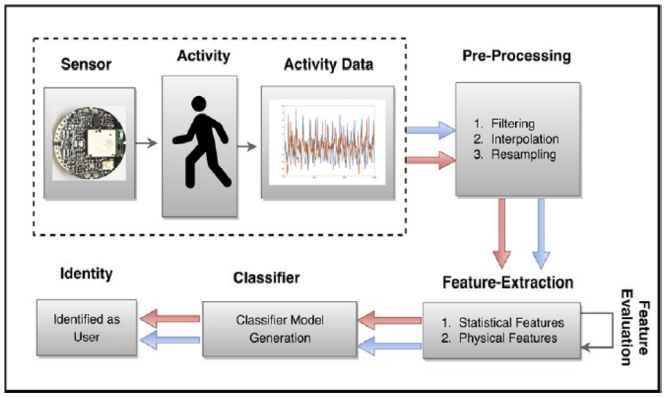

Fig. 1 – The ActID Framework.

2. Motivation

One of the common problems of authentication is its intrusive way of authenticating users. It could be typing the password, raising the phone for face id, touching the fingerprint sensor, giving the voice to identify the user. These kinds of authentications require user interaction every time the user attempts authentication, which leads to lots of inconvenience to the user. Syed Zulkarnain et al. studied on finding the profile of an individual like age, gender etc., based on their behavioral characteristics of keystroke dynamics (Syed Idrus et al., 2014). It would be interesting to see if the same can be achieved with activity sensor data. Heather Crawford et al. proposed a framework that integrates multiple behavioral biometrics to implement an effortless and continuous authentication mechanism without user interaction (Crawford et al., 2013). Similarly, Saevanee et al. proposed a novel text-based multimodal biometric approach using linguistic analysis, keystroke dynamics and behavioral profiling so that the number of intrusive authentication requests required for high security applications will be decreased (Saevanee et al., 2015). All these approaches are trying to achieve authentication without any intrusion to the user. We believe activity sensor based user identification is less intrusive because it does not require much user interaction with the device thus to make authentication easier.

Activity sensor based biometrics has been a hot research topic in the last several years. The pervasive availability of activity sensors, such as accelerators and gyroscopes, lead to many novel designs and innovations that aim to construct user identity based on the activity sensor data. Previous designs have used different activities such as walking, running, jumping, and arm gestures for identities (Abate et al., 2017; Gupta et al., 2013; Nickel et al., 2012). However, we have not yet seen large-scale deployments of these technologies because of the following concerns. First, we have observed the deployment of sensors on different body parts, including waist (Ailisto et al., 2005; Mantyjarvi et al., 2005), leg (Gafurov et al., 2006), sternum (Vural et al., 2013), wrist (Kumar et al., 2016), and on multiple body locations at the same time (Al Kork et al., 2017). Many of them are not practical in real-life scenarios. Considering the rising popularity of smartwatches (e.g., Apple Watch) and activity bands (e.g., Fitbit), we believe it is more practical to make use of activity data collected with the help of the activity sensors installed on these devices to construct identity. In this way, we do not need to add any extra sensors to the human body. Also, we need to reduce the number of sensors so that the design will be cost-effective. Second, the big size of the feature set increases the complexity of the identification algorithm. We need to keep the feature set size as small as possible. On the other hand, we do not want to miss important features that work well to produce the uniqueness of identity. It is a challenge to identify a user accurately based on a small set of high-quality features. Third, there is still space to improve the accuracy of existing activity sensor based identification algorithms. Fourth, several user identification applications have real-time requirements, yet many embedded devices such as smart lockers and smart wristbands are heavily resource-constrained, including a slow processor and a small-size memory. Therefore, the user identification algorithms need to be lightweight so that it can be easily executed on various smart devices. Finally, to provide a smooth user experience and to satisfy real-time requirements, the identification should be completed in a very short period, like less than a minute. Hence, only a small set of data should be collected.

We tackle the above challenges by designing the ActID framework, which consists of a feature evaluation and selection mechanism, a set of high-quality features from multiple perspectives, and a sliding window based identity modeling algorithm.

3. Design of the ActID framework

The ActID framework is depicted in Fig. 1. The framework consists of two phases, the *identity modeling phase* and the *identification phase*.

In Fig. 1, the *identity modeling phase* is shown by the path of blue arrows, and the *identification phase* is depicted by the path of red arrows. In the first phase, when the user walks around, the changes in motion are captured by an activity sensor consisting of an accelerometer and gyroscope, which is placed on the wrist of the user. The sensing data is then transferred to a smart device via a Bluetooth channel. Next, the received data is filtered, resampled, and interpolated to improve the quality of the data. A set of features are extracted

epoc (ms)	timestamp (-0500)	elapsed (s)	x-axis (g)	y-axis (g)	z-axis (g)
1563477690259	2019-07-18T14.21.30.259	0.000	-0.956	0.432	0.082
1563477690269	2019-07-18T14.21.30.269	0.010	-0.968	0.441	0.081

Fig. 2 – Samples of Raw Data.

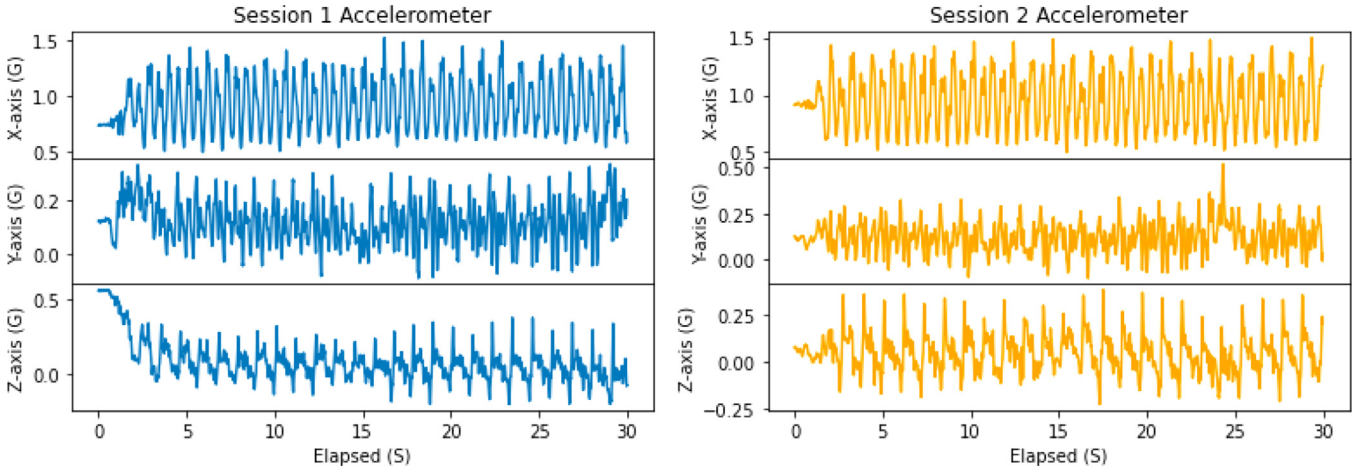

Fig. 3 – Samples of an accelerometer readings of the same user for two sessions.

from the processed data. These features consist of both statistical attributes such as mean, standard deviation, and variance, as well as physical attributes like peak value for an acceleration of hand motion. Feature evaluation algorithms, including Optimal Feature Evaluation and Selection (OFES) and Correlation-based Feature Subset Selection (CFSS), are used to evaluate extracted features and select high-quality features. Then, we establish a Sliding Window based Voting (SWV) classifier as the identity model using a sliding window algorithm and voting method. In the second phase, user activity data is collected similar to the first phase. Subsequently, the collected user data is given as the input to the trained classifier, and the classifier identifies the user. Next, we present the details of the ActID framework.

3.1. *Data acquisition*

In our experiment, we collect activity data from 30 users in two sessions. In each session, users walk as they usually walk on a plain surface for 60 s. We use MetaWear C board mbi (0000) to collect the activity data. The MetaWear C board comes in a very small round form-factor equipped with two sensors including an accelerometer and a gyroscope. The sensor is placed on the wrist of the user. The sensor captures the hand movement of users as they walk. Sensor readings consist of an accelerometer and gyroscope readings along *x*, *y*, and *z*-axes. Therefore, each data point is a 6-tuple, (*Ax*, *Ay*, *Az*, *Gx*, *Gy*, *Gz*), where A_i and G_i specify an accelerometer and gyroscope on the *i* axis, respectively. Each session collects 60 s of data sampled at a frequency of 100 Hz.

Among the two sessions, the data collected in the first session is used to construct the classifier as illustrated in phase one. The data collected in the second session will be used to test the classifier in phase two. The output of the classifier is interpreted as the identity of the user.

Figure 2 represents the sample consisting of 0.01 s of raw data. Figure 3 displays the sample of an accelerometer data of a user in X, Y, and Z dimensions for two sessions (S1 and S2). In the figure, blue color lines represent session 1 data where as orange color lines represent session 2 data. Several studies (Gafurov et al., 2006; Yang et al., 2018) have used a combined signal of all three dimensions by using a vector summation method. These approaches have the advantage of reducing computation time by reducing dimensions; however, if the amplitude of the signal in a particular dimension is much higher than others, dimensions with smaller amplitude signal become ignored. In our study, we use data in all three dimensions separately for feature computation and comparison because this strategy helps in identifying high-quality features.

3.2. *Data pre-processing*

We pre-processed the activity data using interpolation and resampling. Resampling is the process of filling the missing data point with the nearest possible value using the linear interpolation method. Figure 4 shows the scatter plot of a set of sampled data before and after interpolation, where the blue dots represent the data before interpolation and the orange dots depict the data after interpolation. In addition, because the first few and last few data points may contain more noise, we eliminated the first and the last 2000 data points in the dataset and selected 2000 data points.

3.3. *Feature evaluation and selection*

One of the most important steps in developing any biometrics-based identification algorithm is to identify unique features of

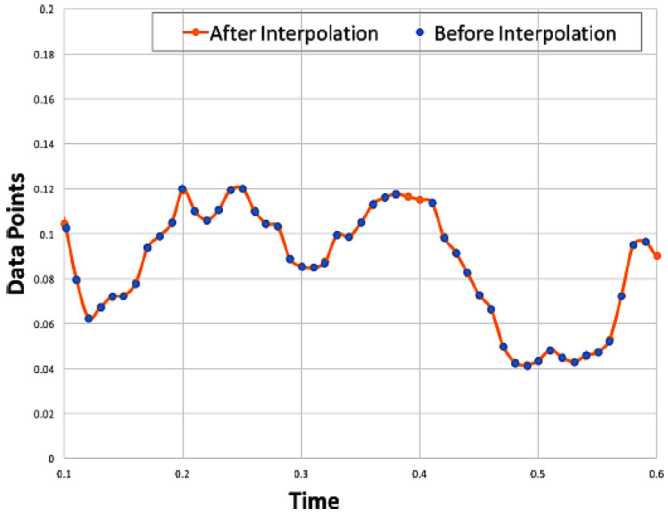

Fig. 4 – Results of Resampling and Interpolation.

the biometric dataset (Derawi et al., 2010). On one hand, the efficiency of the identification algorithm is influenced by the size of the feature set. Typically, to identify a user, a single feature may not be sufficient. Most of the previous studies use a vector of features in their algorithms (Al Kork et al., 2017; Ohana et al., 2013) which increases both the size and dimension of the dataset and results in the increase of complexity of the identification algorithm. On the other hand, the accuracy of the results of identification is primarily influenced by the quality of selected features. We would need high-quality features that can differentiate any two users distinctly which increases the accuracy of the user identification significantly. Distinguishing a particular user from other users is not significant if they are compared using a weak feature. Thus, by excluding weak features based on the results of the feature evaluation, we seek to find a minimum set of high-quality features.

We select a minimum set of high-quality features for gait identification based on the results of our feature evaluation by applying Optimal Feature Evaluation and Selection (OFES) (Kayastha, 2019; Kayastha and Sha, 2019; Sai Ram et al., 2020) and Correlation-based Feature Subset Selection (CFSS) (Hall, 1999) algorithms. First, we extract biometric features which consist of statistical attributes such as mean, median, and variance, as well as physical attributes like peak value for an acceleration of hand, from the processed raw dataset. OFES provides two of the measures, Farness Value and Farness Ratio to evaluate features (Kayastha, 2019; Kayastha and Sha, 2019; Sai Ram et al., 2020). Based on these values, we rank the features according to the ranking method of OFES and identify the high-quality features subset. Second, we reduce the number of sensors used to collect data from users during the identification process in order to make a cost-effective design. To do so, we select only the high-quality features from a sensor that contributes to 70% of high-quality features or more. For example, let's say that among the top 10 selected features, the first 7 features are from the accelerometer, and the last 3 features are from the gyroscope sensor. Since the accelerometer contributes to the majority (i.e., 70%) of the high-quality features, we replace the last 3 features from gyroscope with accelerometer features whose ranks are closest to those 3 gyroscope features. This way we select the 10 high-quality features from the accelerometer sensor only. Third, we apply CFSS to select the set of high-quality features that are correlated to the class label, but independent of each other. To do so, for each feature, we check correlation with every other feature with respect to the class label and identify a set of features that are independent of each other but correlated with the class label.

3.4. *Sliding window vote (SWV) classifier*

Satisfying the real-time requirements of the user is important in identification. We need to collect only a small set of data from the user so that identification completes in a very short period and provides a smooth user experience. Achieving high accuracy with less amount of data is a challenge in classification. Overcoming this challenge, we design Sliding Window Vote (SWV) Classifier on top of a traditional classifier. To make decisions on a small set of data, SWV utilizes sliding windows which not only helps normalize the data but also helps in reusing data in multiple windows. It also adopts a voting method which helps to improve the accuracy of identification.

The sliding window method solves three issues. First, while comparing two users, it is important to align their activity cycles. Second, a small amount of data will not be sufficient enough to classify a user. With a sliding window, we can generate more windows by overlapping and reusing a set of data. Third, overlapping data between subsequent windows improves the accuracy of the classification.

The design of SWV classifier (also referred to be SWV for the rest of the paper) is depicted in Fig. 5. It consists of three major components: a set of windows represented using $W_1, W_2, W_3 \ldots, W_n$, a traditional classifier, and an aggregator.

The windows are used to hold the data segmented from the sensor data stream using the sliding window approach, the main idea of which is presented in Fig. 6. As shown in the figure, d_i represents the data points at position i. The sliding

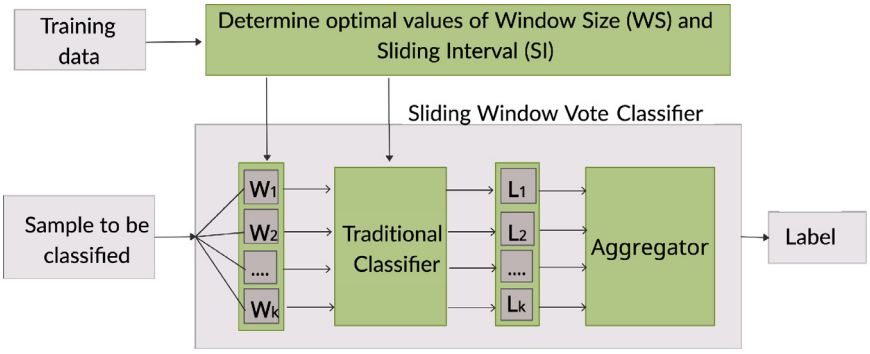

Fig. 5 – Design of the Sliding Window Vote Classifier (SWV).

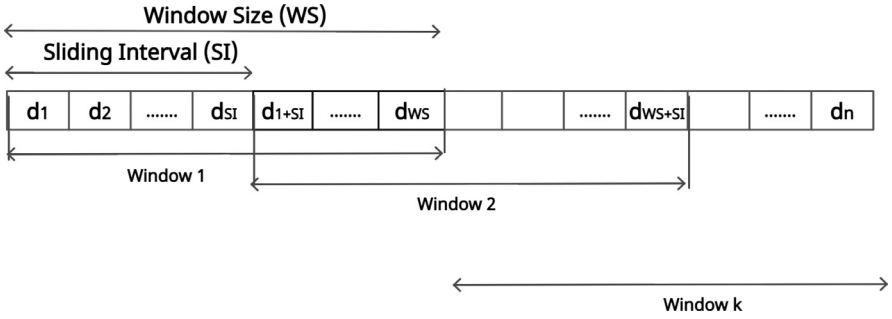

Fig. 6 – Sliding Window Based Feature Extraction.

window takes the first window of WS data points beginning at position d_1 and ending at position d_{WS}, and places it in W_1 in Fig. 5. Then, it slides right by *SI* positions and takes the second window of data starting at position d_{1+SI} and ending at position d_{WS+SI}. This set of data will be placed into W_2. This process will be continued until W_k is filled, which is the last window of the data sequence.

In the sliding window approach, two parameters, *Window Size* that is defined as the fixed amount of time for how many data points contained in a window, and *Sliding Interval* that is defined as a fixed amount of time for how many data points the window will shift, have a big impact on the performance of the classifier. Therefore, the values of these two parameters should be carefully determined, which is achieved by the process of determining optimal values of window size and sliding interval represented in Fig. 5. Once the optimal values are determined, they need to be kept the same for the rest of the process.

The traditional classifier can be any existing lightweight classifier such as Random Forest, Support Vector Machine (SVM), K-Nearest Neighbor (KNN), and Naive Bayes Classifier. Our SWV classifier is built and optimized based on these classifiers. The choice of classifier also impacts the performance of the SWV classifier.

The last component of SWV is the aggregator. Data in each window will be used as the input to the traditional classifier. Accordingly, a class label will be generated for each window of data. The aggregator generates the final class label by aggregating the class label of each window. Majority voting is used in the process of aggregating. In other words, the aggregator counts the votes for each label and selects the label with the highest number of votes.

SWV is trained using the training dataset, which is produced from session one data collected in Section 3.1. First, we find the optimal values for the parameters such as window size and sliding interval, the process of which is discussed below. Then, we generate windows of data with the optimal values of window size and sliding interval from session one data of activity dataset as discussed before. After that, we extract selected features from each window of data to generate a feature dataset. This feature dataset is used as a training dataset and sent to the traditional classifier component as input to train SWV.

To determine optimal values of Window Size and Sliding Interval, first, we initialize window size with any small value and a fixed size for Sliding Interval e.g., 0.5 s, corresponding to 50 data points. As before, we generate a training dataset from session one data of the activity dataset. Then, we train any traditional classifier with a training dataset. Similar to training data, we generate test data from session two data of the activity dataset. Next, we test the classifier using test data to measure accuracy. From our results, we observe that the accuracy of the classifier increases with the increase of window size until a certain point and then decreases. Hence, we increase the window size, extract the feature dataset, and generate the classifier again. We repeat this process until the accuracy of the classifier starts decreasing. Finally, we select the window size which results in the highest accuracy of the classifier. Similarly, we determine the optimal sliding interval that gives high accuracy by fixing the optimal value for window

size and increasing the values of the sliding interval starting from 0.01 s (sliding only one data point), 0.25 s, and so on. In the process of determining sliding interval, we observe that the accuracy of the classifier decreases with the increase of sliding interval. However, with a sliding interval of 0.01 s, data generation time is very long and accuracy is only a little higher than in case of 0.25 s. Hence, we select 0.25 s as the optimum sliding interval by trading off the accuracy with the efficiency.

After SWV is trained, it is used to identify the users. In this process, a few seconds of user activity data is the input to the SWV, and the identity of the user will be the output of the classifier.

4. Experimental results

In this section, we first determine the parameters of the SWV classifier such as optimal window size and sliding interval, choice of the best classifier, selection of feature sets, and activity data size. Next, we conduct a performance evaluation of SWV based on the optimal parameters. The evaluation includes performance in the reduced data set, performance of the scalability, and performance in the accuracy. Finally, we perform a comparison between ActID and other frameworks.

4.1. *Description of dataset*

As we discussed in Section 3, we select 20 s of activity data, i.e., 2000 samples from the processed dataset of 60 s of data, i.e., 6000 samples. The training and testing dataset is the feature dataset calculated from the 20 s of activity data following the window generation procedure as discussed in Section 3.4. As detailed in Section 4.2.4, we find that 10 high-quality features represent a great trade-off between the classification accuracy and complexity.

Various window sizes and sliding intervals are used in the process of determining their optimal values which are discussed in Section 4.2. We determine the optimum window sizes of 6, 8, and 10 s for 10, 15, and 20 s of activity data respectively, and 0.25 s as an optimum sliding interval in all three cases. After that, the optimal values of window size and sliding interval are used in the rest of the experiment for the specific activity data size. Later, these optimal values of window size and sliding interval are used in the process of generating feature dataset. For each specific feature, we will have two sessions of feature dataset. Session one feature dataset was used as train dataset whereas session two feature dataset was used as test dataset.

4.2. *Finding optimal values of SWV parameters*

4.2.1. *Optimal feature set*

In this experiment, we considered 96 features that are used in (Kayastha, 2019; Kayastha and Sha, 2019; Sai Ram et al., 2020). We extract these features and apply OFES and CFSS algorithms as we discussed in Section 3. To identify the high-quality features, first, we ranked them from highest to lowest based on Farness Value and Farness Ratio (Kayastha, 2019; Kayastha and Sha, 2019; Sai Ram et al., 2020). Then, we identify the top 10 features each from the Farness Value and Farness Ratio list. In both of these lists, 8 out of 10 features are in common. Next, we select the top 10 features from both Farness Value and Farness Ratio list considering the ranks of both Farness Value and Farness Ratio. Table 1 represents the top 10 features selected. In the table, all the top 10 features belong to accelerometer readings. Hence, we use only one sensor, i.e., an accelerometer to collect activity data during user identification.

4.2.2. *Optimal window size*

This experiment was conducted to find the optimum window size required to uniquely identify a person. We select SVM classifier as our default standard classifier which is discussed in the following subsections. To find the optimal window size, we use various values of window sizes starting from 2 s and a fixed size of sliding interval. For example, we use 0.5 s of sliding interval for this experiment.

Figures 7 and 8 demonstrates the accuracy with different window sizes for 15 and 20 s of activity data or data segment respectively. In these figures, the x-axis represents the window size in seconds whereas the y-axis represents the accuracy of the SVM classifier. From both figures, we observe that, since the size of the total dataset is fixed in this study, the graph achieves a peak and then starts to fall. We select the window sizes at the peak point which are 8 s and 10 s as optimum values in the case of 15 and 20 s of activity data respectively.

4.2.3. *Optimal sliding interval*

Similar to window size, an experiment was conducted to find the optimum sliding interval required to uniquely identify a person. Likewise, when analyzing the impact of sliding interval on the classification accuracy, we fix the window sizes to optimal values of 8 s and 10 s for 15 and 20 s of activity data respectively.

Figure 9 demonstrates the accuracy of SVM classifier with different sliding intervals for 15 and 20 s of activity data. In the figure, the x-axis represents the sliding interval in seconds whereas the y-axis represents the accuracy of the SVM classifier. We use different values for sliding intervals such as 0.01, 0.25, 0.5, 1 s, and so on. As mentioned in Section 3.4, we skip the sliding interval size of 0.01 s. We observe that since the size of the total dataset is fixed in this study, the accuracy of the classifier decreases with the increase in the sliding interval. As per our analysis, 0.25 s of the sliding interval is an optimum size of the sliding interval in both cases of 10 and 20 s of activity data which results in the highest accuracy of the SVM classifier.

4.2.4. *Optimal number of features*

The size of feature set impacts the accuracy as well as time complexity of the classifier. Hence, it is necessary to select a minimum number of high-quality features. We conduct an experiment where a set of classifiers are constructed using various classification algorithms and based on a different number of selected features. We select four lightweight classification algorithms which are widely used in user identification applications, including K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Naive Bayes, and Random Forest Classifier. Four different sets of top-ranked features with sizes 8, 10, 12,

Table 1 – Top 10 features selected.

Rank	OFES	Definition
1.	Mean ACC X	Mean of acceleration data along the x-axis. The mean is the most common measure of central tendency. It is simply the sum of the numbers divided by the number of numbers.
2.	Median ACC X	Median of acceleration data along the x-axis. The median is also a frequently used measure of central tendency. The median is the midpoint of a distribution.
3.	Mean ACC Y	Mean of acceleration data along the y-axis.
4.	Median ACC Y	Median of acceleration data along the y-axis.
5.	Energy ACC X	Energy of acceleration data along the x-axis. The total energy of a signal x is defined as the sum of squared moduli.
6.	Median ACC Z	Median of acceleration data along the z-axis.
7.	Mean ACC Z	Mean of acceleration data along the z-axis.
8.	Energy ACC Y	Energy of acceleration data along the y-axis.
9.	Skewness ACC Y	Skewness of acceleration data along the y-axis. Skewness is a measure of symmetry, or more precisely, the lack of symmetry. A distribution, or data set, is symmetric if it looks the same to the left and right of the center point. We compute the Skewness by using the scipy.stats.skew library in Python.
10.	Root Mean Square ACC X	Root Mean Square of acceleration data along the x-axis. The root mean square, also known as the quadratic mean, is a statistical measure of the magnitude of a varying quantity, or set of numbers. Its name comes from its definition as the square root of the mean of the squares of the values.

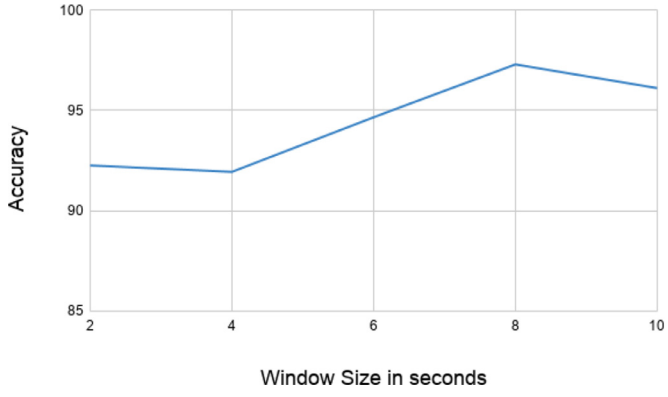

Fig. 7 – Impact of window size on 15 s of data.

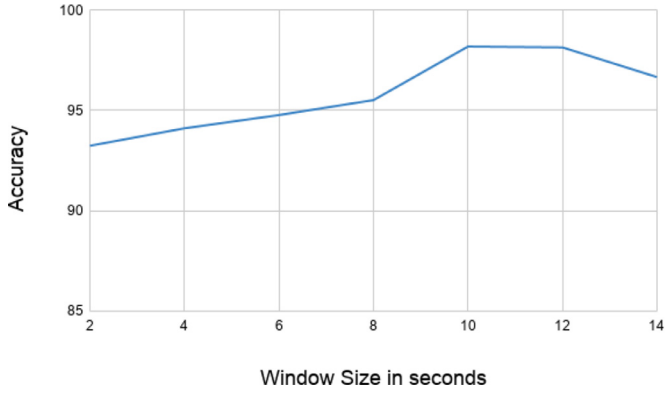

Fig. 8 – Impact of window size on 20 s of data.

and 14 are used to construct different classifiers and the accuracy of each classifier is evaluated.

Figure 10 shows the results of the above experiment, where the x-axis specifies the size of the feature set, and the y-axis indicates the accuracy of the classifier constructed using a different number of selected features. Each colored line represents the accuracy of a classifier constructed based on a different classification algorithm for a specific number of selected features. From the figure, we observe that classifiers built based upon 4 different sets of features exhibit close per-

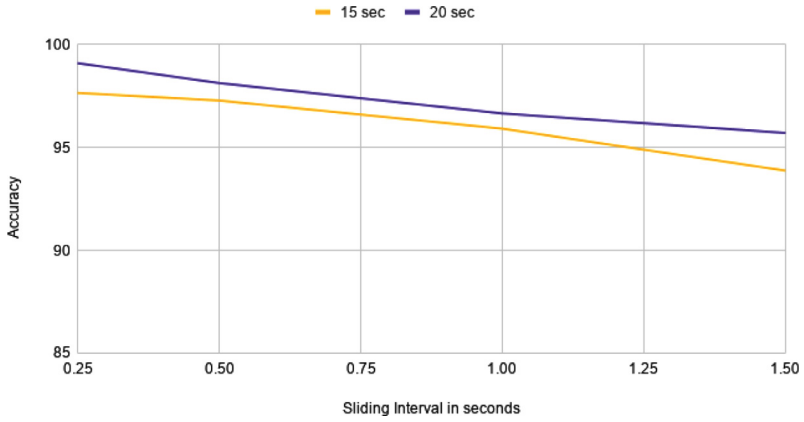

Fig. 9 – Impact of sliding interval.

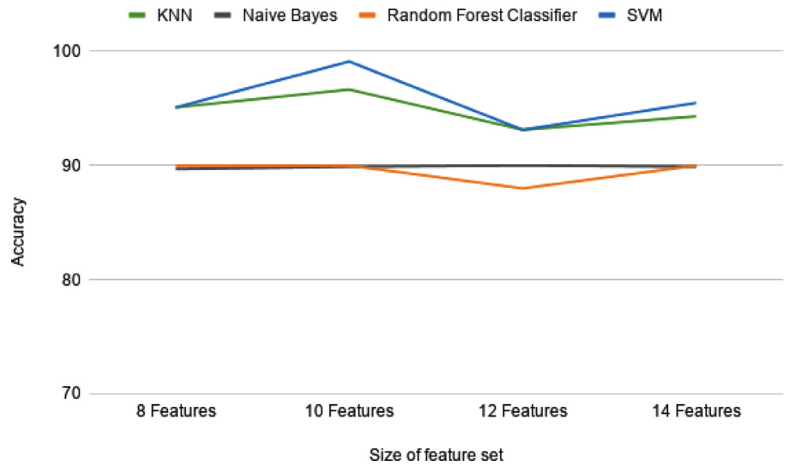

Fig. 10 – Impact of number of features.

formance in terms of accuracy, which is mostly between 90% and 100% except for the Random Forest Classifier which results in around 85%. Classifiers built based on 8, 12, and 14 features have a very close performance for all four classification algorithms, while the classifier on 10 features has slightly higher accuracy. Hence, we select 10 feature set as the minimum feature set that results in high accuracy. Among the four classification algorithms, the SVM exhibits the best accuracy while Random Forest Classifier has the least accuracy. Some classification algorithms like Naive Bayes and Random Forest Classifier are less sensitive to the number of features. The above observations confirm our belief that a small number of high-quality features is sufficient to build a highly accurate classifier. It is also necessary to identify a set of high-quality features to reduce the complexity of the classification process.

4.2.5. *Optimal classifier*

Our SWV classifier is built on top of a traditional classifier. Therefore, the choice of different classifiers may impact the performance of our voting classifier. We believe that deep learning classifiers are too heavy for real-time user identification. Hence, we test four popular lightweight classifiers including KNN, SVM, Naive Bayes, and Random Forest Classifier.

Table 2 – Performance comparison between SWV and traditional classifiers in terms of accuracy.

Classifier Model	KNN	Naive Bayes	RFC	SVM
SWV	96.66%	96.66%	86.66%	100%
Standard Classifier	96.53%	94.76%	85.76%	97.98%

We compute the accuracy of the SWV Classifier built on top of these traditional classifiers for comparison.

A comparison between standard classifier and SWV classifier built on top of respective standard classifier can be found in Table 2. The results mentioned in the table represent the accuracy of the multi-class classifier that classifies 30 users with 20 s of activity data each. SWV classifier with traditional classifier as Random Forest Classifier achieves the least accuracy of 86.66% whereas KNN, SVM, and Naive Bayes results in the accuracy of 96.66%, 100%, and 96.66% respectively. For all the four traditional classifiers, the SWV classifier improves the accuracy. We select the SVM classifier as the best traditional classifier for the SWV classifier since it achieves the highest accuracy compared to others.

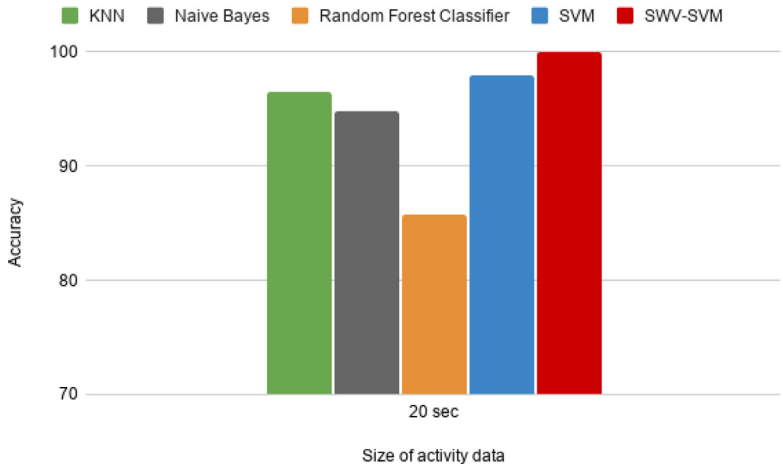

Fig. 11 – Performance comparison between SWV classifier and other traditional classifiers.

4.3. *Performance evaluation of SWV*

From the above experiment, we select SVM classifier as our standard classifier to build SWV classifier, SWV-SVM, in terms of accuracy, scalability, and stability when applied to a small dataset.

4.3.1. *Performance comparison between SWV and traditional classifiers*

Figure 11 represents the performance of SWV-SVM with other traditional classifiers. In the figure, the *x*-axis represents different classifiers whereas the *y*-axis represents the accuracy of the classifier for 20 s of activity data. Random Forest Classifier achieves the least accuracy of 85.76% whereas KNN, SVM, and Naive Bayes results in the accuracy of 96.53%, 97.98%, and 94.76% respectively. SWV-SVM achieves the highest accuracy of 100% when compared to others.

4.3.2. *Scalability of SWV*

The accuracy of classifiers usually decreases with the increase in the number of class labels in a multi-class classification (Kumari and Thakar, 2017). Classifiers constructed based on high-quality features should be scalable with the number of class labels. In other words, classifiers should maintain high accuracy with the increase in the number of class labels.

In this experiment, we compare the performance of the SVM classifier (the best-performed classifier among the four evaluated traditional classifiers) and SWV-SVM in 14, 20, 25, and 30-class classification. The results are depicted in Fig. 12, where the *x*-axis specifies the number of class labels, and the *y*-axis indicates the accuracy of the classifier for 20 s of activity data. Blue color represents SVM classifier where red color represents SWV-SVM classifier.

From the figure, we observe that, for all datasets with 14, 20, 25, and 30 users, SWV-SVM results in consistent high accuracy while traditional SVM classifier's accuracy decreases with the increase of the number of users. Similar results are seen using other traditional classifiers as well. It shows that SWV not only improves the accuracy of traditional classifiers, but it is also scalable to the size of labels.

4.3.3. *Stability of SWV when applied to a small dataset*

Increasing the size of collected data will both result in a longer data process and longer data collection time, and cause inconvenience to the user. However, smaller activity data size may not capture the entire cycle of walking. Therefore, an optimum size of activity data is required.

Figure 13 demonstrates the accuracy of the SVM and SWV-SVM with 10, 15, and 20 s of activity data. In the figure, the *x*-axis represents the activity data size in seconds whereas the *y*-axis represents the accuracy of classifiers. We observe that SVM trained with 15 s and 20 s of activity data results in similar performance with an accuracy of 97.7% and 97.96% respectively whereas SVM trained with 10 s of activity data results in slightly lesser accuracy of 95.74%. SWV classifier results in 100% accuracy in all three cases. In general, the accuracy of traditional classifiers decreases when the dataset size gets smaller, e.g., 10 s. SWV exhibits a better performance than the traditional classifier. As shown in the figure, it not only always has a better performance than traditional SVM but also remains 100% accurate even when the dataset size is reduced to 10 s. This helps to achieve real-time authentication.

4.4. *ActID with other similar user identification approaches*

In this section, we compare ActID with other similar user identification approaches. Table 3 shows the comparison of ActID with others in terms of a number of features, best classification method, user set size, activity data size, and accuracy. In the table, two measures including EER, and accuracy are used to show the results. EER is defined as the equal error rate which indicates that the proportion of false acceptances is equal to the proportion of false rejections. The lower the EER, the higher the accuracy of the identification.

In the table, Nickel et al. (2012) uses the highest number of 52 features with EER 8.24% whereas (Gafurov et al., 2006) uses only one feature with EER 5% and 9%. We observe that both the highest and least number of features result in a significant decrease in accuracy. ActID uses an optimum number of 10 features which results in the highest accuracy of 100%.

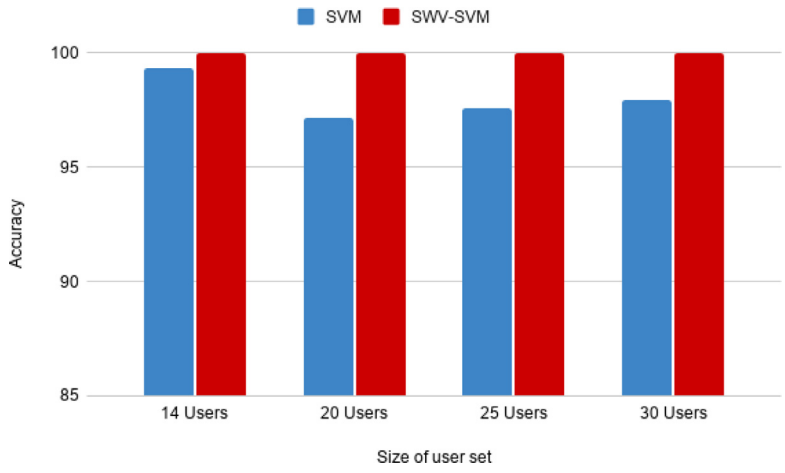

Fig. 12 – Scalability of SWV.

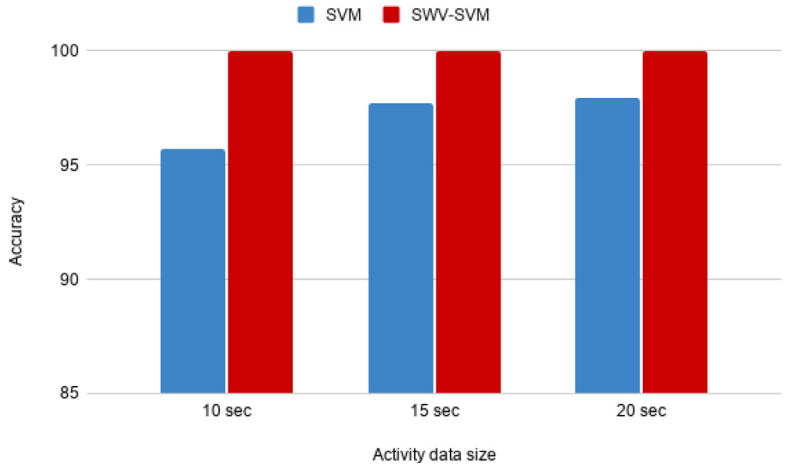

Fig. 13 – Impact of activity data size.

Table 3 – Comparison of our approach versus other approaches.

Paper	Features	Best Classification Method	Size of User Set	Activity data size	Results
Kumar et al. (2016)	31 features	K-NN	12	2 min	Accuracy: 95%
Damaševičius et al. (2016a)	10 features	Heuristic (random projections + PDFs + Jaccard distance)	14		Accuracy: 95.52%
Liu et al. (2017)	20 features (time and frequency- domain)	C4.5 decision tree classifier	7	20 min	Accuracy: 86.7%
Johnston and Weiss (2015)	6 features	Rotation Forest	59	5 min	Accuracy: 84%
Nickel et al. (2012)	52 features	K-NN	20	1.7 min	EER: 8.24%
Al Kork et al. (2017)	3 types of features	Manhatten method	23	4.5 min	EER: 1.23% to 4.07%
Gafurov et al. (2006)	1 feature	Histogram Similarity and Cycle Length methods	21		EER: 5%, 9%
Our Approach	**10 features (time and frequency- domain)**	**SWV-SVM**	**30**	**10 sec**	**Accuracy: 100%**

Table 4 – List of high quality features.

No.	Features
1.	Energy ACC X
2.	Energy ACC Y
3.	Energy ACC Z
4.	Variance ACC X
5.	Variance ACC Y
6.	Variance ACC Z
7.	Mean ACC X
8.	Mean ACC Y
9.	Median ACC X
10.	Median ACC Y
11.	Root Mean Square ACC X
12.	Root Mean Square ACC Z

Johnston and Weiss (2015) uses 5 min of activity data and results in a lesser accuracy of 84%. Al Kork et al. (2017) results in low EER of 1.23% to 4.07% but collects 4.5 min of activity data. Liu et al. (2017) collects 20 min of activity data and results in lesser accuracy of 86.7%. ActID only uses 10 s of activity data but results in the highest accuracy of 100%. Nickel et al. (2012) and Kumar et al. (2016) select K-NN as the best classification method, while ActID selects SWV-SVM. Johnston and Weiss (2015) uses highest user set size of 59, Liu et al. (2017) uses lowest user set size of 7, whereas ActID uses a user set size of 30. Damaševičius et al. (2016a) and Kumar et al. (2016) results in accuracy of around 95% whereas ActID results in the highest accuracy of 100%.

In summary, ActID uses an optimum number of features, i.e., 10 features, least amount of activity data, i.e., 10 s, yet results in the highest accuracy of 100% when compared to others.

4.5. *Discussion*

Stability of High-Quality Features. We believe the results of our feature selection method are consistent across a different number of users. To verify this hypothesis, we compare the top 15 selected features obtained based on 14-user and 30-user datasets. We have the following two observations. First, all the top 15 features are from the accelerometer sensor. This supports our hypothesis that an accelerometer alone may be sufficient for identifying users based on their behavior. Second, 12 out of the top 15 resulted features are in common. This supports our hypothesis that the top-ranked features from our feature selection process are consistent with gait characteristics in different individuals. Table 4 lists the 12 common features.

Analysis of the Perfect Accuracy. The accuracy results published in this study are based on a 30-user dataset, using our top 10 selected features as well as the optimal values of model parameters, including window size, sliding interval, and data segment size. Many factors may impact the accuracy, including the number of users, the types of users, the choice of parameters, etc., so we believe, for larger size user sets, accuracy may not always be 100% but it could still be very close to 100%, because in our experiments all participants are college students who may have similar activity patterns, which can be considered as a challenging case for identification. In the future, we plan to verify the results of both the feature selection method and the SWV classifier (based on features selected from our feature selection method) with a diversified and large number of user sets.

The two sessions of user data are collected at separate times as we tried to avoid unnecessary similarity introduced in the data collection process. However, we also have to agree that the changes in user's moving patterns over time may have an impact on the identification accuracy. We are currently investigating new approaches that can cope with the pattern changes. This is our future work.

Efficiency Analysis of the Classification Algorithm. We believe our classification algorithm is lightweight. First, because of the feature selection algorithm, we can significantly reduce the number of features. This reduces the complexity of the algorithm while maintaining high accuracy. The feature evaluation is done before the classifiers are trained and it only needs to be done once. We can perform feature evaluation on a powerful device such as at the computing edge. Second, the classifier training phase can be separated from the identification phase. The training phase is more computing-intensive than the identification phase. Third, the identification phase is only based on a small amount of data, 10 s of activity data. Fourth, we can adjust the sliding intervals to keep the classification phase even more lightweight; however, the impact of accuracy also needs to be considered. All the above designs make the algorithm to be a lightweight algorithm. To verify these arguments, we conducted a preliminary experiment to evaluate the computing cost of the proposed algorithm in terms of execution time as summarized below.

In the experiment, we first evaluated the execution time of identification on an old Macbook Air (Early 2015 model) with a 1.6 GHz Intel Core 5 processor (64-bit dual-core) and 8GB memory size. The identification only took 4 milliseconds. If we consider more computing-intensive tasks, feature extraction and classifier training, the execution time is 2 s and 33 milliseconds respectively. Although we were not able to find a direct performance comparison between the processing speed of Macbook Air (early 2015 model) and Apple Watch 6, we found a performance comparison between MacBook Air (early 2015 model) processor and Snapdragon 200, as well as Apple Watch 6 processor and Snapdragon 200. This enables us to have an indirect comparison. The report from Notebookcheck (Hinum, 2020) said the processor of Apple Watch 6 is comparable to Snapdragon 200, while the processor of MacBook Air (early 2015 model) is 10 times as fast as the processor of Motorola Moto E i.e., which uses Snapdragon 200 Benchmarks (2021). Therefore, we estimate that the execution time in the smartwatch (Apple Watch 6) would be approximately 20 s for feature extraction, 330 milliseconds for classifier training, and 40 milliseconds for identification. When we offload the feature extraction and classifier training to a smartphone like the iPhone 12, which executes 3 times as fast as MacBook Air (early 2015 model) (Benchmarks, 2021), the estimated execution time will be less than 1 s for feature extraction and 11 milliseconds for classifier training. In conclusion, we believe our algorithm is sufficiently lightweight to be executed on mobile devices, even for smartwatches like Apple Watch 6, especially when we of-

Table 5 – A summary of user identification based on activity sensor.

Study	Subjects	Sensor Location	Results
Ailisto et al. (2005)	36	Waist	EER: 6.4%
Mantyjarvi et al. (2005)	36	Waist	EER: 7% - 19%
Gafurov et al. (2006)	21	Lower leg	EER: 5%, 9%
Al Kork et al. (2017)	23	Leg, hand, wrist, pant pocket, shirt pocket and bag (left and right side) Hand (holding smartphone)	EER: 0.17% - 2.27% EER: 1.23% - 4.07%
Derawi et al. (2010)	51	Pocket attached to the belt (right-hand side of the hip)	EER: 20.1%
Rong et al. (2007)	21	Waist	EER: 5.6%, 21.1%
Sun and Yuao (2012)	22	ankle	EER: 3.03%
Kwapisz et al. (2010)	36	Front pants leg pocket	Accuracy: 82.1%, 92.9%
Thang et al. (2012)	11	Trouser pocket position	Accuracy: 92.7% (SVM)
Johnston and Weiss (2015)	59	Waist (smartwatch)	EER: 2.6% - 8.1%

fload the heavy computing tasks to an edge device like the iPhone.

Currently, we are developing a continuous authentication protocol based on both smartwatch and smartphone. We will build a prototype to quantitatively evaluate the CPU utilization rate, communication cost, and power consumption.

5. Related work

Activity-based user identification has been an interesting research topic. In this section, we list a set of work that is related to our research.

5.1. *Activity sensor-based user identification*

Biometrics-based user identification is an effective solution to identify or verify individuals based on their unique physiological or behavioral characteristics (Vacca, 2007). Physiological biometrics is associated with the precise measurements, dimensions, and physical traits of an individual. In contrast to physical biometrics, behavioral biometrics are easily gathered with existing hardware or wearable sensors that require less power consumption, requiring only software for analysis purposes. Hence, it makes behavioral biometrics cost-effective and easy to implement. Our study falls into the category of behavioral biometrics.

In behavioral biometrics, activity sensor based user identification has shown great research potential in the last few years.

One of the most popular activity-based biometric characteristics is gait because researchers have shown it to be feasible means for authentication. Table 5 summarizes some of the recent studies on gait recognition based on the activity sensor. Ailisto et al. (2005) were the first to propose sensor-based gait authentication. Their gait authentication was based on the acceleration sensor that was attached to the user's waist. They applied cross-correlation as a measure of similarity achieving 6.4% of EER. Their approach was further developed and analyzed by Gafurov et al. (2006). Some designs have used sensors attached to different parts of the body (e.g., leg, waist, hip, arm, and all over the body) for gait authentication (Al Kork et al., 2017), which is not practical in real-life scenarios. Therefore, we have not yet seen large-scale deployments of these technologies.

5.2. *Smartphone and wrist sensor based user identification*

Modern smartphones and wrist-wearables are equipped with powerful sensors that capture activity sensor data of individuals who carry them. These devices have become a rich data source to measure human activities such as walking, jogging, sitting, climbing stairs, and so on (Su et al., 2014). Hence, these devices are unobtrusive, easier to carry, and convenient to collect activity data for user identification compared to other technologies. Nickel et al. (2012) developed a method to extract gait features using the K-Nearest Neighborhood algorithm and demonstrated its feasibility on smartphones achieving an EER of 8.24%. Al Kork et al. (2017) developed a multi-model biometric database for human gait using wearable sensors and a smartphone. They achieved a very low EER of 0.17% to 2.27%. At the same time, it can be noted that they have used five sensor nodes on different body locations in addition to a smartphone with built-in accelerometer and gyroscope sensors held in hand. We, on the other hand, have used a single sensor node in our method. Also, their data collection time is 4.5 min while our data collection time is 60 s out of which we use only 10 s of data. Garcia et al. (2016) were the first to consider hand dynamics for authentication based on hand movement while opening a door. They used sensors, namely, accelerometer, gyroscope, and magnetometer embedded in Google Nexus 4 smartphones to collect sensor data. For classification, they proposed a machine learning-based approach, consisting of various statistical and physical features and Support Vector Machine (SVM). With their approach, they achieved an accuracy of 92%. Most studies on smartphone-based gait recognition assume that the phone is placed at a fixed location (e.g., waist, pocket, or hand) so that they can disregard the variations introduced in the walking pattern captured by motion sensors due to changes in the placement of the phone (e.g., from pocket to hand) (Primo et al., 2014). However, in a real sit-

uation, there is no precise location of the phone on the user's body and no proper framework that can locate the position of the phone automatically exists currently (Kumar et al., 2016).

Wrist-wearables like smartwatches and wristbands provide great advantages over smartphones, particularly in gait authentication because users usually wear their smartwatches or wristbands in the same location and orientation. Compared to the most common location for smartphones such as pockets or handbags, the wrist location provides more accurate information about a user's movements (Johnston and Weiss, 2015). Wearable sensor based activity recognition has several useful applications in health care, patient or elderly monitoring, rehabilitation training, and many other areas of human interaction (Xu et al., 2016). Due to its rising popularity, location consistency, and wide applicability, it is more practical to collect activity data from wrist-wearables for user identification.

In Johnston and Weiss (2015), Johnston et al. used a smartwatch to collect gait data and achieved the EER of 2.6% using features derived from the accelerometer data and EER of 8.1% using data derived from gyroscope data. They showed their result using 6 types of features, namely, average, standard deviation, average absolute difference, the time between peaks, binned distribution, and average resultant acceleration by training five minutes of the dataset with a maximum identification accuracy of 84%. In both above studies, a long duration of data was used for training the model. Our experiment used only 10 s of data and provided a promising result of 100%. In a realistic scenario where data acquisition time will be limited, our analysis is more feasible and optimum.

Kumar et al. (2016) proposed four continuous authentication designs by using the characteristics of arm movements while individuals walk. They collected motion data with a smartwatch's sensor. Their first design uses an accelerometer sensor to capture acceleration of arms, the second design uses a gyroscope sensor to collect rotation of arms, and the third one uses the combination of both accelerometer and rotation at the feature level and the fourth design uses fusion at score-level.

A recent study done by Liu et al. (2017), illustrated an approach for authentication using 20 different features from time and frequency domain. They adopted the C4.5 decision tree in their proposed scheme and achieved an accuracy of 86.7%. The author concluded with the need for a feature selection strategy to improve the performance of the model and reduce computational complexity.

López-Fernández et al. (2015) proposed a multi-view gait recognition on curved paths using local variations on the angular measurements along time. They have used a stream of images from a certain number of fixed cameras (Eg. surveillance cameras) to recognize a user based on gait patterns whereas we used activity data from the accelerometer sensor on the wrist of the user. We shared some similar ideas in the classifier design, but our design couples with a unique feature selection and our identification approach has fewer constraints on user movement and is less costly. In addition, we have also introduced a mechanism to obtain optimal values of the parameters such as window size and sliding interval during the sliding window process.

This study is based on but significantly extends Ms. Namrata Kayastha's Master's Thesis (Kayastha, 2019). The differences are summarized below. The focus of the thesis is to develop a feature evaluation and selection mechanism, while in this paper, we focus on designing a multi-class classification algorithm. In the evaluation of the thesis, the experiments are based on a 14-user single-session dataset, while in this paper, the experiments are based on a 30-user two-session dataset. We have also improved the feature selection algorithms in this paper by applying correlation analysis and sensor reduction. Consequently, the classification in this paper is based only on a set of accelerometer data, while the classification in the thesis uses both accelerometer and gyroscope data. Furthermore, the thesis only utilizes and evaluates existing traditional classification algorithms, but we designed and evaluated a novel sliding window based voting classification algorithm in this paper. As a result, the paper improves classification accuracy.

In summary, compared with many previous research, our experiment only uses 10 s of data and we tackle the challenges faced by the previous studies. With our proposed framework, we intend to keep the size of the feature set as small as possible, identify a set of high-quality features that can help distinctly identify individuals, provide a smooth user experience, as well as provide a promising result.

6. Conclusion and future scope

In this study, we proposed a novel ActID framework that effectively addresses various real-time challenges of user authentication based on activity sensor data. We introduced a novel Sliding Window Vote Classifier which significantly improved the identification accuracy over traditional classifiers. It demonstrates that even a small amount of activity data and optimal feature dataset is sufficient to uniquely identify a user. This suggests that a balance can be achieved between computation time and accuracy while designing an identification protocol. Furthermore, the SVM classifier is shown to be the consistent and best classifier among the traditional classifiers for user identification based on activity sensor data. Our empirical analysis provided a mechanism to determine the optimal window size and sliding interval, and to reduce the number of sensors used to collect activity data.

In the future, we plan to extend the ActId framework to continuous authentication applications and evaluate several factors such as a large number of user sets, spoofing, etc. We would also introduce a mechanism to learn the biometric changes of the user that occur as the user ages along with a method to detect various activities of the user like walking, running, sitting, etc.

Declaration of Competing Interest

We have no competing interests to declare.

CRediT authorship contribution statement

Sai Ram Vallam Sudhakar: Software, Validation, Investigation, Visualization, Writing - original draft. **Namrata Kayastha:**

Software, Investigation, Writing - review & editing. **Kewei Sha:** Conceptualization, Methodology, Formal analysis, Visualization, Writing - original draft, Supervision, Project administration, Funding acquisition.

Acknowledgement

This paper is based upon work supported by the National Science Foundation under grant no. DEG-1723596 and University of Houston-Clear Lake Faculty Research Support Funds.

REFERENCES

Abate A, Nappi M, Ricciardi S. I-Am: implicitly authenticate me person authentication on mobile devices through ear shape and arm gesture. IEEE Trans. Syst. Man Cybern. 2017;PP:1–13. doi:10.1109/TSMC.2017.2698258.

Abuhamad M, Abusnaina A, Nyang D, Mohaisen D. Sensor-based continuous authentication of smartphones users using behavioral biometrics: a contemporary survey. IEEE Internet Things J. 2021;8(1):65–84. doi:10.1109/JIOT.2020.3020076.

Ailisto HJ, Lindholm M, Mantyjarvi J, Vildjiounaite E, Makela S-M. Identifying people from gait pattern with accelerometers. In: Jain AK, Ratha NK, editors. In: Biometric Technology for Human Identification II. International Society for Optics and Photonics. SPIE; 2005. p. 7–14. doi:10.1117/12.603331.

Al Kork SK, Gowthami I, Savatier X, Beyrouthy T, Korbane JA, Roshdi S. Biometric database for human gait recognition using wearable sensors and a smartphone. In: 2017 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART); 2017. p. 1–4. doi:10.1109/BIOSMART.2017.8095329.

Alizadeh M, Abolfazli S, Zamani M, Baaaharun S, Sakurai K. Authentication in mobile cloud computing: a survey. J. Netw. Comput. Appl. 2016;61:59–80. doi:10.1016/j.jnca.2015.10.005.

Benchmarks. Primate Labs Inc., (Accessed: 9 April 2021). https://browser.geekbench.com/.

Blasco J, Chen TM, Tapiador J, Peris-Lopez P. A survey of wearable biometric recognition systems. ACM Comput. Surv. 2016;49(3). doi:10.1145/2968215.

Casanova J, Ávila C, Bailador G, Sierra A. Authentication in mobile devices through hand gesture recognition. Int. J. Inf. Secur. 2012;11:65–83.

Chatra AS. Cognitive biometrics based on eeg signal. In: 2014 International Conference on Contemporary Computing and Informatics (IC3I); 2014. p. 374–6. doi:10.1109/IC3I.2014.7019605.

Chen J. Gait correlation analysis based human identification. ScientificWorldJournal 2014;2014:168275. doi:10.1155/2014/168275.

Chen L, Hoey J, Nugent CD, Cook DJ, Yu Z. Sensor-based activity recognition. IEEE Trans. Syst. Man Cybern. Part C 2012;42(6):790–808. doi:10.1109/TSMCC.2012.2198883.

Crawford H, Renaud K, Storer T. A framework for continuous, transparent mobile device authentication. Comput. Secur. 2013;39:127–36. doi:10.1016/j.cose.2013.05.005. https://www.sciencedirect.com/science/article/pii/S0167404813000886

Damaševičius R, Maskeliunas R, Venčkauskas A, Woźniak M. Smartphone user identity verification using gait characteristics. Symmetry 2016;8(10):100. doi:10.3390/sym8100100.

Damaševičius R, Vasiljevas M, Šalkevičius J, Woźniak M. Human activity recognition in AAL environments using random projections. Comput. Math. Methods Med. 2016;2016:17. doi:10.1155/2016/4073584.

Derawi MO, Nickel C, Bours P, Busch C. Unobtrusive user-authentication on mobile phones using biometric gait recognition. In: 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing; 2010. p. 306–11. doi:10.1109/IIHMSP.2010.83.

Dey M, Dey N, Mahata SK, Chakraborty S, Acharjee S, Das A. Electrocardiogram feature based inter-human biometric authentication system. In: 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies; 2014. p. 300–4. doi:10.1109/ICESC.2014.57.

Face id security [online]. 2017. https://www.apple.com/ca/business-docs/FaceID_Security_Guide.pdf.

Gafurov D, Helkala K, Torkjel S. Biometric gait authentication using accelerometer sensor. J. Comput. 2006;1. doi:10.4304/jcp.1.7.51-59.

Gafurov D, Snekkenes E. Gait recognition using wearable motion recording sensors. EURASIP J. Adv. Signal Process. 2009;2009:1–16.

Garcia FT, Krombholz K, Mayer R, Weippl E. Hand dynamics for behavioral user authentication. In: 2016 11th International Conference on Availability, Reliability and Security (ARES); 2016. p. 389–98. doi:10.1109/ARES.2016.107.

Guan D, Yuan W, Sarkar A. Review of sensor-based activity recognition systems. IETE Tech. Rev. 2011;28:418. doi:10.4103/0256-4602.85975.

Gupta JP, Singh N, Dixit P, Semwal VB, Dubey SR. Human activity recognition using gait pattern. Int. J. Comput. Vis. Image Process. 2013;3(3):31–53. doi:10.4018/ijcvip.2013070103.

Hall MA. In: Technical Report. Correlation-based Feature Selection for Machine Learning; 1999.

Hinum, K., 2020. Apple S6 processor - benchmarks and specs. https://www.notebookcheck.net/Apple-S6-Processor-Benchmarks-and-Specs.502601.0.html.

Johnston AH, Weiss GM. Smartwatch-based biometric gait recognition. In: 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS); 2015. p. 1–6. doi:10.1109/BTAS.2015.7358794.

Kayastha N. Biometrics-based user identification with optimal feature evaluation and selection. College of Science and Engineering, University of Houston-Clear Lake; 2019. Master's thesis.

Kayastha N, Sha K. Poster abstract: a novel and efficient approach to evaluate biometric features for user identification. In: 2019 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE); 2019. p. 21–2. doi:10.1109/CHASE48038.2019.00016.

Kumar, R., Phoha, V. V., Raina, R., 2016. Authenticating users through their arm movement patterns. arXiv preprint arXiv:1603.02211.

Kumari A, Thakar U. Hellinger distance based oversampling method to solve multi-class imbalance problem. In: 2017 7th International Conference on Communication Systems and Network Technologies (CSNT); 2017. p. 137–41. doi:10.1109/CSNT.2017.8418525.

Kwapisz JR, Weiss GM, Moore SA. Cell phone-based biometric identification. In: 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS); 2010. p. 1–7. doi:10.1109/BTAS.2010.5634532.

Lee H, Hwang JY, Kim DI, Lee S, Lee S-H, Shin JS. Understanding keystroke dynamics for smartphone users authentication and keystroke dynamics on smartphones built-in motion sensors. Sec. Commun. Netw. 2018;2018:2. doi:10.1155/2018/2567463.

Lin C-L, Hwang T. A password authentication scheme with secure password updating. Comput. Secur. 2003;22:68–72. doi:10.1016/S0167-4048(03)00114-7.

Liu B, Luo H, Chen CW. A novel authentication scheme based on acceleration data in WBAN. In: 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and

Engineering Technologies (CHASE); 2017. p. 120–6. doi:10.1109/CHASE.2017.70.
López-Fernández D, Madrid-Cuevas FJ, Carmona-Poyato A, Muñoz Salinas R, Medina-Carnicer R. Multi-view gait recognition on curved trajectories. In: Proceedings of the 9th International Conference on Distributed Smart Cameras. New York, NY, USA: Association for Computing Machinery; 2015. p. 116–21. doi:10.1145/2789116.2789122.
Mantyjarvi J, Lindholm M, Vildjiounaite E, Makela S, Ailisto HA. Identifying users of portable devices from gait pattern with accelerometers. Proceedings. (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005., 2005. ii/973–ii/976 Vol. 2
Marsico MD, Mecca A. A survey on gait recognition via wearable sensors. ACM Comput. Surv. 2019;52(4). doi:10.1145/3340293.
Metawear c product specification v1.0. https://mbientlab.com/documents/MetaWearC-CPRO-PS.pdf.
Merkle RC. A digital signature based on a conventional encryption function. In: Pomerance C, editor. In: Advances in Cryptology — CRYPTO '87. Berlin, Heidelberg: Springer Berlin Heidelberg; 1988. p. 369–78.
Mondal S, Bours P. Swipe gesture based continuous authentication for mobile devices. In: 2015 International Conference on Biometrics (ICB); 2015. p. 458–65. doi:10.1109/ICB.2015.7139110.
Nickel C, Wirtl T, Busch C. Authentication of smartphone users based on the way they walk using k-NN algorithm; 2012. p. 16–20.
Ohana DJ, Phillips L, Chen L. Preventing cell phone intrusion and theft using biometrics. In: 2013 IEEE Security and Privacy Workshops; 2013. p. 173–80. doi:10.1109/SPW.2013.19.
Primo A, Phoha VV, Kumar R, Serwadda A. Context-aware active authentication using smartphone accelerometer measurements. In: 2014 IEEE Conference on Computer Vision and Pattern Recognition Workshops; 2014. p. 98–105. doi:10.1109/CVPRW.2014.20.
Rong L, Jian-zhong Z, Ming L, Xiang-feng H. A wearable acceleration sensor system for gait recognition. In: 2007 2nd IEEE Conference on Industrial Electronics and Applications; 2007. p. 2654–9.
Saevanee H, Clarke N, Furnell S, Biscione V. Continuous user authentication using multi-modal biometrics. Comput. Secur. 2015;53(C):234–46. doi:10.1016/j.cose.2015.06.001.
Sai Ram VS, Kayastha N, Sha K. In: UHCL Technical Report 2020-01. OFES: Optimal Feature Evaluation and Selection for Multi-Class Classification; 2020.
Sha K, Kumari M. Patient identification based on wrist activity data. In: Proceedings of the 2018 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies; 2018. p. 29–30. doi:10.1145/3278576.3278590.
Su X, Tong H, Ji P. Activity recognition with smartphone sensors. Tsinghua Sci. Technol. 2014;19(3):235–49. doi:10.1109/TST.2014.6838194.
Sugimori D, Iwamoto T, Matsumoto M. A study about identification of pedestrian by using 3-axis accelerometer, Vol. 2; 2011. p. 134–7. doi:10.1109/RTCSA.2011.64.
Suh GE, Devadas S. Physical unclonable functions for device authentication and secret key generation. In: Proceedings of the 44th Annual Design Automation Conference. New York, NY, USA: Association for Computing Machinery; 2007. p. 9–14. doi:10.1145/1278480.1278484.
Sun H, Yuao T. Curve aligning approach for gait authentication based on a wearable accelerometer. Physiol. Meas. 2012;33:1111–20. doi:10.1088/0967-3334/33/6/1111.
Syed Idrus SZ, Cherrier E, Rosenberger C, Bours P. Soft biometrics for keystroke dynamics: profiling individuals while typing passwords. Comput. Secur. 2014;45:147–55. doi:10.1016/j.cose.2014.05.008. https://www.sciencedirect.com/science/article/pii/S0167404814000893
Tan W, Hsu J, Pinn F. In: US Patent App. 09/792,785. Method and System for Token-Based Authentication; 2001.
Thang HM, Viet VQ, Dinh Thuc N, Choi D. Gait identification using accelerometer on mobile phone. In: 2012 International Conference on Control, Automation and Information Sciences (ICCAIS); 2012. p. 344–8. doi:10.1109/ICCAIS.2012.6466615.
Vacca JR. Biometric Technologies and Verification Systems. USA: Butterworth-Heinemann; 2007.
Vural E, Simske S, Schuckers S. Verification of individuals from accelerometer measures of cardiac chest movements. In: 2013 International Conference of the BIOSIG Special Interest Group (BIOSIG); 2013. p. 1–8.
Windows hello face authentication [online]. 2017. https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-face-authentication.
Wildes RP. Iris recognition: an emerging biometric technology. Proc. IEEE 1997;85(9):1348–63. doi:10.1109/5.628669.
Xu H, Liu J, Hu H, Zhang Y. Wearable sensor-based human activity recognition method with multi-features extracted from Hilbert-Huang transform. Sensors 2016;16(12):2048. doi:10.3390/s16122048.
Yang C, Liang D, Chang C. A novel driver identification method using wearables. In: 2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC); 2016. p. 1–5. doi:10.1109/CCNC.2016.7444722.
Yang W, Wang S, Hu J, Zheng G, Chaudhry J, Adi E, Valli C. Securing mobile healthcare data: a smart card based cancelable finger-vein bio-cryptosystem. IEEE Access 2018;6:36939–47. doi:10.1109/ACCESS.2018.2844182.
Zhang H, Hu D. A palm vein recognition system, Vol. 1; 2010. p. 285–8. doi:10.1109/ICICTA.2010.425.

Vallam Sudhakar Sai Ram is currently a Master student of Computer Science at University of Houston-Clear Lake. His research interests include Big Data Analysis, Internet of Things, Healthcare Systems, and Machine Learning.

Namrata Kayastha is currently working as a Computer Systems Engineer. She got her Bachelor's degree in Computer Science from University of Houston-Downtown and Master's degree in Computer Information Systems with focus in Data Science from University of Houston-Clear Lake. Her research interests include Affective Computing, Big Data Analytics, Internet of Things, Computer Vision, and Machine Learning.

Dr. Kewei Sha is an Associate Professor of Computer Science and the Associate Director of the Cyber Security Institute at the University of Houston-Clear Lake (UHCL). Before he moved to UHCL, he was the Department Chair and Associate Professor in the Department of Software Engineering at Oklahoma City University (OCU). He received his Ph.D. degree in Computer Science from Wayne State University in 2008. His research interests include Network Security and Privacy, Internet of Things, Distributed Computing, and Data Management and Analytics. As a PI or co-PI, he received more than 3 million dollars of research support from NSF, UHCL, and OCU. Dr. Sha has published numerous publications in prestigious peer-reviewed journals and conferences. These publications have been cited more than 1300 times. Dr. Sha has served as editors in several prestigious journals, key organizing committee members for many conferences, and reviewers for numerous IEEE and ACM Transactions. Dr. Sha is a recipient of UHCL President's Outstanding Research Award, IEEE Outstanding Leadership Award, and Albert Nelson Marquis Lifetime Achievement Award. He is a senior member of both ACM and IEEE.