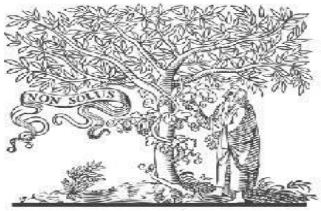
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 05th Apr 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 04

10.48047/IJIEMR/V12/ISSUE 04/138

Title LiSA-G: AUTHENTICATE AND IDENTIFY USERS ON THE WIDELY AVAILABLE COMMERCIAL SMARTWATCHES

Volume 12, ISSUE 04, Pages: 1077-1084

Paper Authors

Dr. Bagam Laxmaiah, Neelam Priyansha, Pasumarthi Prashanthi, Zeba Unnissa.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

LiSA-G: AUTHENTICATE AND IDENTIFY USERS ON THE WIDELY AVAILABLE COMMERCIAL SMARTWATCHES

1. **Dr. Bagam Laxmaiah,** Associate Professor, Department of CSE, CMR Technical Campus, Kandlakoya, Medchal, Hyderabad, India, laxmaiah.cse@cmrtc.ac.in
2. **Neelam Priyansha**, Department of CSE, CMR Technical Campus, Kandlakoya, Medchal, Hyderabad, India, neelampriyansha01@gmail.com
3. **Pasumarthi Prashanthi**, Department of CSE, CMR Technical Campus, Kandlakoya, Medchal, Hyderabad, India, prashanthiprashu1460@gmail.com
4. **Zeba Unnissa**, Department of CSE, CMR Technical Campus, Kandlakoya, Medchal, Hyderabad, India, zebaunnissa10@gmail.com

ABSTRACT: We are able to quickly screen human activities, many of which are oblivious or subliminal, with the abundance of wearable Internet of Things equipment that is currently available. Surprisingly, a number of these activities offer the possibility of removing relevant features for client inspection and present distinct instances for each user. One of the most common and significant of these activities is strolling. The stride, which is an illustration of appendage motions while moving forward, could be used as a biometric trademark for client-recognisable evidence by taking into account each person's unique walking style. We present LiSA-G, a cost-effective smartwatch-based gait-based seamless authentication system that can identify and verify users. In contrast to previous research, the method we propose separates factual characteristics and human-activity-associated elements from aggregated sensor data to provide a more accurate and genuine picture of various instances. Notwithstanding requiring less qualities and sensor data, our preliminary outcomes exhibit that our construction beats past works with regards to confirmation accuracy (a average equal error rate (EER) of 8.2%). Our idea can be implemented more quickly and easily by wearable IoT devices with limited processing power and battery capacity.

Keywords *– User authentication, gait, wearable device, Internet of Things, machine learning.*

1. INTRODUCTION

The Internet of Things (IoT) has changed various systems as well as how people cooperate with PCs and correspondence associations. In addition to the prevalent mobile phones, the number of wearable IoT devices, such as smartwatches, smartglasses, and so on, is rapidly rising. In 2019, we will sell 225 million wearable IoT devices worldwide, according to Gartner Inc. [1]. While the initial wearable devices only had limited connectivity, such as Bluetooth, the latest models include a number of communication modules, such as WiFi, as well as a variety of sensors. However, a large number of connectives on wearable devices could reveal a wide range of personal data and increase the potential for safety breaches [2], necessitating extensive security measures. Regrettably, quantitative results have lagted behind mindfulness regarding wearable IoT device security concerns. Wearable IoT devices are more vulnerable to a variety of security threats than previous IoT devices, such as mobile phones, due to a lack of security measures (such as inadequate client authentication) and limited assets. such as the power and energy limitations). Programmers, for instance, were able to remotely enter Google Glass

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

frameworks in 2013 in order to monitor and record customer actions [3]. A 2015 HP investigation found that all smartwatches have security flaws [4].

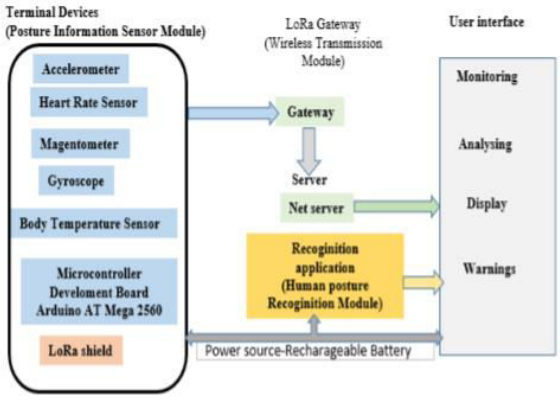


Fig.1: Example figure

Consequently, we view client validation as one of the primary security methods for addressing the shortcomings of the current wearable IoT security framework. Due to their simplicity, passwords are one of the most widely used client verification methods. To obtain a certain level of strength for confirmation, customers must regularly store at least 19 distinct passwords for their various devices and services [5]. As a result, it's usually hard for people to remember the right mystery state. Hidden word indignation was experienced by 33% of study participants, according to a Centrify survey conducted at Infosecurity Europe 2015 [6].

2. LITERATURE REVIEW

Leveraging semantic transformation to investigate password habits and their causes:

It is an irrefutable reality that buyers battle to create and recollect safe passwords, especially when provoked to pick various passwords for various records. Although research has shed light on the flaws and reuse of secret keys, little is known about the mental processes that clients go through when engaging in difficult secret key practices. We might be able to make better arrangements that complement rather than hinder client behaviors if we are aware of these cognitive processes. We conduct in-depth customer research by collecting and analyzing clients' genuine passwords and the motivations behind their secret word creations. We can thus compare actual customer behavior to their objectives. We discovered that client goals frequently diverge from training, and that this, in addition to specific comfort and false perceptions, keeps dangerous covert word rehearsals going. Our findings quickly demonstrate that clients sacrifice security for memorability when creating passwords and that there is a gap between client logic and practice.

An empirical study of touch-based authentication methods on smartwatches:

Smartwatches give new difficulties to information security. While touch-based confirmation systems for mobile phones are well-established, their application to smartwatches is still unknown. To find out how validation procedures (PIN and Example), user interfaces (Square and Round), and display widths (38mm and 42mm) affect confirmation accuracy, speed, and security, a 16-person customer survey was completed. For smartwatches with fewer UI components, round UIs are designed. The outcomes demonstrate this: 1) PIN is quicker and more precise than Example; 2) Model is a lot quicker than PIN; 3) Roundabout UIs are more precise than square UIs, but they are safer. 4) While show size has no effect on accuracy or speed, it does have a significant effect on security; 5) The Square PIN method is the most secure for everyone. There is also a security issue with the assessment: The preferred strategy of the members fails every test. Last but not least, we

discuss the implications for future plans for touch-based smartwatch confirmation.

Spoof attacks on gait authentication system:

Biometric gait recognition research has advanced. Past work on step conspicuous proof had strong discoveries, yet with a little example size. A couple of bigger scope tests show step's full capacity as a biometric from which individuals might be recognized. The issue of stride vulnerability to assaults has received little attention despite widespread interest in step distinguishing evidence. Using stride biometrics, this study compares the closest individual attack to the minimal exertion pantomime attack. Our method uses an accelerometer sensor attached to people's hips to record each step, in contrast to the majority of previous stride identifying evidence frameworks, which record walk from a decent position using a (camcorder). For obvious confirmation, hip speed expansion in three even bearings—up-down, forward-backward, and sideways—is used. 760 step groupings were received from 100 distinct individuals. The first round consisted of two sections. People walked a lot in the first half, and they found that the cycle method fixed an EER of about 13% at its middle value. People attempted to walk like other people at the next location. A low-effort pantomime assault on walk biometric does not always increase the likelihood of identifying a faker, according to FAR botches. On the other hand, aggressors who have access to the data set from their closest individual may pose a significant threat to the validation system.

Gait-based authentication using a wrist-worn device:

Everyone walks in a different way. As a result, step might turn into a significant part of biometric processes pointed toward validating as well as distinguishing the client of a wearable gadget. A straightforward authentication strategy based on the user's wrist-registered acceleration is presented in this paper. A collection of acceleration-based features are used to detect anomalies to determine whether the device is being worn by a new user, an impostor, or a thief after learning the user's normal stride pattern in the beginning. The method was put to the test with a success rate of 15 participants and an equal error rate of 2.9%. A wrist-worn device appears to be capable of precise stride-based validation, as shown by our findings. Also compared is a similar procedure that was carried out on a pocket-worn device.

Performance of gait authentication using an acceleration sensor:

Wearable sensors are turning out to be generally perceived for empowering an assortment of sensor-based applications as ICT and MEMS development progress. A step verification method using wearable sensors, a type of biometric validation, is shown in this study. Gaint development in daily existence is both novel and undeniable. The examples of speed increase values provided by walking vary from person to person. We anticipate that the continuous walk data gathered by wearable sensors will be the basis for the development of a variety of new services. We evaluate each person's individual walk limits using data from a wearable sensor. A wearable sensor was placed on the right lower thigh of each participant. A confirmation calculation is proposed and assessed. The characteristics that enable solid separation ought to serve as the basis for the validation computation. Consequently, our validation framework makes use of the increased voyaging speed during the swing stage. According to the

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

findings, the EER increased by 20% when the maximum value was raised to 1700.

3. METHODOLOGY

In this paper, the author presents a method for validating customers based on data from smart devices like wellness monitoring sensors, smart watches, personal digital assistants (PDAs), and smart glasses. Sensitive customer data, such as diseases, personal information, or banking passwords, may be saved by each clever gadget sensor. Already, passwords were utilized to forestall unapproved access, and just those clients who had passwords could open savvy gadgets and access information. However, consumers are unable to memorize all of their passwords in today's computerized environment, where a single person can use multiple great devices. The creator used "Accelerometer and Gyroscope Sensor Information" instead of passwords to solve this problem. Sensor information includes client appendage development data based on client walking and sitting instances. The author asserts that individual walking and sitting patterns can be used to identify individuals. Therefore, users may be permitted without having to learn any passwords by utilizing sensor patterns.

By comparing collected photos with real-time traffic data to a reference image of an empty route, this paper offers a method for determining traffic density. Because it serves the purpose of our confirmation framework, which is to transmit reliable and simple check, we consider stride, an example of appendage movements during progress, among other subconscious workouts. For instance, it has been discovered that even individuals with identical physical characteristics exhibit distinct examples of gait, and walking is perhaps the most straightforward and common activity that requires exceptional effort to imitate.

Advantages:

1) The user will request that the sensor record his walking and sitting habits after registering with the smart devices.

2) MEAN and Standard Deviation will be used to analyze the sensor-generated data from the gyroscope and accelerometer. This dataset will receive the user id.

3) The delivered information will be shown utilizing various ML procedures, like random forest, KNEAREST Neighbors, and Multi-layer Perceptron Calculation. Random Forest outperforms the other two methods when it comes to user authentication accuracy.

4) A model representing all of the trained data will be kept.

5) When the same user or a new one tries to access a smart device, the device will ask the user to go for a walk, use the accelerometer and gyroscope to record how he walks, and then use the data.

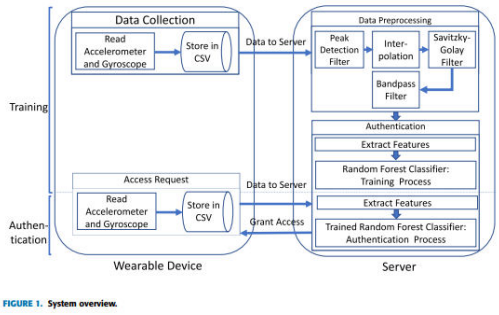


FIGURE 1. System overview.

Fig.2: System architecture

MODULES:

In order to finish the project that was just described, we created the modules that are listed below.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

- Upload Accelerometer and Gyroscope Sensor Dataset
- Create Train test model
- Run KNN algorithm
- Run Random forest method
- Run Multilayer perceptron algorithm
- Accuracy graph

4. IMPLEMENTATION

ALGORITHMS:

KNN:

One of the most essential sorts of machine learning (ML) calculations is the KNN, and it is every now and again used for request. It orchestrates the data directs arranged by nearness toward each other. KNN sorts out new data guides in light of the fact that they are so like applicable information that has been put away before. Tomatoes and bananas might be remembered for the dataset. K Nearest Neighbor is an immediate computation that stays aware of up with each continuous model and get-togethers pushing toward data or models considering a resemblance rule. It is every now and again used to order a data point in view of its neighbors' attributes.

RANDOM FOREST:

A controlled ML procedure known as an Random Forest Computation is as often as possible used in ML for Portrayal and Backslide applications. We know that there are a great deal of trees in a woods, and the more trees there are, the better the woodland gets. Random Forest makes no suppositions in regards to the appropriation of the information. Subsequently, information changes are normally insignificant. With high-layered datasets, the random forest strategy can perform well since it utilizes irregular element picks. a huge dataset with a great deal of highlights).

MULTILAYER PERCEPTRON:

Controlled learning troubles, computational neuroscience, and equivalent appropriated enlistment research all utilize Multi-Layer Perceptrons. Talk acknowledgment, picture acknowledgment, and machine understanding are instances of models. There should be something like one mystery layer in a Multi-layer Perceptron (MLP). with the exception of a solitary outcome and data layer). A single layer perceptron can get immediate capacities, yet a multi-layer perceptron can moreover learn underhanded limits.

Advantages of the Multi-layer Perceptron Model:

- A multilayered perceptron model could be used to deal with difficult non-direct challenges.
- It functions effectively with both small and large amounts of input data.
- After training, it lets us make quick projections.
- With both large and small data sets, it helps achieve the same accuracy ratio.

5. EXPERIMENTAL RESULTS

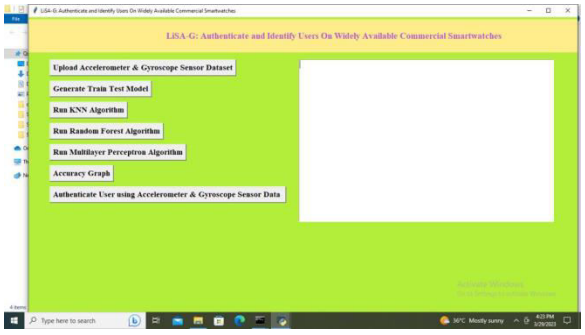


Fig.3: Home screen

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

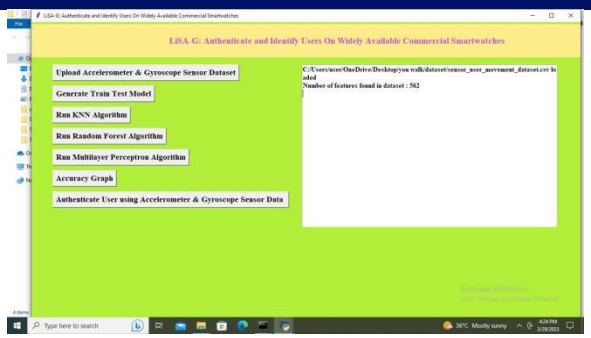


Fig.4: Upload Accelerometer & Gyroscope Sensor Dataset

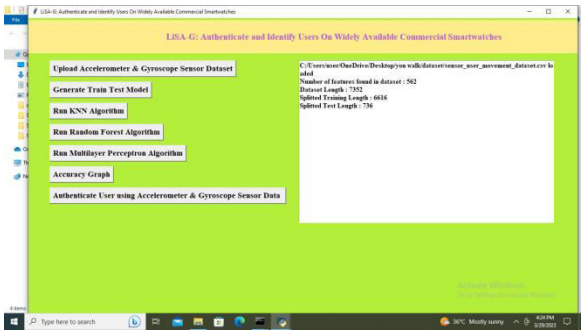


Fig.5: Generate Train Test Model

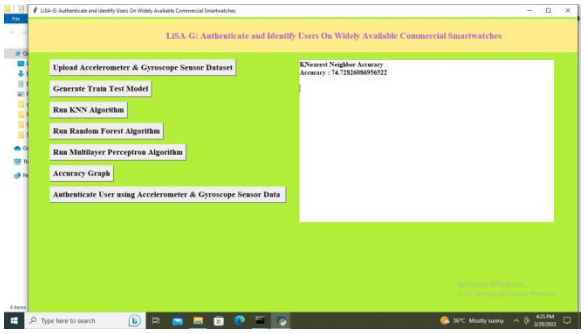


Fig.6: Run KNN Algorithm

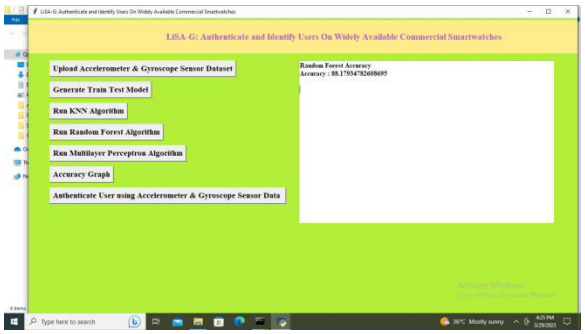


Fig.7: Run Random Forest Algorithm

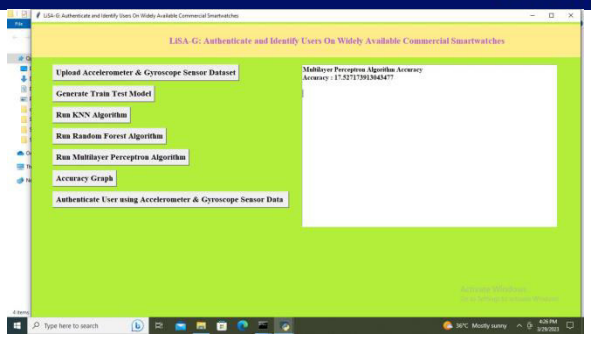


Fig.8: Run Multilayer Perceptron Algorithm

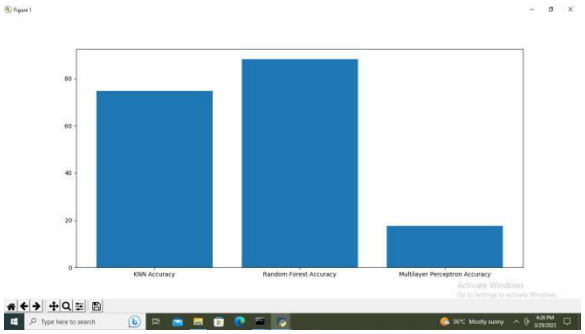


Fig.9: Accuracy graph

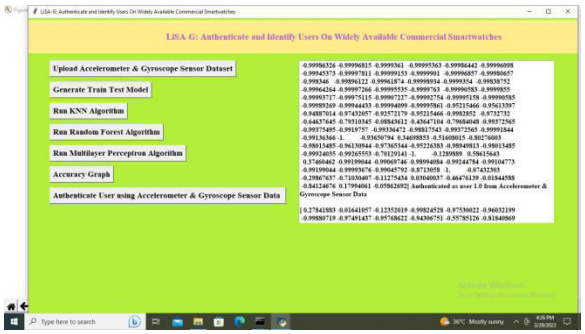


Fig.10: Authenticate User using Accelerometer & Gyroscope Sensor Data

6. CONCLUSION

Persons can be effectively authenticated using walking patterns like arm swings while walking. In this study, we proposed LiSA-G, a novel step-based verification framework that is reliable, easy to use, and simple to implement. Our framework may order clients with greater accuracy (91.8% success rate) and with fewer highlights than previous current investigations by distinguishing a remarkable mix of characteristics relevant to human behavior views.

Because it utilizes low-cost smartwatches, the proposed structure is quick to set up and easy to use. Additionally, it capitalizes on customers' existing activities.

7. FUTURE WORK

By omitting the step-by-step identification method and making use of significantly less information, the proposed structure is intended to be lightweight in light of the IoT ecosystem's limited resources. We anticipate that the proposed structure will effectively link with other frameworks to provide comprehensive confirmation and will make it easier to arrange consistent validation.

ACKNOWLEDGEMENT

We thank CMR Technical Campus for supporting this paper titled “LiSA-G: Authenticate and Identify Users On The Widely Available Commercial Smartwatches”, which provided good facilities and support to accomplish our work. Sincerely thank our Chairman, Director, Deans, Head Of the Department, Department Of Computer Science and Engineering, Guide and Teaching and Non- Teaching faculty members for giving valuable suggestions and guidance in every aspect of our work.

REFERENCES

[1] S. Draper. (Dec. 2018). Wearable Device Sales Will Grow 26 Percent Worldwide in 2019, Says Research Company Gartner. Accessed: Feb. 1, 2019.[Online]. Available: https://www.wearabletechnologies.com/2018/12/wearable-device-sales-will-grow-26-percentworldwide-in-2019-says-research-company-gartner/

[2] T. Micro. (Mar. 2018). Are your Wearables Fit to Secure You? Researchers Outline 3 Attack Surfaces. [Online]. Available: https://www.trendmicro.com/vinfo/ph/security/news/internet-of-things/are-yourwearables-fit/-to-secure-you-researchers-outline-3-attack-surfaces

[3] M. Prigg. (May 2013). Google Glass Hacked to Transmit Everything You See and Hear: Experts Warn ’the Only Thing it Doesn’t Know are Your Thoughts. [Online]. Available: http://www.dailymail.co.uk/sciencetech/article-2318217/Google-Glass-HACKED-transmithear–experts-warn-thing-doesnt-know-thoughts.html

[4] K. Rawlinson. (Jul. 2015). Hp Study Reveals Smartwatches Vulnerable to Attack. [Online]. Available: http://www8.hp.com/us/en/hp-news/pressrelease.html?id=2037386

[5] S. Faris. (Jul. 2016). Do You Suffer From Password Rage?.[Online]. Available: http://theweek.com/articles/637588/suffer-from-password-rage

[6] J. Chatzky. (May 2017). Password Rage, it’s a Thing. [Online]. Available: https://lifelockunlocked.com/tips/password-rage-thing/

[7] A. Hanamsagar, S. S. Woo, C. Kanich, and J. Mirkovic, ‘‘Leveraging semantic transformation to investigate password habits and their causes,’’ in Proc. CHI Conf. Hum. Factors Comput. Syst., 2018, p. 570.

[8] Y. Zhao, Z. Qiu, Y. Yang, W. Li, and M. Fan, ‘‘An empirical study of touch-based authentication methods on smartwatches,’’ in Proc. ACM Int. Symp. Wearable Comput. (ISWC), New York, NY, USA, 2017, pp. 122–125. [Online]. Available: http://doi.acm.org.proxy.library.stonybrook.edu/10.1145/3123021.3123049

[9] J. Myerson. (Mar. 2017). How to Fool a Fingerprint Sensor. [Online]. Available: https://www.electronicproducts.com/Mobile/Devices/How_ to_fool_a_fingerprint_sensor.aspx

[10] S. Khandelwal. (Mar. 2015). Hacker Finds a Simple Way to Fool Iris Biometric Security Systems. [Online]. Available: https://thehackernews.com/2015/03/iris-biometric-security-bypass.html

[11] D. Gafurov, E. Snekkenes, and P. Bours, ''Spoof attacks on gait authentication system,'' IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 491–502, Sep. 2007.

[12] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikäinen, J. Bustard, and M. Nixon, ''Can gait biometrics be spoofed?'' in Proc. 21st Int. Conf. Pattern Recognit. (ICPR), Nov. 2012, pp. 3280–3283.

[13] (Sep. 2018). It's the Era of the Smartwatch: Idc Says Device to Rule Nearly Half of Wearables by 2022. Accessed: Mar. 1, 2018. [Online]. Available: https://economictimes.indiatimes.com/magazines/panache/its-the-eraof-the-smartwatch-idc-says-device-to-rule-nearly-half-of-wearables-by2022/articleshow/65810524.cms

[14] G. Cola, M. Avvenuti, F. Musso, and A. Vecchio, ''Gait-based authentication using a wrist-worn device,'' in Proc. 13th Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services (MOBIQUITOUS), New York, NY, USA, Nov. 2016, pp. 208–217.

[15] S. Terada, Y. Enomoto, D. Hanawa, and K. Oguchi, ''Performance of gait authentication using an acceleration sensor,'' in Proc. 34th Int. Conf. Telecommun. Signal Process. (TSP), Aug. 2011, pp. 34–36.