*Section A-Research paper*
**ISSN 2063-5346**

# DESIGN AND ANALYSIS ON LIGHTWEIGHT SEAMLESS AUTHENTICATION BASED ON GAIT IN WEARABLE IOT SYSTEMS

**R.Sreedhar**
**Associate Professor, Department of IT**
**Sridevi Women's Engineering College, Telangana**
**rachasreedharswec@gmail.com**

**B.Aishwarya**
**Btech Student, Department of IT**
**Sridevi Women's Engineering College, Telangana**
**aishwaryabarvadhi@gmail.com**

**B.Bhargavi**
**Btech Student, Department of IT**
**Sridevi Women's Engineering College, Telangana**
**rbhargavi427@gmail.com**

**M.Akhila**
**Btech Student, Department of IT**
**Sridevi Women's Engineering College, Telangana**
**mangaakhila04@gmail.com**

## ABSTRACT

Biometric systems are gaining importance because they are more trustworthy and efficient for identity verification. Gait is one such biometric. The manner in which a person walks is referred to as gait. It is locomotion accomplished by the movement of a person's limbs. Unlike other methods, gait is a behavioural biometric that is considered for user authentication because it reveals unique patterns for each individual. In addition, the fact that this biometric technique is less intrusive to the user makes it superior to others. This survey focuses on various gait approaches, applications, and machine learning techniques that will be used for classifying gait characteristics and their applications.

Keywords— Gait, Gait Approaches, Gait Dataset, Gait Features, Machine Learning Techniques, Deep Learning Techniques, Gait Applications.

## 1. INTRODUCTION

In the context of information security, "biometric confirmation" refers to a procedure that relies on the unique biological traits of an individual in order to identify the user. The biometric information that was taken is compared and verified with the actual information that is stored in a database by biometric verification frameworks. Because a person's biometric traits cannot be easily shared, misplaced, or copied, biometric recognition creates a robust interface between the individual and his character.

Therefore, biometric recognition is naturally more prevalent and secure than the tactics of personal identification numbers (PIN), passwords, and tokens. These techniques are susceptible to several attacks, so you will need to remember them. Other typical biometric approaches, such as face detection, iris matching, and fingerprint identification, are affected by a variety of environmental factors, need integration and additional hardware, and necessitate that the user be present during the authentication process. A biometric that is based on gait is taken into consideration so that these problems can be solved.

Gait is the pattern of steps that are taken in succession while walking. The results of medical research indicate that each person has a distinct walking pattern, known as gait. Walking is a common and natural process; yet, when it is used as a criterion for authentication, it transforms into a complicated phenomenon [1].

Although the first wearable devices were only equipped with a limited amount of connectivity, such as Bluetooth, the most recent wearable devices are equipped with a variety of communication modules, such as WiFi, as well as a wide range of sensors. However, wearable devices with various connectives might expose a range of personally identifiable information and substantially raise the danger of security breaches [2], which is why comprehensive security measures are required.

The attention paid to the security implications of wearable Internet of Things devices has not, however, kept pace with the quantitative increase of these devices. When compared to the preceding Internet of Things devices, such as smartphones, wearable Internet of Things devices are more susceptible to a variety of security attacks. This is due to the absence of security mechanisms (for example, insufficient user authentication) and restricted resources (for example, computational power and energy capacity). For instance, in 2013, hackers were able to remotely access Google Glass networks in order to monitor and record everything that users did while wearing the device [3]. A study that was carried out by HP in 2015 indicated that every single smartwatch has the potential to be breached by malicious actors [4].

Consequently, in order to address the vulnerability of the existing security system for wearable Internet of Things devices, we take into consideration user authentication, which is one of the most fundamental security measures. Because it is so easy to do so, the usage of passwords is one of the user authentication methods that is utilised the most frequently. However, in order to obtain a particular level of robust user authentication, users need save a minimum of 19 distinct passwords on average for their many devices and services [5]. As a consequence of this, a lot of people struggle to correctly recall their passwords. According to the results of a survey that Centrify carried out at Infosecurity Europe 2015, 33 percent of the people who took part in the study experienced "password rage" [6].

## 2. LITERATURE REVIEW

Machine vision is an image-based technology that uses cameras to capture images for the purpose of doing automatic analysis and identification of people. When we take this method, we are concentrating on the angles that are visible from the outside. It is perfectly adapted for offering indeed a long distanced acknowledgment of an individual, which is a role that no other biometric approach has been able to fulfil. Data is acquired through the use of automated cameras, and then various signal, picture processing algorithms, and machine learning calculations are utilised for the goal of recognition and confirmation.

Gait is the pattern of steps that are taken in succession while walking. The results of medical research indicate that each person has a distinct walking pattern, known as gait. Walking is a common and natural process; yet, when it is used as a criterion for authentication, it transforms into a complicated phenomenon [1].

In this method, the model-free and model-based research areas [2, as indicated in figure 1] are the two primary research domains to focus on. In some circles, the model-free method is also referred to as the silhouette-based approach. Because of this, the human form can be inferred by separating the individual from their environment. Once this has been accomplished, the human form can be acknowledged by examining how the form shifts throughout the course of time.

The model-based method is another option available within the realm of machine vision. In this tactic, a mathematical model is tailored to human movement by extracting features from walking patterns and then using those features to match the model. It is composed of two submodels: one represents the fundamental views of walking, and the other describes the kinematics of movement. Because there is no mediation provided by clothing or any other things, this tactic is more advantageous than the model-free technique. However, it is difficult to carry out since it necessitates a higher level of computational control compared to the model-free method.

Elrefaei et al. [3] have developed a gait-based biometric system using a fuzzy basis for machine vision. The suggested system is then put through its paces utilising databases from CMU MoBo and CASIA A. These are datasets that are accessible to the general public. After the walk highlights have been extracted from the gait photos utilising the local ternary pattern (LTP) concept, the average of one whole walk cycle utilising the gait energy image (GEl) concept has then been determined.

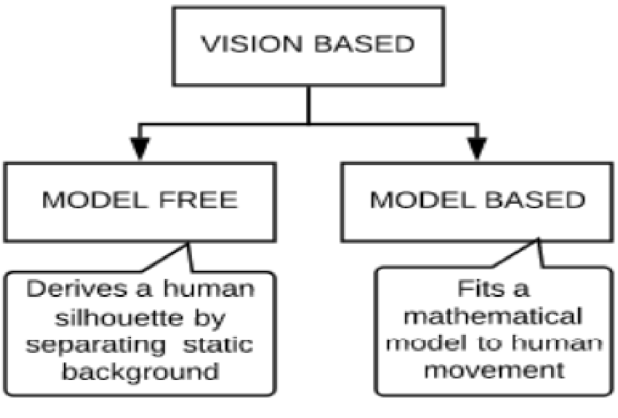

VISION BASED
MODEL FREE
MODEL BASED
Derives a human silhouette by separating static background
Fits a mathematical model to human movement

Fig. 1. Classification of vision based model

In their research, Tao et al. [4] utilised a MEMS inertial sensor to collect data, which was subsequently applied to the process of user authentication. These miniature sensors are affixed to the smart shoes, and once activated, they will gather the signals and send them to the server. This information was gathered in an office setting with 22 participants, who were each given the instruction to walk 20 times in a row.

The dataset was obtained by ISIR at Osaka University (OU), and it is available to the general public. Gadaleta et al. [5] used this dataset. It includes data gathered from 744 individuals through the use of three inertial sensors, including a gyroscope and a tri-axial accelerometer.

Shen et al.[6] have obtained their results by using an Android smartphone that is equipped with both a gyroscope and an accelerometer. It is made up of seven attributes, one of which is a timestamp value. Other attributes include three axes of an accelerometer and a gyroscope. A total of ten participants took part in the process of collecting the data and were given the task of performing five everyday activities, which included moving the phone into five distinct postures.

## 3. METHODOLOGY

### Sensor Based Approach

In this method, people are identified by sensors that are either attached to their bodies or they are required to walk on sensor-monitored flooring, from which data is collected.These two strategies are illustrated in Figure 2. This strategy provides an additional benefit, which is the capability to carry out authentication in a continuous manner, which is not possible with fixed sensors or cameras. A large number of sensors are utilised in order to record the various stride combinations. Electromyography is a technique that records the movement of a muscle while the subject is engaged in a variety of activities. At that moment, these signals are utilised in order to discover various treatment deviations from the norm. An accelerometer measures force along each of its axes, a gyroscope measures angular velocity in relation to the body's axis, and a magnetometer provides information regarding orientation in relation to magnetic north and south. GRF plates, also known as force plates, are measuring instruments that are used to determine the forces that are generated by an individual while they are moving across or standing on the plates.

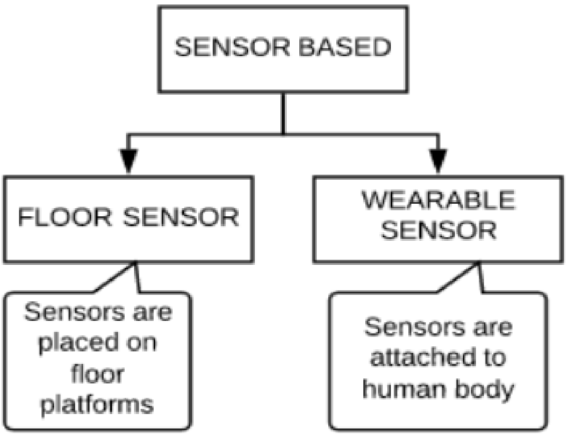

SENSOR BASED
FLOOR SENSOR
WEARABLE SENSOR
Sensors are placed on floor platforms
Sensors are attached to human body

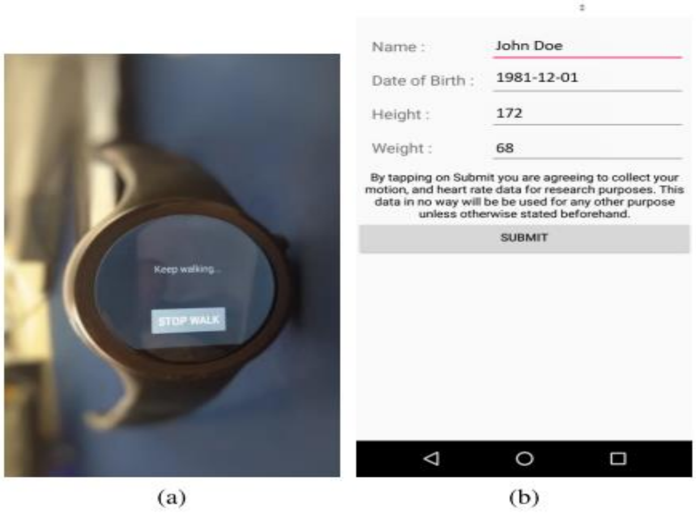
Fig. 2. Classification of sensor based model

ISSN 2063-5346

## DATA COLLECTION

We designed two Android applications, one for smartwatches and one for smartphones, so that we could collect behavioural data from users. These applications run on Android devices. Because the smartwatches we utilised in this experiment only had Bluetooth connectivity, we had to couple a smartphone and a wristwatch together in order for the smartphone to function as an access point and transmit the sensor data stream recorded in the smartwatch to the remote server. This was accomplished by pairing the smartphone and the smartwatch. In order to complete the registration process, customers are required to provide the following fundamental information by way of the custom smartphone application that was developed: 1) the person's name, 2) their birth date, 3) their height, and 4) their weight. Following the completion of the submission, the application for the smartwatch displays a button that can be pressed to begin recording the sensor data. When the button is pressed, the wristwatch starts recording data from the two types of sensors that are present on the smartwatch: 1) an accelerometer, and 2) a gyroscope, both of which operate at a frequency of one hundred hertz (Hz).

Note that our system does not perform any further calibrations in advance. This is because, in practise, people do not manually calibrate their smartphones or smartwatches, thus our system reflects this reality by not performing any more calibrations. In order to record the users' data, they individually walk a distance of around 500 metres using their regular stride. The data from the sensors is saved in the smartwatch in comma-separated values, or CSV, files, and then transmitted via Bluetooth to the smartphone with which it is paired. Following that, the information is transferred from the mobile device to the authentication server. The graphical user interfaces (GUI) of the Android application that was used for data collecting are depicted in Figure 3.



Name : John Doe

Date of Birth : 1981-12-01

Height : 172

Weight : 68

By tapping on Submit you are agreeing to collect your motion, and heart rate data for research purposes. This data in no way will be be used for any other purpose unless otherwise stated beforehand.

(a) (b)

FIGURE 3. Android applications for data collection. (a) Smartwatch application. (b) Smartphone application.

## DATA PREPROCESSING

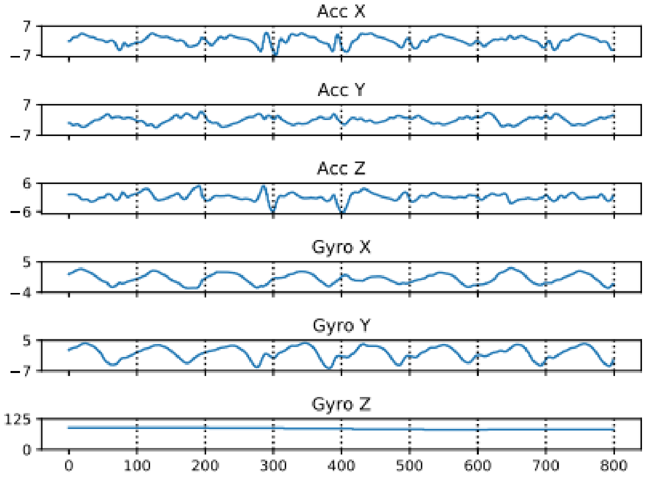


FIGURE 4. Sensor data collected from an user.

The data preprocessing procedure involves cleaning and refining the raw sensor data obtained from smartwatches. This is necessary since the raw sensor data may contain unwanted noise if it is not calibrated first. In order to have a better understanding of how to analyse the data, the raw sensor data are initially visualised before the preprocessing step is carried out. As can be seen in Figure 4, we were able to determine that the data patterns repeat themselves after roughly one hundred samples, which we can interpret as an arm swing. Several of the data sequences, however, present values that are not normal.

## CONCLUSION

It is possible to verify people by analysing their walking patterns, such as the way they swing their arms when walking. Within the scope of this study, we suggested a novel gait-based authentication framework known as LiSA-G. This framework is dependable, user-friendly, and simple to implement. Our framework can categorise users with a greater accuracy (91.8% success rate) than other current works while utilising less number of features. This is made possible by the extraction of a new combination of characteristics that are related to the human behavioural aspects. The proposed framework is user-friendly because it capitalises on the routine behaviours of users, and it is easily deployable because it makes use of smartwatches that are currently on the market. The suggested framework is designed to be lightweight in consideration of its applicability to the IoT ecosystem, which has restricted resources. This is accomplished by removing the gait cycle detection procedure and making use of a much reduced amount of data. We anticipate that the framework that has been proposed will be able to contribute to the provision of seamless authentication and will be easily connected with other systems in order to enable multi-factor authentication.

## 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:

1

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.htm