

Plantar Biometrics for Edge Computing

Mads Stege
Technical University of Denmark
Copenhagen, Denmark
s165243@student.dtu.dk

Charalampos Orfanidis
Technical University of Denmark
Copenhagen, Denmark
chaorf@dtu.dk

Xenofon Fafoutis
Technical University of Denmark
Copenhagen, Denmark
xefa@dtu.dk

ABSTRACT

Biometric systems are getting integrated into our daily life as the needs for authentication are increased rapidly. In smartphones fingerprint and face identification are used already widely as a method for user authentication. A relatively novel area of biometrics is the usage of plantar biometrics, foot sole features, to verify human identities. There are several approaches to utilise plantar biometrics but most of the proposed approaches require bulky, obtrusive or an immobile design. In this paper, we introduce a unobtrusive biometric system based on a shoe wearable, which is able to authenticate individuals with the assistance of Neural Network Classifier. The implemented system is evaluated on 10 individuals achieving 94.3% accuracy with a loss of 1.87. Furthermore, the learning and authentication part takes place on the edge which has numerous benefits towards the performance but also the security aspects of the system.

CCS CONCEPTS

• **Human-centered computing** → **Ubiquitous and mobile computing**; • **Computer systems organization** → **Embedded systems**; • **Security and privacy** → **Biometrics**.

KEYWORDS

authentication, biometrics, plantar data, embedded systems

ACM Reference Format:

Mads Stege, Charalampos Orfanidis, and Xenofon Fafoutis. 2022. Plantar Biometrics for Edge Computing. In *Workshop on Body-centric Computing Systems (BodySys '22)*, July 1, 2022, Portland, OR, USA. ACM, New York, NY, USA, 6 pages. <https://doi.org/10.1145/3539489.3539589>

1 INTRODUCTION

Digitalization is the procedure to convert information in digital form which is beneficial towards multiple applications. In business and industry for instance, digitalization is applied to automate processes, monitor the production and several other purposes which will assist and increase the production [6]. Beside industry, digitalization started being integrated in daily life. Managing bank accounts, paying monthly bills, daily money transactions that substitute paper and coin currency, travel documents, Covid-19 certificates and passports, all these examples can be managed using

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

BodySys '22, July 1, 2022, Portland, OR, USA

© 2022 Association for Computing Machinery.

ACM ISBN 978-1-4503-9402-4/22/07...\$15.00

<https://doi.org/10.1145/3539489.3539589>

mobile devices but they have to authenticate the corresponding user. The last years the fingerprint biometric and the face identification are used widely for authentication by mobile devices and consequently for authenticating users for the aforementioned examples.

A less common area of biometrics is the utilisation of foot biometrics. The plantar pressure, gait pattern and other foot related biomarkers adhere the main properties of biometrics, namely they are characteristics that (almost) every user has, there is a uniqueness in these characteristics [12, 19], they are quantifiable and they are obtained without the user's notice to avoid their influence. The biometric systems, which are designed around foot biomarkers, can be classified into three main classes: sole-based, mat-based and photography-based. The first class includes biometric systems, which use a set of sensors placed on carefully selected areas on the foot sole or around the lower leg. These platforms are mobile, and are to be carried by the user over the course of a workday. Sole-based systems most of the times though are bulky and obtrusive. Mat-based biometric systems use a pressure sensitive mat, often placed at the entrance of a restricted area before allowing access. They are immobile but have a more restrictive platform resulting in better protection against physical tampering [5, 20]. Photography-based approaches use feature extraction, rather than foot pressure, to distinguish between data subjects. They are also immobile and require the use of a (camera) sensor to capture the relevant pieces of information [13, 15].

In this paper we propose a sole-based biometric system based on a shoe wearable which is able to authenticate users using three force sensors mounted under the shoe insole and an accelerometer placed on the heel, from a common Arduino platform [2]. In most of the sole-based approaches, the architecture is such that the obtained raw data (plantar pressure, gait pattern) is transferred to another entity where the authentication process takes place because of the computational burden. The biometric system we propose incorporates the authentication process into the device, using a Neural Network (NN) classifier designed for embedded systems. In that way, the raw data is not compromised. The application scenarios that motivate our approach are organisations and institutes that require different levels of security. For instance, federal institutions, medical research and development, military contractors. Using such a biometric system besides allowing a user to access only authorised regions, a proof authority can verify at any point that the user has the authorisation to be the present region.

In traditional authentication, after a user has been authenticated (using either user credentials, smartcard or biometrics) user authentication is guaranteed only during the login point. Thus, there is gap to ensure security during the period after login to logout of a system. *Continuous authentication (CA)* [19] is an approach able to guarantee user authentication during the whole period of

using a system, by utilising biometric verification. Therefore, CA is associated with foot biometrics as well and in this paper, we illustrate how the proposed biometric system can incorporate this approach.

The rest of the paper is organised as follows: Section 2 presents the state of the art and how the introduced system is related to them. Section 3 describes the system design, the implementation and all the technical details around it. Section 4 illustrates a pilot evaluation we conducted on 10 individuals and Section 5 concludes the paper.

2 RELATED WORK

This section focuses on sole-based biometric systems since this class foot related biometrics is more related to the introduced approach.

Whilst most papers only focus on one type of verification methods and then expanding various iterations of this. However, a small number focused more on biometrics in general, with a sub-discussion on plantar biometrics. One example of this would be Khoker and Singh's survey [14], which focuses on the broader scope of biometrics, herein plantar. This work sheds light on the three types of biometric features, such as the physiological (face, fingerprint, DNA, iris, etc.), the behavioural (voice, signature, key-stroke patterns, etc.) and the "soft" features (height, weight, gender, ethnicity, etc.). Along this approach, the survey goes on to discuss a number of different areas of discourse within the field. Within these expected subjects are the effects of age, the various methods of extractions, and the prospects of multi-modality. Additionally, the difficulties of user acceptance, an increasing societal reliance on varying degrees of biometrics and ultimately, the very limitations of the whole concept is also entertained. The survey rounds up with a brief recap of the different methods, and finishes off with a taste on some of the future prospects of plantar biometrics.

Appropriately titled "I Walk, Therefore I Am", Yeh et al. [19] present a comprehensive overview of the problems typically associated with wearable Internet of Things (IoT) devices, their downsides, and the need for changes in both typical policy and standards of security within the field. They use this introduction to lead into the concept of CA through IoT, and the effectiveness of several biometric verification's towards this approach. Using a Raspberry Pi II and six pressure sensors, their platform used Naïve Bayes and Support Vector Machine (SVM) with Gaussian Radial Basis Function to analyse the data and thereby ultimately generate an authentication token for individual identification and verification. Whilst initial results showed high degrees of verification accuracy (a low False Rejection Rate), it also highlighted a potential for two individuals to score high or even similar scores (a high False Acceptance Rate). This was identified to be caused by the humans themselves, or environment interference. A proposed data purification procedure was implemented to avoid this, and much cleaner results was derived. At worst, the true individual verification rate was 99.40% correct, whilst the closest false individual verification rate was 80% at best.

Describing the concept of a Body Sensory Network (BSN), Ivanov et al. [12] cite an expectation for growing need of biometric footwear to help facilitate this. By using a segmented design, they propose a two-part system, with one part being fastened to the shoe sole and transmitting the data to a central processing system. The argument

is that this design allows for only minimal weight and equipment being installed on the user. Using nine separate sensors and a prior paper on the optimal placement of these [11], the authors investigate four distinct neural network architectures using the previously touched multimodal sensor insoles. They found evidence suggesting that these multimodal sensor-enabled footwear could serve a biometric purpose in the next generation of BSN. With a 70% segmentation overlap, Ivanov et al. were able to reach a mean accuracy of up to $93.3\% \pm 0.009$ with some architectures. Taking a more humble approach to the number of sensors and instead relying on different parameters, Huang et al. [10] propose a different modular system design that only uses four individual force sensors. On the other hand, they remedy this by adding peripheral parameters, such as: the tilt angle, gyroscope readings, a bend sensor, and an accelerometer. Whereas the previous papers solely focused on using force sensors for acquiring their data sets, Huang's team instead focused on broadening their scope of possible data sources. Such sensors can be many times smaller than a regular force sensor. This approach would, after carefully extracting the most valuable data using Principal Component Analysis (PCA) and a SVM to train and classify the data, result in successful recognition rates of about 98%.

Having gone over the various dispositions and results of the peer research, it is evident that they all show great success in authenticating the user through various means. Most of the systems transmit the raw data from the sensors to another entity to perform the authentication process. The potential for an adversary to exploit and potentially infiltrate the systems is both substantial and concerning. The system we propose performs the authentication process onboard and the only data transmitting to another entity is the results. Beside the security aspects, the onboard operation is decreasing the cost and delay introduced by the transmission of the raw data. Moreover, the mentioned approaches often necessitates expensive equipment and materials, or the need for strapping cumbersome hardware onto the data subject. All the while, sacrificing the individual's privacy and ease of daily operations.

3 SYSTEM OVERVIEW



Figure 1: The shoe wearable biometric system, the Arduino board it is attached on the heel of the shoe.

This section elaborates on the technical details of the proposed biometric system. The main design principals is to conduct the authentication process onboard while keeping the cost low using commodity electronics by designing a unobtrusive Shoe-Wearable

Biometric System (SWBS). The system is presented in two parts, the hardware prototype and the NN classifier.

3.1 Prototype Design

A regular shoe was used to accommodate the rest of the system components as it depicted in Figure 1. Then consulting the force heat map of Keatsamarn [13] for inspiration, a total of three force sensors (FSR 402 by Interlink [8]) was used to capture the plantar pressure as it is presented in Figure 2. The Force sensors are attached under the shoe insole and they are thin enough to not being noticed by the user. The shoe we used, a typical athletic shoe, includes a sole with a thickness of 35 mm approximately. The Force sensors are attached on an Arduino Nano 33 BLE Sense [2], which is main platform of the system responsible for all the computational tasks. The Arduino board is mounted on the heel of the shoe and its three-axis accelerometer is used to capture the gait pattern. To power the system a battery should be included to this design or utilising energy harvesting methods [16] can be also an option. The system is supposed to authenticate a user and then transmit the result to the proof authority using the Bluetooth Low Energy (BLE) technology. Figure 3 depicts the system flow.

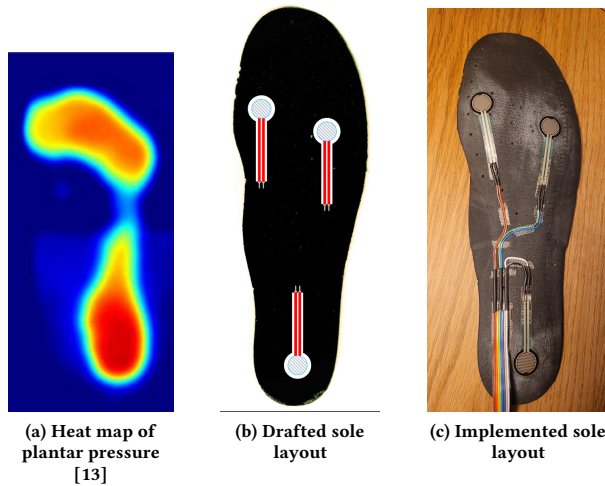


Figure 2: Chosen sole layout for force sensors used to capture plantar pressure for biometric purposes.

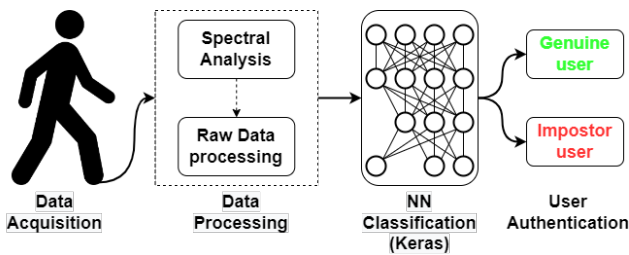


Figure 3: The biometric system's flow, sensors are obtaining the data, then they are processed and then a NN classifier is giving the output, an authenticated user or not.

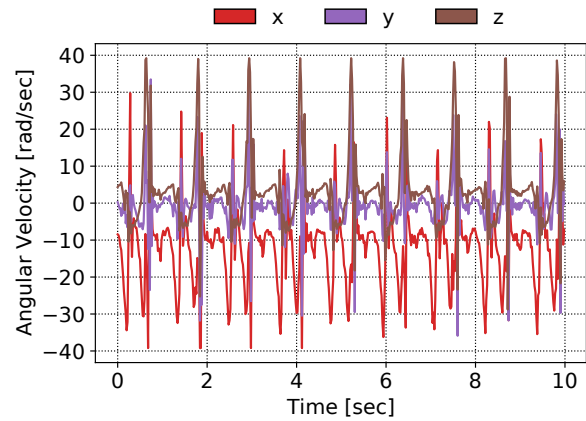


Figure 4: Raw data from the three-axis accelerometer.

3.2 Neural Network classifier

Developing a novel NN classifier tailored to the design requirements was out of the scope of this paper. Therefore we use Edge Impulse [7], a development platform for machine learning on edge devices which specialises in bringing machine learning to a wider audience of developers. Their platform allows for numerous processing platforms to be used for both data gathering and model generation, as well as varying degrees of control of the data processing and neural architecture.

In order to generate sufficient data, we asked 10 individuals to participate in our research following all the recommended regulations about pseudonymization and data privacy by GDPR. The volunteers were asked to walk casually outdoors for a specific distance, in their usual walking pattern along a flat distance. They were to ignore the adjacent researcher walking behind them, with a laptop collecting data. This included to avoid coordinating their gait or speed to that of the researcher. Likewise, they were asked to note if anything felt off, hurt, they would like a break, or if anything felt uncomfortable otherwise. Each volunteer was given a designated moniker to easily group their data, such as "Data Subject XX", or "DSXX" for short.

A data frequency of 50 Hertz was chosen. The six data points (three axis accelerometer and three force sensors) were recorded for between 100 to 300 seconds, resulting in between 30,000 to 90,000 data points captured for each data subject. A part of the obtained raw data is illustrated in Figures 4 and 5. In addition, the system beside raw data from the sensors is able to capture spatiotemporal parameters like gait and stride speed for more complex models in the future. A 80%/20% relationship between training and test data was utilised for the models. Due to the only available shoe provided for the project being a size 45 (EU standard), this imposed a minor restriction on the data subjects eligible for data acquisition. All 10 data subjects who volunteered for the project were: biological male, between 22 and 78 years of age, weighed between 70 and 105 kilograms, and between 170 and 195 centimetres tall.

The Edge Impulse defines a very specific operational framework. Firstly, the acquired data is sent through a spectral analysis procedure, used to extract frequency and power characteristics of the

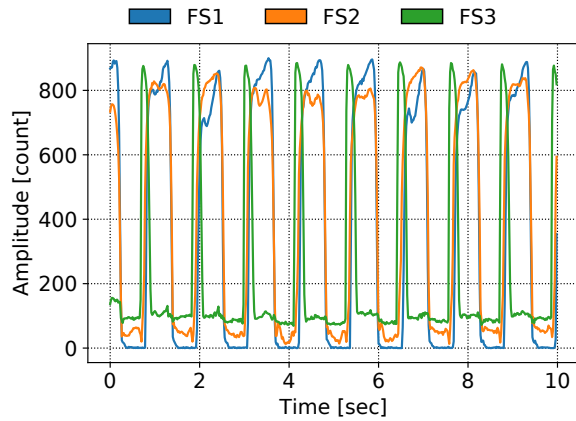


Figure 5: Raw data from the force sensors.

signals by scaling the raw input signal, applying a Butterworth filter (a signal processing filter designed to make a frequency response to be as flat as possible in the passband) and adding the root mean square of the output to the features' list. This simply applies an additional scaling of the input axis. Next, the data is forwarded into a Keras-based Neural Network architecture. Keras is an open-source Python Library running on top of the learning platform TensorFlow [18]. For the purpose of avoiding potentially overfitting the model, a Learning rate of 0.00015 was chosen, over the course of 100 training cycles using trial and error. The NN consists of four layers, an input layer with 366 Features, before being processed by another two hidden layers. Lastly, the output of these are classified into 10 separate classes, one for each data subject.

4 PILOT EVALUATION

This section provides a pilot evaluation we did on 10 individuals by reporting the F1 score of the NN classifier, reflecting on the advantages and disadvantages of the proposed biometric system and comparing it based on an amount of aspects important for wearable biometric systems.

Edge Impulse allows for comparison of test data to the trained model classes. A confusion matrix, as shown in Table 1, highlights the performance of the model. A plausible argument may be that the biometric system should only need to recognise a single individual. In some ways, the model's robustness and accuracy is put under greater stress, than it would if only a single data subject were to be recognised. Additionally, by presenting the data in a matrix and organising it in this manner, it is easier to compare with the state of the art [5, 19]. Overall, a 94.3% accuracy was achieved, with a Loss of 1.87. Additionally, Edge Impulse reported a 27 millisecond inference time, a peak ram usage of 2.3 KB and a flash memory usage of 160.0 KB.

The results showed consistent recognition rate across the classifications. Combined with a low inference time of just 27 ms, this indicates that the system has a significant potential for implementing a biometric system on the edge utilising the CA paradigm. The data and the results also demonstrates how the system can be used

for a gradient-scale authentication scheme, to restrict user access rights depending on the latest recognition score.

Whilst the results highlight the potential for a lightweight and more affordable solution, there are a number of factors to consider. Neither the algorithm nor the data was optimised beyond rudimentary data processing, and inserted into a NN classifier (using Keras). This was a preliminary design but a proper data processing and optimisation should be planned in future designs. The volunteers all shared a similar physiological stature. Additionally, the only shoe available may have resulted in poor data acquisition due to slight shoe size differences. No deep investigation on the topic of potential overfitting of the model - this again was not the explicit purpose of the paper, but rather something to note. In order to accommodate the volunteers to the greatest extent, the data acquisition had to be done close to their homes. This meant that the distance they walked might not have been completely level and smooth.

On the other hand, for the short extent of the evaluation, the proposed system presented some very encouraging features. The data and subsequent NN for classification was made for a much more complex scenario/model, than a likely implementation of the system. As mentioned previously, the model only needs to be certain of one individual's identity, not to classify more than 10 different people. Very little data has been gathered. Between 100 and 300 seconds worth of data was acquired for each data subject. A minuscule amount of data, in comparison to contemporary works. This means that whilst the amount of data for training and testing is very modest, the model had little to no issues achieving 100% recognition rate for multiple data subjects. Despite only using 6 data vectors (three force sensors, three axis), of which 3 were largely insignificant in the final result, very consistent and assured results were produced.

In order to better analyse the proposed biometric system, aspects such as price of the unit, weight, ergonomics, size, etc. are obvious to look into. To provide a fair comparison between the introduced biometric system and the state of the art, the most similar system(s) will be used. These are the Raspberry Pi 2B-based system by Yeh et al. [19], the custom board of Ivanov et al. [12] and Huang et al's microcontroller-based proposal. To quantify the different aspects of the three systems, table 2 presents a number of differences between the three.

System architecture: Only the introduced biometric system has adopted a monolithic architecture (the authentication is carried out onboard), whereas the other proposals use their wearable systems as simple data loggers and transports. The design choice to go with this type of system architecture has far-reaching consequences for a number of the following characteristics. The outcomes for a multitude of parameters is discussed below.

Sensory equipment: The number of force sensors utilized is the minimum compare with the other approaches. We should mention though that the introduced approach and Huang's proposal [10] use secondary sensors to compliment the primary force sensors. Using less sensors contributes towards less power consumption, less memory and less data complexity.

Power consumption: Another important aspect is the power consumption. Whereas Ivanov's minuscule data gathering processor board only draws 3 mA, the SWBS draws around 32 mA [17]. Huang did not disclose the system's wattage, but somewhere around

Tester/Classifier	DS01	DS02	DS03	DS04	DS05	DS06	DS07	DS08	DS09	DS10
DS01	100%	0%	0%	0%	0%	0%	0%	0%	0%	0%
DS02	0%	87.5%	0%	0%	0%	0%	0%	6.3%	6.3%	0%
DS03	0%	0%	95%	0%	0%	0%	5%	0%	0%	0%
DS04	0%	0%	0%	100%	0%	0%	0%	0%	0%	0%
DS05	0%	0%	0%	0%	94.7%	0%	0%	5.3%	0%	0%
DS06	0%	0%	0%	0%	0%	88.2%	2.0%	9.8%	0%	0%
DS07	0%	0%	1.9%	0%	1.9%	9.4%	86.8%	0%	0%	0%
DS08	0%	0%	0%	0%	0%	0%	0%	100%	0%	0%
DS09	0%	0%	0%	0%	0%	0%	0%	0%	100%	0%
DS10	0%	0%	0%	1.8%	0%	0%	0%	0%	1.8%	96.4%
F1 Score	1.00	0.93	0.95	0.97	0.96	0.89	0.91	0.91	0.98	0.98

Table 1: Confusion matrix showcasing the model’s recognition rate between the 10 classes of data subjects. The F1 Score rates how successful the classifier is - it is the harmonic mean of precision and recall [4].


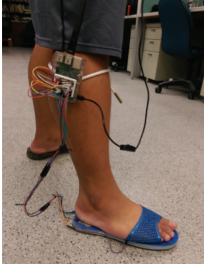
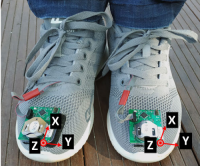
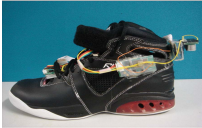
	SWBS	Yeh [19]	Ivanov [12]	Huang[10]
System architecture	Monolithic	Modular	Modular	Modular
Number of force sensors	Three	Six	Nine	Four
Physical shape				
Secondary sensors	Accelerometer	None	None	Yes

Table 2: Simple comparison chart of the three systems proposed between this paper, Yet et al. [19], Ivanov et al. [12], and Huang et al. [10]. Note how Yeh’s system utilises two data collectors, one for each foot.

those two points are to be expected. Meanwhile, Yeh’s Raspberry Pi-based system draws between 320 to 450 mA [9]. Regarding the communication SWBS, Yeh’s [19] and Ivanov platform [12] uses BLE and Huang’s proposal [10] an older version of a Bluetooth radio. The radio communication has been proven to consume the most amount of power in IoT devices. Thus, sending just the result to the proof authority instead of a series of raw data can decrease the power consumption significantly. The sensors of course consume a considerable amount of power. Hence, the relation between number of sensors and power consumption is proportional.

Weight: All four platforms are very lightweight, making for only a small potential impact on the wearer’s gait. Whilst Yeh’s platform [19] may weigh somewhere around 55 grams, and the SWBS around 35 grams (excluding the battery), Ivanov’s smaller data collecting unit [12] would undoubtedly weigh even less¹. Huang’s work [10] offered no details on this, but from the provided images, it should be in the multitude of Yeh’s platform.

Costs: Whilst the complete cost of SWBS can be calculated for around \$52.00, assuming a cost of around \$7.00 per sensor [1]² at

¹No official weight was disclosed, estimate between 20 and 30 grams including a CR2032 button battery.)

²This price will be used for calculating the costs of the other systems as well.

the time of writing and a cost of around \$31.00 for the Arduino [3]. Meanwhile, Yeh’s system [19] would cost around \$77.00, assuming a Raspberry pi cost of \$35.00. The data processing server is not counted as an expenditure, as the job can be taken up by a workstation or server. Huang’s platform [10] with its four sensors would be at least \$28.00. Whilst there are no concrete details on the specific sensors in use on the platform, a fair estimate would be between \$20 – \$25 of additional costs, putting the platform up around \$48 – \$53. Lastly, whilst Ivanov’s processing board [12] only consists of inexpensive components like a radio sender, a small battery and a wireless proprietary System on a Chip (SoC), the amount of sensors alone pushes the price for the system up to \$63.00. In conjunction with the necessary custom data logging system, Ivanov’s proposal is the most expensive in terms of materials.

Security & Hardiness: Considering the security aspects of both physical design and communication channels, SWBS has much greater capacity for security built in, than its contemporaries. Both Ivanov’s [12] and Yeh’s [19] platforms are exposed to outside physical tampering. Ivanov’s platform has a slight edge in comparison to Yeh’s due to the Raspberry Pi’s many USB ports and physical interfaces. However, both of these falls short in relation to the security of the communication channels they employ. Ivanov’s platform

have no mentioned methods of encryption or verification of message integrity. Meanwhile, while Yeh's platform does support this, due to its UNIX kernel, there are no mentions on the possibilities of hardening its data communications. Huang's platform [10] describes a capacity to use Forward Error Correction (FEC) to help reduce transmission error and improve the wireless communication reliability. There are no other mentions of security measures on board of the system. The proposed platform supports both encryption of the data on the chip (AES-128), usage of up to 16 separate keys/certificates with Elliptical Curve Diffie-Hellman key exchange, and integrity checks using SHA-256. Also worth mentioning is the potential for a very small physical footprint. It is safe to assume that the WBAS has much greater potential for secure and hardy communications as the crypto chip ensures that no secrets are ever exposed in plain-text [2].

Ease of installation: Ivanov's proposal [12] is incorporated directly into the shoe sole, and connects to the smallest and lightest processing board. Both SWBS and Huang's system [10] requires only minimal gluing of sensors to a shoe sole and the processor board to the shoe itself. The wires are short and kept minimal. Lastly, Yeh's proposal [19] is arguably the most fragile, with multiple dangling wires and a loose slipper as a platform. To top it off, the processing board is tied to the data subject's leg with a shoestring. It should again be mentioned how none of the platforms was made with this purpose in mind. It was however included, to debate the prospects of the platforms.

Ergonomics: SWBS and Huang's system [10] are both incorporated directly onto the shoe and beneath the shoe sole, resulting into a less obtrusiveness wearable. Likewise, by having a shoe sole with all the sensors directly embedded, the impact is virtually non-existent. Lastly, while Yeh's proposal [19] is kept light, the many wires, the unfastened flipper and the usage of potentially unstable securing of the processor may influence the data subject's walking pattern. We have to mention that we did not evaluate the wearability and the user experience of SWBS but this is an interesting aspect we plan to evaluate in the future. Nevertheless, no volunteers mentioned discomfort, requested a break, or otherwise voiced apprehension with the overall process.

5 CONCLUSION

This paper introduced a shoe-wearable biometric system which is able to perform the authentication process onboard. The design was carried out to keep the cost low, use off-the-shelf electronics and implement a unobtrusive wearable. The prototype is built based on a regular shoe attaching three force sensors under the shoe sole and an accelerometer on the heel. The computing platform we use is an Arduino Nano 33 BLE Sense [2] and a NN classifier built and executed onboard with the support of Edge Impulse [7] development platform. A pilot evaluation of 10 individuals demonstrates that the proposed biometric system was able to authenticate each user with 94.3% with loss of 1.87. Unlike the state of the art approaches, the proposed biometric system do not compromise the sensitive raw data obtained by the sensors by transmitting them to another entity since the authentication takes place on the edge. Furthermore, there is not cost and delay overhead because of the same reason.

As future work we plan to propose a tailored learning model and a more advanced data processing method to optimise further the results. We also plan to have a proper evaluation with more volunteers and also design several sizes of prototypes to have more diverse group of volunteers. Furthermore we plan to increase the evaluation time and include several activities (walking, standing, climbing stairs) to evaluate further the efficiency of the proposed biometric system.

REFERENCES

- [1] ADAFRUIT. Round Force-Sensitive Resistor (FSR) - Interlinky 402. <https://www.digikey.com/en/products/detail/interlink-electronics/30-81794/2476468>. Accessed: 2022-03-17.
- [2] ARDUINO. Nano 33 BLE Sense. <https://docs.arduino.cc/hardware/nano-33-ble-sense>. Accessed: 2022-02-12.
- [3] ARDUINO.CC. Arduino Nano 33 BLE Sense. <http://store-usa.arduino.cc/products/arduino-nano-33-ble-sense>. Accessed: 2022-03-17.
- [4] BAELDUNG. F-1 Score for Multi-Class Classification. <https://www.baeldung.com/cs/multi-class-f1-score#f-1-score>. Accessed: 2022-03-15.
- [5] BASHEER, S., NAGWANSHI, K. K., BHATIA, S., DUBEY, S., AND SINHA, G. R. Fed: An approach for biometric human footprint matching using fuzzy ensemble learning. *Ieee Access* 9 (2021), 26641–26663.
- [6] DALENOGARE, L. S., BENITEZ, G. B., AYALA, N. F., AND FRANK, A. G. The expected contribution of industry 4.0 technologies for industrial performance. *International Journal of Production Economics* 204 (2018), 383–394.
- [7] EDGE IMPULSE™. Edge Impulse's official website. <https://www.edgeimpulse.com/>. Accessed: 2022-03-22.
- [8] ELECTRONICS, I. FSR 400 Series Data Sheet. Official website. Accessed: 2022-02-16.
- [9] GEERLING, J. Power Consumption Benchmarks | Raspberry Pi Dramble. <https://www.pidramble.com/wiki/benchmarks/power-consumption>. Accessed: 2022-03-17.
- [10] HUANG, B., CHEN, M., YE, W., AND XU, Y. Intelligent shoes for human identification. *2006 Ieee International Conference on Robotics and Biomimetics, Robio 2006* (2006).
- [11] IVANOV, K., MEL, Z., LUBICH, L., GUO, N., XILE, D., ZHAO, Z., OMISORE, O. M., HO, D., AND WANG, L. Design of a sensor insole for gait analysis. *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (2019), 433–444.
- [12] IVANOV, K., MEL, Z., PENEV, M., LUBICH, L., MUMINI, O. O., NGUYEN VAN, S. V., YAN, Y., AND WANG, L. Identity recognition by walking outdoors using multimodal sensor insoles. *Ieee Access* 8 (2020), 150797–150807.
- [13] KEATSAMARN, T., AND PINTAVIROOJ, C. Footprint identification using deep learning. *Bmeicon 2018 - 11th Biomedical Engineering International Conference* (2018).
- [14] KHOKHER, R., AND SINGH, R. C. Footprint identification: Review of an emerging biometric trait. *Macromolecular Symposia* 397, 1 (2021), 2000246.
- [15] KUSHWAHA, R., NAIN, N., AND SINGAL, G. Detailed analysis of footprint geometry for person identification. *Proceedings - 13th International Conference on Signal-Image Technology and Internet-based Systems, Sitis 2017 2018-* (2018), 229–236.
- [16] ORFANIDIS, C., DIMITRAKOPOULOS, K., FAFOUTIS, X., AND JACOBSSON, M. Towards battery-free lpwan wearables. 52–53.
- [17] TANNER, G. Arduino Nano 33 BLE Sense Overview. <https://gilberttanner.com/blog/arduino-nano-33-ble-sense-overview>. Accessed: 2022-03-17.
- [18] TENSORFLOW. Tensorflow Official Install. <https://www.tensorflow.org/install>. Accessed: 2022-03-20.
- [19] YEH, K. H., SU, C., CHIU, W., AND ZHOU, L. I walk, therefore i am: Continuous user authentication with plantar biometrics. *Ieee Communications Magazine* 56, 2 (2018), 150–157.
- [20] YUN, J., ABOWD, G., WOO, W., AND RYU, J. Biometric user identification with dynamic footprint. *2007 2nd International Conference on Bio-inspired Computing: Theories and Applications, Bicta 2007* (2007), 225–230.