Performance evaluation of Mobile Sensor for Context Awareness User Authentication

ARTICLE HISTORY

Received 13 March 2022
Accepted 02 May 2022

Eniola S Adewumi
Department of Computing, Collage of Bussines,
Technology and Engineering,
Sheffield Hallam University
Sheffield - United Kingdom
b8009528@my.shu.ac.uk

Timibloudi S Enamamu
Department of Computing, Collage of Bussines,
Technology and Engineering,
Sheffield Hallam University
Sheffield - United Kingdom
t.enamamu@shu.ac.uk

Aliyu A Dahiru
Department of Computing, Collage of Bussines,
Technology and Engineering,
Sheffield Hallam University
Sheffield - United Kingdom
b8040371@my.shu.ac.uk

E. Adewumi, T. Enamamu, A. Dahiru,
"Performance Evaluation of Mobile Sensor for Context Awareness User Authentication",
Latin-American Journal of Computing (LAJC), vol. 9, no. 2, 2022.

Performance Evaluation of Mobile Sensor for Context Awareness User Authentication

Eniola S. Adewumi
Department of Computing,
Collage of Bussines,
Technology and Engineering,
Sheffield Hallam University
Sheffield – United Kingdom
b8009528@my.shu.ac.uk

Timibloudi S. Enamamu
Department of Computing,
Collage of Bussines,
Technology and Engineering,
Sheffield Hallam University
Sheffield – United Kingdom
t.enamamu@shu.ac.uk

Aliyu A. Dahiru
Department of Computing,
Collage of Bussines,
Technology and Engineering,
Sheffield Hallam University
Sheffield – United Kingdom
b8040371@my.shu.ac.uk

Abstract— With the increase of smart devices and their capacities, their use for different services have also increased. As much as this is an advantage, it has posed additional risks because of the confidential information stored on them. This has increased the need for additional security on the smart devices. Most of the methods used for user authentication pose certain drawbacks that are either easy to circumvent or cumbersome to use. As a result, multi-level means of authentication is needed to improve the security of mobile devices. Sensors are playing a vital role in the mobile ecosystem to enhance different services. These sensors can be leveraged upon as a solution for user authentication. This research analyzed and evaluated different mobile device sensors for continuous and transparent user authentication. The mobile data used includes gyroscope, accelerometer, linear accelerometer, proximity, gravity, and magnetometer sensor data. A feedforward neural network was used for data classification. After extracting features from the different sensors available in the mobile device, the most effective sensor was selected by evaluating performance of the different sensors. The best sensor, the accelerometer was further experimented on. The experiment showed that smartphone accelerometer sensor exhibits sufficient discriminability, stability, and reliability for active and continuous authentication, by achieving a performance of 6.55% for the best overall EER.

Keywords— Mobile Sensor, Authentication, Mobile Device, Accelerometer

I. INTRODUCTION

The number of Internet of Things (IoT) devices is projected to be 120 billion by the year 2025 [1]. The present-day smartphones have the capacity to support the user's needs. As a result, people rely on the services and information on their mobile device to complete their daily activities such as business or personal activities. Some of these daily activities include meeting schedules, accessing emails, online games, online shopping, accessing news, and sharing of documents.

Most recent mobile devices have increased capacity in terms of storage, and this means increase in the storage of sensitive data on such devices. As more of these data are stored in the device, information leakage becomes a concern to organizations and users of these mobile devices.

Researchers from University of Pennsylvania demonstrated how latent smudges leave smartphones susceptible to hacking. Smudges attack is used to obtain PIN and pattern of a smartphone, simply by increasing or decreasing the contrast of the smartphone [2].

Pattern, PIN, and password also suffer from shoulder surfing attacks; this attack occurs when a malicious user can fully observe or watch the login session [3].

Cameras on mobile devices are getting better with increased pixels, therefore, it will be useful for capturing biometric data for user authentication [4] and can be used for spying. Once a user is identified while using a camera, the pictures can be used to fool the system.

Transparent and continuous biometric authentication system should improve the security of mobile devices, it should provide a convenient protection mechanism for mobile devices [5]. To enhance mobile device security with continuous mechanisms, usability should be considered. Out of various authentication solutions, a promising technique is the utilization of sensory data. Unlike other special biometric techniques for smartphone authentication (such as touch behavior or fingerprints), most sensors do not require any specialized hardware to obtain biometric data [4]. Furthermore, from the analysis of most sensors on mobile devices, sensory data can be in a continuous manner if the mobile device is being used. Hence, sensory data from mobile devices can provide a non-intrusive, active, and continuous authentication solution.

Recently, there has been an increase in literature toward sensors behavior for authentication. Research on entry-point authentication [4] [6] as well as active continuous authentication [7] shows multi-motion sensor (such as accelerometer and gyroscope) investigation and analysis. Most research based their work on motion-sensor users' authentication. Nevertheless, the research work using these sensors for motion-based authentication have not been comprehensively evaluated; these sensors need detailed analysis of accuracy, stability, and usability across various application scenarios. Therefore, this paper focuses on evaluating the performance of mobile sensor behavior for active smartphone authentication. Table 1 below shows publications about mobile phone sensors for user authentication.

TABLE I. CONTRIBUTIONS IN USER AUTHENTICATION USING MOBILE PHONE SENSORS

Name of Author	***Year***	***Type of data used***	***Accuracy***	***Conti-nuous/ non-continuous authentication***
Wei and Ruby [16]	*2017*	*Fingerprint and ear pattern*	*90.23%*	*Non-continuous*
Mohammad et. al. [15]	*2017*	*Proximity Sensor*	*97.38%*	*Non-continuous*
Hernandez-Alvarez et. al [17]	*2021*	*Gyroscope and accelerometer*	*76.85%*	*Continuous*
Alqarni et. al. [20]	*2020*	*Hand movement and waving pattern*	*74.9%*	*Continuous*
Papavasileiou et. al. [24]	*2021*	*Gait (Smart socks and smart shoes)*	*EER of 0.01% and 0.16% , respectively*	*Continuous*

In this article, we evaluated the performance of various mobile phone sensors for active and continuous user authentication, the user's environment was also put into consideration. The experiment evaluated the performance of different sensors across various user activities. These sensors data can be fused to increase the authentication accuracy based on a predefined threshold by using the most suitable data for continuous authentication taking cognizance of the environment. To achieve this, the following research objectives were established:

- To investigate the various mobile sensor data suitability for active authentication.
- Evaluate and analyze the different sensor's data based on different activities.
- A further analysis of the best performing sensor.

II. RELATED WORK

There has been various works on different methodology for securing mobile device. It is necessary to improve on these methods as the traditional method of knowledge-based authentication has memorability issue [8] when a complex password or pin is used. Using biometrics like fingerprint, facial and voice print are common methods for mobile device authentication [9]. This is made easy due to the sensor in them and therefore, don't require any installation on the devices [10]. In [11], the use of spoofing for attacking biometric systems was explained, this is on the increase. Hence, the work proposed a 3D anti spoof touchless ear biometric sensor using a laser biospekled fringe projection profilometry based imaging algorithm. The algorithm uses the combination of biospekle analysis and fringe profilometry technique. The accuracy of the techniques is affected by shadows and hair which are unavoidable [12].

In a similar work, a finger imaging using contactless 3D convolutional neural network (CNN) for user authentication was proposed [13]. The imaging framework use Multiview deep learning for extracting the minutiae feature of the fingerprint. This method is used to overcome the problem of elastic deformations of the friction skin and local regions of fingerprint images. This is caused by sweat, dirt, dryness of the skin or skin diseases, and inconsistent finger pressure while extracting the fingerprint. This method, when used can solve the problem of latent lifting in 2D fingerprint authentication.

A similar method like the last two authors was introduced, using fingerprint, and retina for authentication [14]. Here, an RSA (Rivest-Shamir-Adleman) asymmetric cryptographic algorithm for encrypting the biometric template to improve security for authentication was proposed. To reduce error in the process and make it more flexible, any of the two

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763156

biometric can be used, and can be fused using it to encrypt the template gotten from the biometric features. They also mentioned that the fusion of the three biometric features would reduce the error, provide flexibility, and build resistance to spoofing attacks when compared to using unimodal biometric systems. However, based on the nature of asymmetric encryption, it will increase the overall process time, which makes this proposal slow.

In [15], the issue with using knowledge-based, and physiological-based authentication mechanisms was explained, based on the usage of a mobile phone as a multi-purpose device for different activities. Evidently, the frequency of its usage is high, resulting in an increased frequency of both PIN and password inputs. As a result, employing non-intrusive methods for user authentication seems to be most ideal. For instance, in [16], an accuracy of 90.23% was achieved, using fingerprint and ear pattern captures to identify a user. A training and testing time of 6.07s and 20s were used respectively. This novel biometric user authentication achieved high accuracy levels, justifying its convenience, compared to hardware-based methods.

In [15], "IntelliAuth" was introduced, based on the user's behavioral biometric with the ability to use the environmental sensing to improve the authentication using a proximity sensor. Mobile sensors of accelerometer, gyroscope, and magnetometer are used user authentication. This proposal is novel as the result of the Bayes-Net classifier produced a 97.38% accuracy when compared to the other classifiers (decision tree, K-NN and SVM). The work presented in [16] proposed a multisensory authentication system which continuously authenticates the user. Just like previous work, behavioral biometrics are used, so it does not require direct user involvement. Also, like its predecessor, the method proposed in [16] uses the accelerometer, orientation, and magnetometer sensors.

In addition, the proposal presented in [17] uses the gyroscope and accelerometer sensor to authenticate a user. The preservation of the users data captured from the sensors was considered by implementing a format preserving encryption technique. This was a countermeasure to reduce personal data leaks since most of the authentication systems use machine learning algorithms which are sometimes outsourced to the Cloud, making them be prone to attacks. Despite using cryptography for securing user data, an accuracy of 76.85% was achieved with no significant impact on the authentication process.

In the area of using voice for authentication, researchers in [18] developed a continous authentication system using a fusion of mobile phone sensors and speaker information. This proposal is novel as it is a multimodal form of authentication, similar to the one in [19], which produced high accuracy rate. However, voice recognition has setbacks because it is not convenient to be used by people with learning difficulties, or speech impediments. Also, its accuracy may be compromised if a person's voice changes due to different health and emotional conditions.

In [20], a subystem for continous user identification using mobile phones was introduced. It was based on how they interact with their phones (hand movement and waving patterns). To test the performance of the system, random forest, support vector machine and Bayesian networks were used, reaching an accuracy of 74.9% using the random forest classifier.

In conclusion, the mobile sensor will enhance user authentication for the implementation of transparent authentication for a mobile device. The fusion of several sensors will improve the data available, resulting in an increased accuracy for mobile user authentication.

III. EVALUATION METHOD

This proposed work is to evaluate and analyze the explicit and continuous authentication of mobile phone users. The availability of real-time sensorial data via mobile phone sensors provides useful information to analyze a user's environment, the usage patterns, and user mobility

Using the sensorial data and the computational capabilities of smartphones, the proposed work includes data collection, pre-processing of data, feature extraction, and classification. The details of each step are explained in the following sections.

A. DATA COLLECTION

Data is collected from 30 healthy participants using a third-party application called TOHRC data logger available on the android play store. To create a real-life scenario, participants carried out some activities sitting, standing, walking both on plain floor and staircase, on a platform and walking down a staircase. These activities are used because data was collected in a controlled (University building, individual homes) environment under a short period of time and those activities reflects a person's usual day-day activities. Each of this activity is recorded for thirty (30) seconds with a sampling rate of 50Ghz.

The mobile device was held by the participant while doing all activities. The experiment was carried out using four different activities for each participant. The activities are listed below:

- Activity 1: User sitting for a defined time while the data was collected.
- Activity 2: User standing for a defined time while the data was collected.
- Activity 3: User walking for the duration for a defined time while the data was collected.
- Activity 4: User walking down and up a staircase for a defined time while the data was collected.

B. OVERVIEW OF SENSORS

Mobile phone sensors are categorized into three, this is based on the sensor data type. The sensor categories are

1. Motion sensors
2. Position sensors
3. Environmental sensors

The motion sensors measure acceleration and rotational forces along the X, Y, Z-axis. Examples of motion sensors are the accelerometer, gyroscope, gravity sensors etc.

The position sensors measure the physical position and orientation of the mobile phones. the position sensors include the orientation, proximity, and magnetometer sensors. The environmental sensors are used in measuring environmental parameters. Examples of environmental sensors are thermometers, barometers. For this project, the position and motion sensors were used. Position and motion sensors have shown to be accurate and have been widely used for mobile phone user authentication [21]. The sensors selected in this study are used because they represent useful information about the user's behavior and environment. Based on the research work presented in [16], the accelerometer can detect coarse-grained motion of a user. This can be used for gait recognition while the orientation sensor can be used for analyzing how the user positions the device and the magnetometer is useful for environment representation. A combination of two or more of these sensors with similar functions would enhance mobile user authentication accuracy. The list of the sensor include:

- Accelerometer, linear acceleration sensor and gyroscope
- Orientation, proximity, and magnetometer sensors
- GPS and gravity sensors

TABLE II. SHOWING THE SENSOR AND POSSIBLE FEATURES (* REPRESENTS FEATURES THAT CAN BE EXTRACTED FROM THE SENSOR AND – REPRESENTS OTHERWISE)

Sensors / Feature	Variance	Sum	Maximum	Minimum	Mean	Standard Deviation	Percentile 25	Rootmean square	Peak-Peak	Kurtosis	Skewness
Accelerometer	*	*	*	*	*	*	*	*	*	*	*
Gyroscope	*	*	*	*	*	*	*	*	*	*	*
Line Acceleration	*	*	*	*	*	*	*	*	*	*	*
Gravity-sensor	*	*	*	*	*	*	-	-	-	-	-
Magnetometer	*	*	*	*	*	*	-	-	-	-	-
Rotation-sensor	*	*	-	-	*	*	-	-	-	*	*
Total	6	6	5	5	6	5	3	3	3	4	4

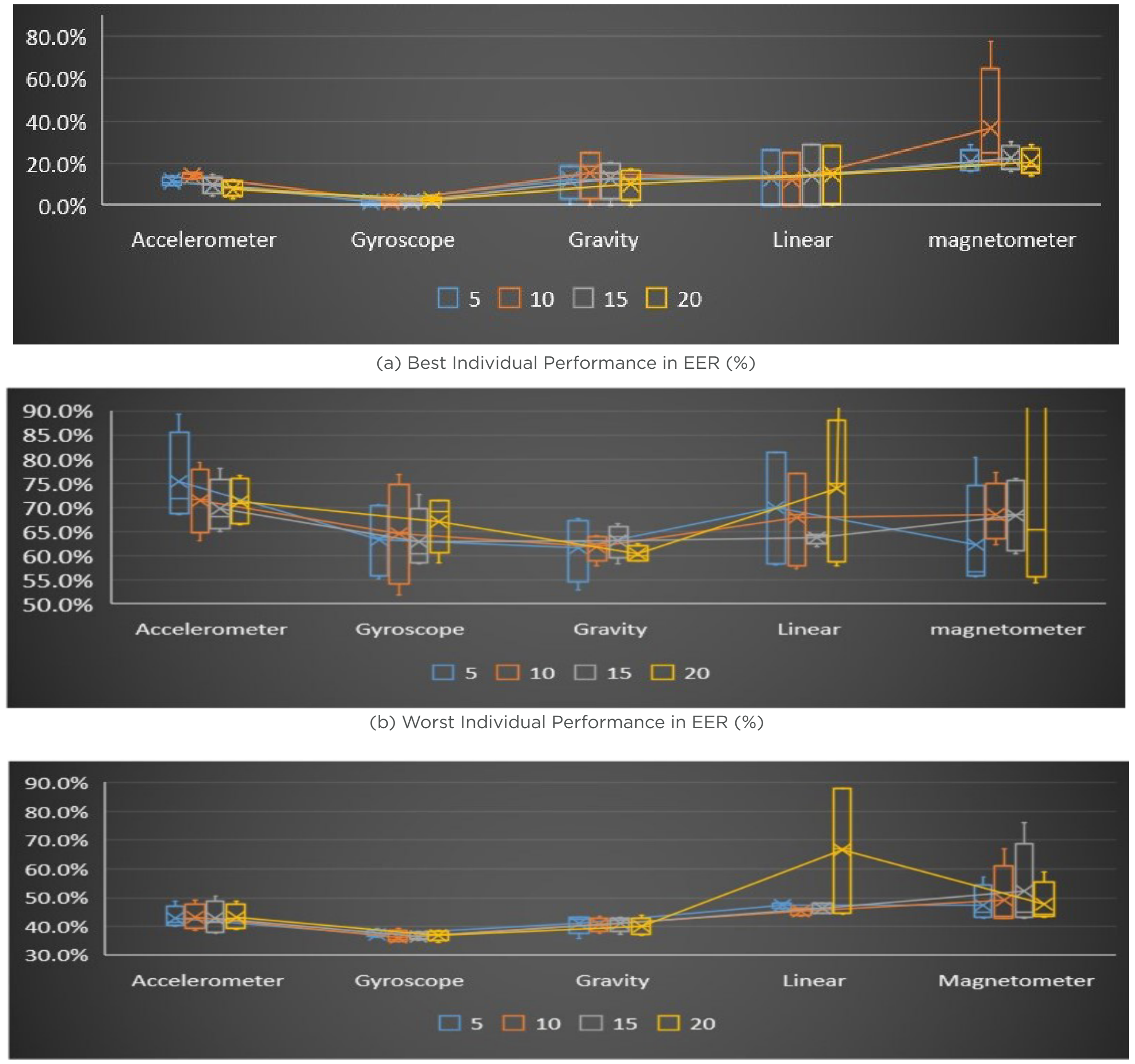
C. NEURAL NETWORK CLASSIFIER

Neural Network is an adaptive system that changes its structure or internal information flow using neuron for training time. This consists of hidden layers, and an output layer in the architecture. The number of neurons used for training the data is useful for determining the accuracy of the overall neural network classification. The number of neurons could be led to either underfitting or overfitting. The underfitting is when few neurons are used in the hidden layer and overfitting is when too many neurons are used for training. To overcome this issue, four different sizes of 5, 10, 15, and 20 network sizes are used to determine the best layer which could be used for each activity. Each of this activity is analyzed per sensor for all the neural network sizes compared.

D. EVALUATION METRICS

The research evaluated the proposed method using three (3) metrics widely in biometric authentication, these are:

- False Acceptance Rate (FAR) the false identity acceptance of an impostor.
- False Rejection Rate (FRR) is the



(a) Best Individual Performance in EER (%)

(b) Worst Individual Performance in EER (%)

(c) Overall Classification Performance in EER (%)

Fig. 1. Classification Performance

probability that the identity verification system incorrectly rejects the genuine user.

- Equal Error Rate (EER) is the meeting point of the plot of FAR and FRR. The lower the value of ERR, the higher the accuracy of the biometric system.

IV. MULTI-USER EVALUATION

Four network sizes are analyzed for the different sensor while participants carried out activities. This includes network size 5 ,10, 15, and 20.

In Figures 1(a) and 1(b), the best and worst individual performance is shown. Figure 1(c) shows the overall performance of all the classification.

A. INDIVIDUAL PERFORMANCE

The individual performance shows the best as the gyroscope followed by the accelerometer irrespective of the activity.

B. OVERALL PERFORMANCE

The overall performance shows the gyroscope as the best. However, the overall performance in Figure 2 shows that when using a different network size to improve the performance, the accelerometer performed better when a 45-size neural network was used.

V. ENHANCED PERFORMANCE EVALUATION FOR THE SENSORS

To investigate the performance of the sensors, we evaluate the performance of the sensors using the four activities. The study used the FAR (false acceptance rate) and FRR (false rejection rate). The final output from the two matric gives the EER (equal-error rate) for evaluation and analysis of the result. The EER biometric accuracy measure is used in this research. The most effective biometric control system is the one with the lowest ERR or CER.

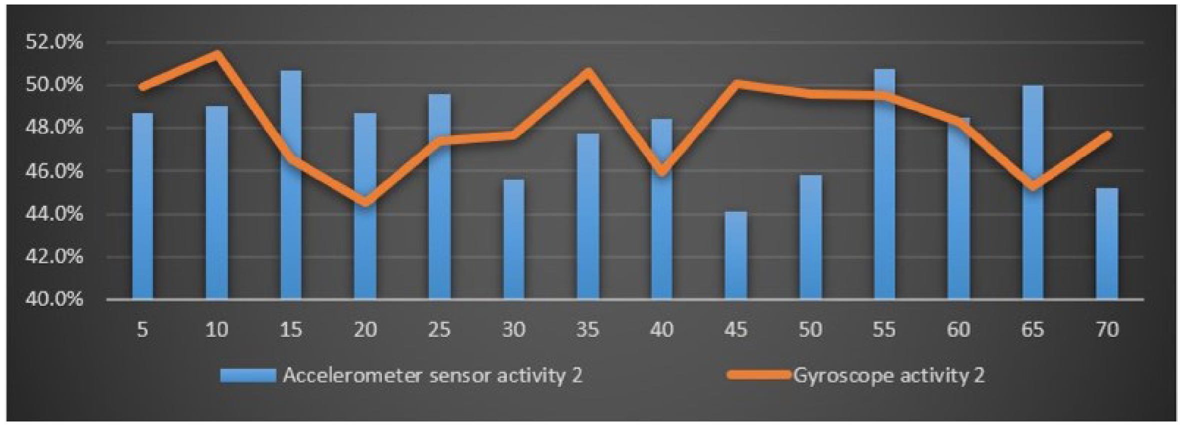
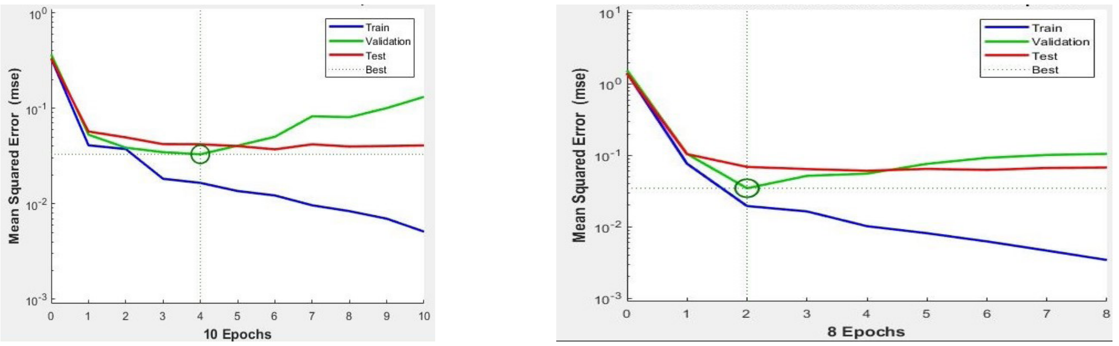


Fig. 2. Overall Performance in EER (%)



a) 0.032946 at epoch 4

b) 0.034672 at epoch 2

Fig. 3. Accelerometer Results for Standing Activity

The biometric that has the highest EER is the most ineffective. However, it is important to ensure the data is fully trained before analyzing the result.

The neural network training tool is used to train the data showing the data trained and the algorithm used. Mean Square Error (MSE) is used as the performance metric.

Performance has four lines: Trains, test, validation, and best. Performance for each of the training, testing, and validation sets is shown on a log scale. The best line (dotted) confirmed that training of the data had been done successfully. In all the activities, it can be seen decreasing as the data was trained. The network that did best on the validation set was used to calculate the ERR of all activities.

The result of the experiment is explained using tables and graphs.

Table 3 shows the result of standing activity. The lowest EER is 0.26% and the highest is 22.14 percent. Figure 3a) and 3b) shows the neural network training performance curve, and the best validation performance for sitting activity is 0.032946 at epoch 4.

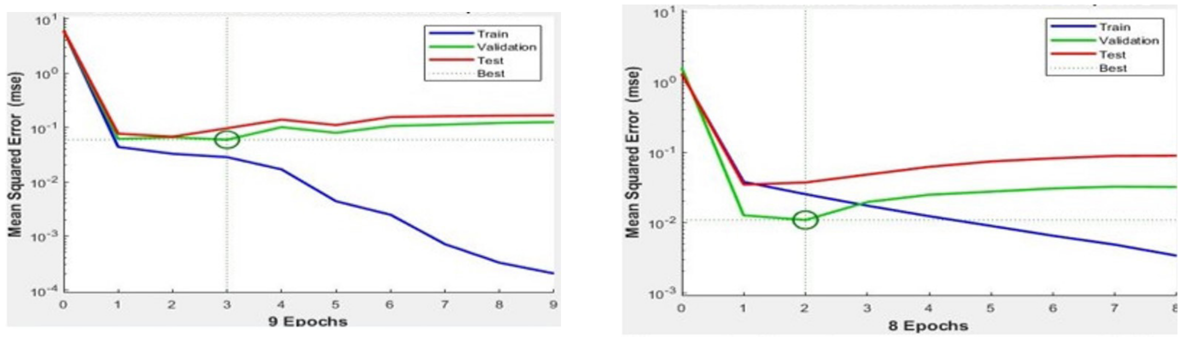
TABLE III. EER IN STANDING ACTIVITY

Activity	*Lowest EER*	*Highest EER*	*Overall EER*
Standing	*0.26%*	*22.14%*	*6.55%*

Table 4 below gives information about sitting activity. Sitting activity result achieved the lowest EER of 0.26%, and the highest EER of 32.49%. The overall ERR of this activity is 10.16%.

TABLE IV: EER IN SITTING ACTIVITY

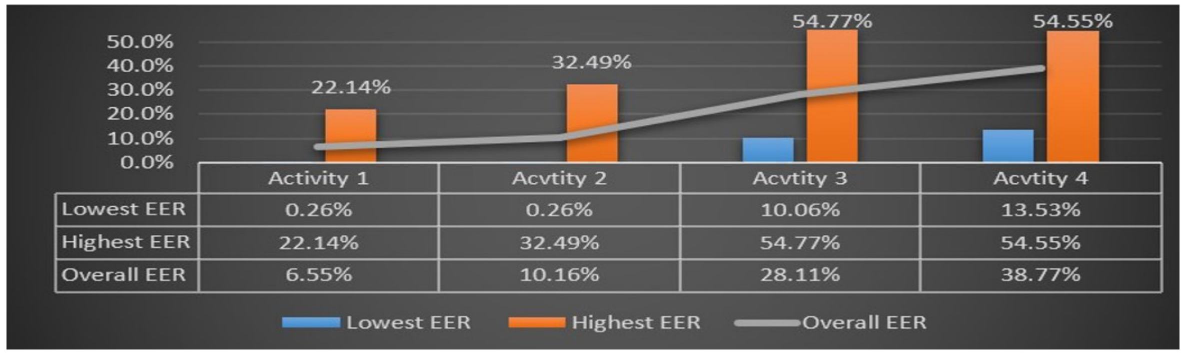
Activity	*Lowest EER*	*Highest EER*	*Overall EER*
Sit	*0.26%*	*32.49%*	*10.16%*



a) 0.05942 at epoch 3 for walking activity

b) 0.010879 at epoch 2 for stair activity

Fig. 4. Accelerometer Results for Walking and Stair Activity



	Activity 1	Acvtity 2	Acvtity 3	Acvtity 4
Lowest EER	0.26%	0.26%	10.06%	13.53%
Highest EER	22.14%	32.49%	54.77%	54.55%
Overall EER	6.55%	10.16%	28.11%	38.77%

Fig. 5. All-Activity EER Performance of the Accelerometer

Figure 4a) shows neural network training performance curve, and the best validation performance for walking activity is 0.05942 at epoch 3.

TABLE V. EER IN WALKING ACTIVITY

Activity	Lowest EER	Highest EER	Overall EER
Walking	10.06%	54.77%	38.11%

Figure 4b) shows neural network training performance curve, and the best validation performance for stair activity is 0.010879 at epoch 2. As the Table 6 below indicates, the lowest EER of 13.53% was achieved. The highest EER is 54.55%. The table also shows the overall EER for stair activity is 38.77%.

TABLE VI. EER IN STAIR ACTIVITY

Activity	No of Features	Lowest EER	Highest EER	Overall EER
Stairs	30	13.53%	54.55%	38.77%

In Figure 5, we use three indicators to describe the overall EER for all activities of the accelerometer sensor. To begin, standing activity has the lowest EER amongst all activities. standing activity (act. 1) has the lowest EER of 6.55%. Then followed by sitting activity (act. 2), which has an EER of 10.16%. The other two activities have an ERR that is significantly high when compared to the first two.

The overall EER of activities walking (act. 3) and walking up and down the stairs (act. 4) are also shown, with act. 3 having the overall EER of 28.11% and act. 4 having 38.77%. The most effective biometric control system is the one with the lowest ERR. The lowest EER of the accelerometer sensor is 6.55%, which means the experiment achieved 93.45% accuracy rate of authenticating the user. The highest EER is the most ineffective, which is 38.77%; this means it has 61.23% accuracy rate of authenticating a user.

VI. DISCUSSION AND FUTURE WORK

This research utilized a dataset of 30 healthy participants (users). The research examined the performance of multiple sensors across four activities: stand, sit, walk, and stairs. The signals (data) extracted from the three sensors of accelerometer, gyroscope, and magnetometer attributed to a larger feature vector which shows that the mobile sensor can be used for active authentication. Using the EER for evaluating the result, the higher the EER value, the lower the accuracy, on the other hand, the lower the EER value, the higher the accuracy of the biometric system [22].

In each activity the difference in the highest and lowest EER is significant because data was collected for 30 seconds. Future work would investigate collecting data for a longer period while users carry out different day-day activities.

In comparison with existing literature presented in the literature review, this research achieved a better performance than some of the existing studies. In [23] for example, a biometrics authentication mechanism using motion sensor of a smartphone was presented. The experiment was performed with the mobile user holding the mobile and moving around to perform a signature. The accelerometer used for the motion pattern detection. The result of the experiment confirmed that a single sensor can be used for authentication purposes. The study also demonstrated how a single sensor could be used for authentication purposes. The experiment achieved a false accept rate (FAR) of 1.46% and false rejection rate (FAR) of 6.87%, which has a better performance than the performance our experiment, which achieved an equal error rate (EER) of 6.55% and 10.16%. However, in [23], researchers developed an application that was explicitly used to gather only the necessary data for user authentication, whereas a third-party application was used in this research. In addition to that, [23] utilized only 6 participants for their experiments. Having more participants in our experiments, it was easier to distinct users and have better results with enhanced biometric performance.

REFERENCES

[1] S. Balakrishna, M. Thirumaran and K. V. Solanki, "A Framework for IoT Sensor Data Acquisition and Analysis," EAI Endorsed Transactions on Internet of Things, vol. 4, no. 16, 2018.

[2] P. Markert, D. V. Bailey, M. Golla, M. Dürmuth and A. J. AviG, "This pin can be easily guessed: Analyzing the security of smartphone unlock pins," IEEE Symposium on Security and Privacy (SP), pp. 286-303, 2020.

[3] N. Chakraborty and S. Mondal, "Color Pass: An intelligent user interface to resist shoulder surfing attack," in Proceedings of the 2014 IEEE Students' Technology Symposium, 2014.

[4] C. Shen, Y. Li, Y. Chen, X. Guan and R. A. Maxion, "Performance analysis of multi-motion sensor behavior for active smartphone authentication," IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, pp. 48-62, 2017.

[5] M. Muaaz, "A Transparent and Continuous Biometric Authentication Framework for User-Friendly Secure Mobile Environments," UbiComp, pp. 4-7, 2013.

[6] C. Giuffrida, K. Majdanik, M. Conti and H. & Bos, "I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics," Proceedings of the 11th Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), pp. 92-111, 2014.

[7] C. Nickel, T. Wirtl and C. Busch, "Authentication of smartphone users based on the way they walk using k-nn algorithm.," Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 16-20, 2012.

[8] G. Savedna and M. Haryana, "Biometrics in Mobile Security," International Journal of Mobile & Adhoc Network, vol. 1, no. 1, pp. 14-17, 2011.

[9] W. Yang, S. Wang, J. Hu, G. Zheng and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," Pattern Recognition, vol. 78, pp. 242-251, 2018.

[10] I. Natgunanathan, A. Mehmood, Y. Xiang, G. Beliakov and J. Yearwood, "Protection of privacy in biometric data," IEEE Access, vol. 4, pp. 880-892, 2016.

[11] A. K. Trivedi, D. M. Thounaojam and S. Pal, "A robust and non-invertible fingerprint template for fingerprint matching system," Forensic Science International, vol. 288, pp. 256-265, 2018.

[12] R. Purkait, "External Ear: An analysis of its uniqueness," Egyptian Journal of Forensic Sciences, vol. 6, no. 2, pp. 99-107, 2016.

[13] C. Lin and A. Kumar, "Contactless and partial 3D fingerprint recognition using multi-view deep representation," Pattern Recognition, vol. 83, pp. 314-327, 2018.

[14] D. Jagadiswarya and D. Saraswady, “Biometric Authentication using Fused Multimodal Biometric,” Procedia Computer Science, vol. 85, pp. 109-116, 2016.

[15] M. Ehatisham-ul-Haq, M. A. Azam, J. Loo, K. Shuang, S. Islam, U. Naeem and Y. Amin, “Authentication of Smartphone Users Based on Activity Recognition and Mobile Sensing,” Sensors, vol. 17, no. 9, pp. 1-31, 2017.

[16] W.-H. Lee and R. B. Lee, “Multi sensor authentication to improve smartphone security,” International Conference on Information Systems Security and Privacy (ICISSP), pp. 5-30, 2016.

[17] L. Hernandez-Alvarez, J. M. de Fuentes and L. González-Manzano, “SmartCAMPP - Smartphone-based continuous authentication leveraging motion sensors with privacy preservation,” Pattern Recognition Letters, vol. 147, pp. 189-196, 2021.

[18] J. M. Espín López, A. Huertas Celdrán, J. G. Marín-Blázquez, F. Esquembre and G. Martínez Pérez, “S3: An AI-Enabled User Continuous Authentication for Smartphones Based on Sensors, Statistics and Speaker Information,” Sensors, vol. 21, no. 11, p. 3765, 2021.

[19] M. Gomez-Barrero, J. Galbally and J. Fierrez, “Efficient Software attack on multimodal biometric systems and its application to face and iris fussion,” Pattern Recognition letters, vol. 36, pp. 243-253, 2014.

[20] M. A. Alqarni, S. H. Chauhdary, M. N. Malik, M. E. U. Haq and M. A. Azam, “Identifying smartphone users based on how they interact with their phones,” Human-centric Computing and Information Sciences, vol. 10, no. 7, 2020.

[21] A. Buriro, “Behavioral Biometrics for Smartphone user authentication,” International Doctoral School in Information Engineering and Communication Technologies (ICT), Italy, 2017.

[22] R. D. Newbold, Newbold’s Biometric Dictionary: For Military and Industry, Bloomington: AuthorHouse, 2008.

[23] A. Laghari and Z. A. Memon, “Biometric authentication technique using smartphone sensor,” 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST), pp. 381-384, 2016.

[24] I. Papavasileiou, Z. Qiao, C. Zhang, W. Zhang, J. Bi and S. Han, “GaitCode: Gait-based continuous authentication using multimodal learning and wearable sensors,” Smart Health, vol. 19, pp. 1-18, 2021.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763156

AUTHORS

Eniola Adewumi

I am currently a PhD. Student since 2021 and graduate teaching assistant at Sheffield Hallam University. I previously studied an MSc in Information System Security at Sheffield Hallam University and a BSc in Computer Science at University of Jos Nigeria.

Over the years I have developed great interest in Authentication and have worked and I am still working on methods for mobile phone and Internet of things (IOT) authentication. I also have great interest in Machine learning algorithms.

My current research is an analysis of Heart rate Variability for authentication ad wellbeing assessment.

Timibloudi Enamamu

Dr. Enamamu received his BSc in Communications Systems from the London Metropolitan University in 2009 and his MSc in Telecommunication Engineering from Middlesex University in 2012, and a Ph.D. degree in Electronics and Communication Engineering in 2019 from the University of Plymouth all in the UK. He is a lecturer in the Department of Computing, Sheffield Hallam University, Sheffield, U.K. His research interests include mobile security, transparent authentication, m-health data security, and biometrics. Dr. Enamamu is a member of the IEEE. He is a reviewer for IEEE Access and MDPI Sensor Journals.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763156

Aliyu Dahiru

E. Adewumi, T. Enamamu, A. Dahiru
“Performance Evaluation of Mobile Sensor for Context Awareness User Authentication”,
Latin-American Journal of Computing (LAJC), vol. 9, no. 2, 2022.