



Article

Wearable Sensor-Based Behavioral User Authentication Using a Hybrid Deep Learning Approach with Squeeze-and-Excitation Mechanism [†]

Sakorn Mekruksavanich ¹ and Anuchit Jitpattanakul ^{2,3,*}

¹ Department of Computer Engineering, School of Information and Communication Technology, University of Phayao, Phayao 56000, Thailand; sakorn.me@up.ac.th

² Department of Mathematics, Faculty of Applied Science, King Mongkut's University of Technology North Bangkok, Bangkok 10800, Thailand

³ Intelligent and Nonlinear Dynamic Innovations Research Center, Science and Technology Research Institute, King Mongkut's University of Technology North Bangkok, Bangkok 10800, Thailand

* Correspondence: anuchit.j@sci.kmutnb.ac.th

[†] This paper is an extended version of our paper published in 24th International Conference on Computational Science and Its Applications (ICCSA 2024), Hanoi, Vietnam, 1–4 July 2024.

Abstract: Behavior-based user authentication has arisen as a viable method for strengthening cybersecurity in an age of pervasive wearable and mobile technologies. This research introduces an innovative approach for ongoing user authentication via behavioral biometrics obtained from wearable sensors. We present a hybrid deep learning network called SE-DeepConvNet, which integrates a squeeze-and-excitation (SE) method to proficiently simulate and authenticate user behavior characteristics. Our methodology utilizes data collected by wearable sensors, such as accelerometers, gyroscopes, and magnetometers, to obtain a thorough behavioral appearance. The suggested network design integrates convolutional neural networks for spatial feature extraction, while the SE blocks improve feature identification by flexibly recalibrating channel-wise feature responses. Experiments performed on two datasets, HMOG and USC-HAD, indicate the efficacy of our technique across different tasks. In the HMOG dataset, SE-DeepConvNet attains a minimal equal error rate (EER) of 0.38% and a maximum accuracy of 99.78% for the Read_Walk activity. Our model presents outstanding authentication (0% EER, 100% accuracy) for various walking activities in the USC-HAD dataset, encompassing intricate situations such as ascending and descending stairs. These findings markedly exceed existing deep learning techniques, demonstrating the promise of our technology for secure and inconspicuous continuous authentication in wearable devices. The suggested approach demonstrates the potential for use in individual device security, access management, and ongoing uniqueness verification in sensitive settings.

Keywords: behavior user authentication; wearable sensors; deep learning; squeeze-and-excitation networks; continuous authentication



Citation: Mekruksavanich, S.; Jitpattanakul, A. Wearable Sensor-Based Behavioral User Authentication Using a Hybrid Deep Learning Approach with Squeeze-and-Excitation Mechanism. *Computers* **2024**, *13*, 337. <https://doi.org/10.3390/computers13120337>

Academic Editor: Wenbing Zhao

Received: 9 November 2024

Revised: 4 December 2024

Accepted: 12 December 2024

Published: 14 December 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In an age marked by the prevalence of smartphones and watches, safeguarding the safety and confidentiality of individual data has become increasingly essential [1,2]. Conventional authentication techniques, including passwords and PINs, are susceptible to several attacks and fail to offer ongoing security during an individual's experience [3]. This constraint has generated curiosity regarding behavior-based verification platforms, which utilize the unique characteristics of an individual's actions to continually and inconspicuously authenticate their true identity [4].

Wearable appliances integrated with various sensors, including accelerometers, gyroscopes, and heart rate tracking devices, provide a substantial repository of behavior

information [5,6]. These sensors can detect subtle variations in an individual's motions, bodily reactions, and daily activities, delivering a complex psychological pattern that is challenging to duplicate. The continuous data flow from these sensors facilitates real-time authentication, augmenting security without detracting from users' experience [7].

Recent developments in deep learning have transformed the domain of psychological biometrics [8,9]. Deep neural networks are proficient in identifying intricate patterns in high-dimensional data, rendering them ideal for representing individuals' behavior complexities [10]. Even with advancements, current methodologies frequently encounter difficulties due to wearable sensor data's fluctuating and complex characteristics, resulting in inadequate authentication effectiveness.

Despite the potential of deep learning methods in sensor-based authentication, certain constraints remain in current research. Numerous contemporary models encounter challenges due to the significant unpredictability and noise in wearable sensor data [11–13]. This results in varying effectiveness among various users and activities. Moreover, most methodologies regard all sensor channels uniformly, neglecting the differing significance of various variables in differentiating user actions. Particular research has utilized intricate structures that, although efficient, incur substantial computational expenses and energy usage. While the main authentication processing occurs on separate computing devices, wearable devices still face energy constraints in their crucial role of continuous sensor data collection and transmission—a consideration that influences the overall system design and efficiency [14,15].

Furthermore, many current models lack interpretability, making it difficult to identify which personality traits have the greatest influence on authentication decisions [16,17]. A significant deficiency exists concerning the temporal dynamics of user behavior, as several contemporary methodologies concentrate predominantly on static feature extraction, failing to sufficiently describe long-term interdependence in behavioral patterns. Ultimately, the issue of continuous authentication, necessitating immediate processing and adaptation to incremental shifts in user behavior, needs to be more adequately handled in several deep learning-based systems [18]. Our suggested methodology seeks to mitigate these constraints by employing a hybrid architecture and integrating the squeeze-and-excitation (SE) process [19,20], providing a more resilient, productive, and versatile alternative for behavior-based authentication via wearable sensors.

This research tackles these challenges by introducing an innovative hybrid deep learning network that integrates an SE method. Our methodology integrates the advantages of convolutional neural networks (CNNs) for spatial feature extraction with SE blocks to augment the network's capacity to concentrate on the most salient information, enhancing its resilience to noise and fluctuations in sensor input. The primary contributions of this study are as follows:

- We propose a novel hybrid deep learning architecture that combines CNNs with SE blocks to achieve behavior-based user authentication using wearable sensor data.
- Our approach demonstrates the effectiveness of SE blocks in enhancing feature discrimination, thereby improving overall authentication accuracy.
- We conduct extensive evaluations on a diverse dataset of daily activities, validating the proposed methodology's robustness and generalizability.

This paper is structured as follows: Section 2 examines the pertinent literature on behavior-based authentication and deep learning methodologies. Section 3 delineates our suggested methodology, encompassing the network architecture and the SE mechanism. Section 4 delineates the experimental configuration and findings. Section 5 presents the findings, while Section 6 finishes the paper by addressing the consequences and potential next steps.

2. Related Works

The past several years have witnessed substantial progress in behavior-based user authentication via wearable sensors, motivated by the widespread adoption of mobile

and wearable technology and the growing demand for reliable, ongoing authentication techniques. This section summarizes the pertinent literature, concentrating on two primary domains: sensor-based authentication and behavioral user authentication. We analyze the progression of technologies that use sensors in mobile gadgets and their utilization in biometric authentication solutions. Furthermore, we examine diverse methodologies for behavior-based authentication, emphasizing new research that employs machine learning and deep learning techniques to assess user activity characteristics. By examining these pertinent studies, we seek to situate our study within the expansive domain of continuous authentication and highlight the originality and prospective benefits of our proposed SE-DeepConvNet model. This evaluation aims to pinpoint deficiencies in current methodologies, which our research intends to rectify.

2.1. Sensor-Based User Authentication

Sensors are becoming advanced as portable technology progresses swiftly. The latest mobile phone releases feature GPS, imaging cameras, microphones, ambient light sensors, 3D touchscreens, and accelerometers, among other components [21,22]. A multitude of sensors facilitate many interactions on contemporary mobile phones. Nonetheless, numerous sensors are devoid of individual accessibility [23]. These attributes are derived from several modern mobile sensors. Biometric authentication could be a suitable option for people who prefer not to use PINs or passwords [24]. On the contrary, non-biometric procedures rely on the owner's authorization or confidentiality to verify identity. Behavioral and physiological biometrics are two distinct categories. These strategies can effectively thwart identity theft and unauthorized access to mobile terminal capabilities. Smartphones equipped with biometrics are readily available, reducing the expense of biometric sensors [25]. The accelerometers embedded in the individual's typical movement illustrate the potential of non-invasive biometric gait evaluations [26]. In addition to the accelerometer, smartphone owners possess alternative authentication methods [27]. Accelerometers have become an essential tool for motion detection.

2.2. Behavioral User Authentication

Numerous investigations have illustrated the adaptability of sensor data for implicit authentication, evidencing its capacity to record user activities. Lee et al. [28] demonstrated the efficacy of smartphone sensors for implicit authentication, attaining an acceptable false rejection rate (FRR) of 0.9% and a moderate false acceptance rate (FAR) of 2.8%. This research underscores the effectiveness of sensor-based biometrics in differentiating authentic individuals from impostors. Shen et al. [29] performed an extensive assessment utilizing sensor data and ten one-class detectors, achieving a notable equal error rate (EER) of 2.21%. As the area advances, additional investigation and development of sensor-based authentication techniques are expected to improve security and user experience in portable gadget innovation. Sensor-based authentication utilizes many data sources, including accelerometers, gyroscopes, and magnetometers, to gather comprehensive information regarding individual motions, device orientation, and context in the surroundings. These extensive data allow the system to construct a detailed profile of the individual's behavior, improving its ability to differentiate between authentic users and impostors reliably [30]. A primary benefit of sensor-based authentication is its capacity to function constantly in the background without requiring specific user actions. This constant surveillance enables the system to identify irregularities instantaneously, facilitating continuous authentication that enhances security without disrupting the user experience. A significant problem of sensor-based authentication is its vulnerability to external conditions that could bring noise or fluctuation into the data. Alterations in the individual's surroundings, such as traveling in a vehicle or traversing uneven surfaces, may influence sensor observations, potentially resulting in elevated false rejection or acceptance rates [28]. Aggregating and analyzing sensor data for authentication purposes presents possible privacy issues. Individuals may be apprehensive about how their activities and habits are surveilled, even if the data are

utilized exclusively for security reasons. It is imperative to guarantee that data-collecting methods are transparent and securely managed to alleviate these worries [29].

3. Methodology

This section provides a comprehensive overview of our proposed methodology for behavior-based user identification by using wearable sensors. We present SE-DeepConvNet, an innovative hybrid deep learning structure integrating SE blocks into a CNN framework. Our approach includes crucial steps such as data gathering from wearable sensors, pre-processing strategies to improve the quality of signals, and building the SE-DeepConvNet model. We examine the datasets utilized in our investigation and the pre-processing techniques implemented on the raw sensor data. Subsequently, we present a comprehensive elucidation of the SE-DeepConvNet architecture, emphasizing the function of SE blocks in enhancing feature discrimination. We delineate the assessment indicators employed to analyze the effectiveness of our model relative to benchmark methodologies. We intend to illustrate the efficacy of our suggested approach in tackling the issues of continuous authentication in mobile and wearable device environments through this complete technique.

Figure 1 depicts the suggested framework for gait-based continuous authentication utilizing wearable sensors. The framework comprises numerous essential phases in the authentication steps. Initially, unprocessed sensor data are gathered from wearable devices, typically comprising accelerometers, gyroscopes, and possibly more sensors. The data are thereafter subjected to pre-processing to clean and normalize the signals. The pre-processed data are input into a hybrid deep learning network, which becomes the fundamental component of the authentication system. This network integrates CNNs for spatial feature extraction and recurrent neural networks (RNNs) for temporal modeling and employs SE blocks to improve feature discrimination. The outcome of this hybrid network is utilized to perform authentication determinations, assessing if the present individual's gait pattern corresponds with the recorded profile of the authorized user. This ongoing authentication procedure facilitates real-time validation of the individual's identification through their gait patterns, offering a safe and discreet means of access control for wearable and portable gadgets.

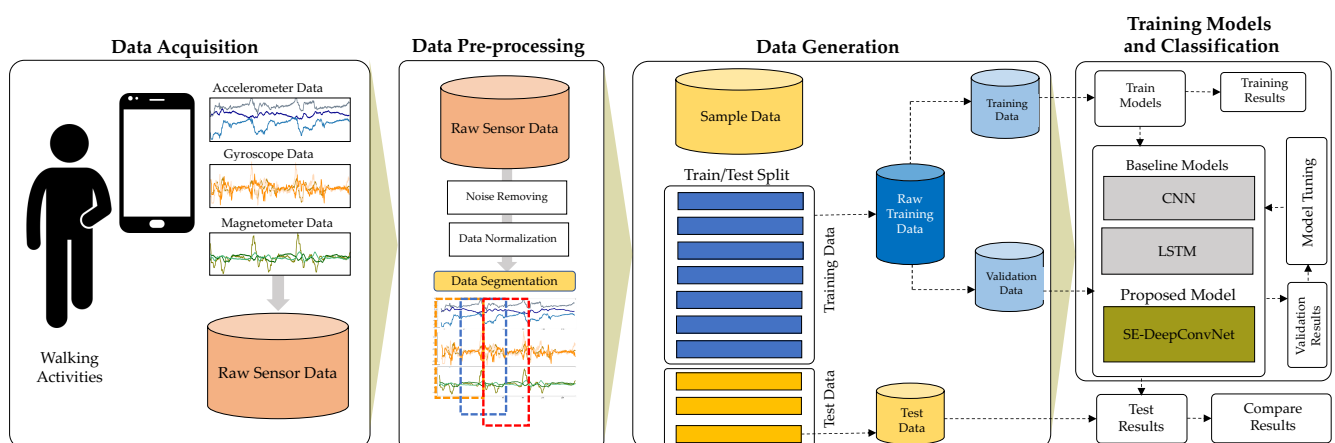


Figure 1. The proposed framework of gait-based continuous authentication using wearable sensors.

3.1. Data Acquisition

To assess the efficacy and resilience of our proposed SE-DeepConvNet model, we employed two separate datasets that encompass a diverse array of user actions and behaviors via wearable sensors. The datasets include the HMOG (Hand Movement, Orientation, and Grasp) dataset and the USC-HAD (University of Southern California Human Activity Dataset). The HMOG dataset concentrates on smartphone user behavior across diverse everyday tasks, whereas the USC-HAD includes a range of walking actions. Utilizing these two complimentary datasets, we intend to illustrate the versatility and efficacy of

our methodology across many contexts of wearable sensor-based authentication. The subsequent subsections offer comprehensive descriptions of each dataset, encompassing their collecting processes, sensor varieties, and the particular actions they address.

3.1.1. HMOG Dataset

The HMOG dataset was compiled and made accessible to everyone [31]. The dataset comprises accelerometer, gyroscope, and magnetometer data pertaining to tap-based properties, including x-y coordinates, finger-covered area, and pressure, collected from 100 smartphone users (53 male, 47 female) during 24 intervals. The data were collected in an appropriately controlled setting throughout multiple intervals of smartphone usage, and each period comprised designated actions classified as reading, writing, or map exploration. Moreover, each exercise was performed while both seated and ambulating. Each encounter was replicated four times, resulting in 24 interactions per subject overall. The dataset comprised accelerometer, gyroscope, and magnetometer sensor data, operating at 100 Hz. Each individual documented six distinctive experience scenarios. Furthermore, sensor data from screen interactions, including touch, keypress, scroll, pinch, and stroke, were documented; however, these were extraneous to this investigation.

3.1.2. USC-HAD

The USC Human Activity Dataset (USC HAD) [32] is the second dataset captured utilizing MotionNode devices equipped with tri-axial sensors, including an accelerometer, gyroscope, and magnetometer. This study's sampling frequency was 100 Hz. The dataset consists of data on movement from 14 participants, seven males and seven females, aged 21 to 49, engaged in 12 tasks.

3.2. Data Pre-Processing

The unprocessed sensor data sources underwent initial processing to purify the signals and standardize their distributions. Filtering procedures were utilized to eliminate noise from the sensor inputs. Subsequently, the processed signals from accelerometers and gyroscopes were normalized to reduce discrepancies from varying sensor scales. The analyzed multi-sensor time series were ultimately segmented into non-overlapping intervals, each lasting 2.56 s, via a sliding window methodology. The segmentation technique produced fixed-length samples that capture user behavior characteristics over time, offering organized input for later learning algorithms to examine.

3.3. The Proposed SE-DeepConvNet Model

This study introduces SE-DeepConvNet, a streamlined CNN developed for continuous authentication utilizing sensor data. The model independently generates spatial representations employing convolutional layers directly from the raw input streams. SE blocks are subsequently implemented to adjust feature reactions on a channel-wise basis, enhancing relevant features, while training, supplementary batch normalization, and ReLU activation layers attain enhanced optimization, standardizing activations and mitigating the vanishing gradient problem. As depicted in Figure 2, this integrated framework efficiently acquires unique personality features from sensor data noise, hence assuring reliable user authentication.

3.4. Convolutional Block

A predetermined collection of components is generally utilized when employing a CNN. CNNs are frequently employed in supervised learning. Generally, these neural networks connect each neuron to every other neuron in the subsequent network layers. The neural network's activation function transforms the neurons' input value into the output value. Two critical factors affect the efficacy of the activation function. This encompasses sparsity and the ability of the neural network's bottom layers to withstand diminished

gradient flow. CNNs commonly utilize pooling as a method for decreasing dimensionality. Max-pooling and average-pooling are both frequently employed techniques.

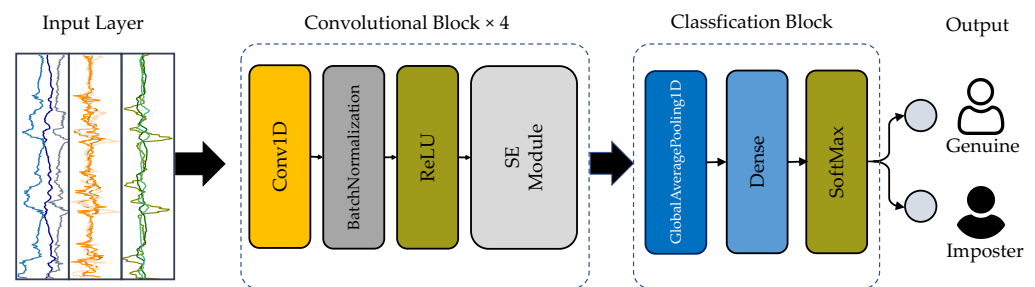


Figure 2. The proposed SE-DeepConvNet Model.

Convolutional blocks (ConvBs) are employed in this research to discern low-level features from raw sensor data. Figure 2 illustrates that ConvBs consist of four layers: one-dimensional convolutional (Conv1D), batch normalization (BN), exponential linear unit (ELU), and max-pooling (MP). Numerous comprehensible convolutional kernels develop unique characteristics in Conv1D, with each kernel generating a feature map. The batch normalization layer was used to regulate and accelerate the training phase. The ELU layer was employed to enhance the model's expressive capacity. The MP layer condensed the feature map while preserving the most vital components.

3.5. Squeeze-and-Excitation Mechanism

Figure 3 shows the design of an SE component. After the convolution process, several feature maps are generated. However, specific feature maps could include redundant data. The SE module executes feature recalibration to enhance prominent features and deactivate less advantageous ones. This component comprises two aspects: the squeezing step and the excitation step.

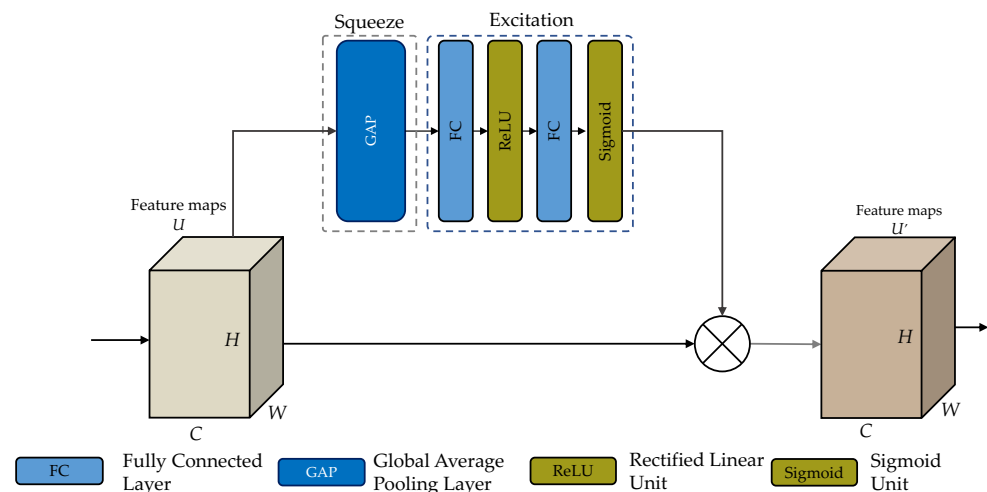


Figure 3. Structure of the SE module.

3.6. Evaluation Metrics

To thoroughly evaluate the efficacy of our proposed SE-DeepConvNet model and compare it with standard techniques, we utilize various conventional assessment criteria often employed in biometric identification systems. These indicators offer insights into the model's capacity to verify legitimate users while dismissing impostors accurately. The principal metrics employed are:

1. False acceptance rate (*FAR*): This indicator denotes the likelihood that the system erroneously recognizes an impostor as an authentic user. It is computed as:

$$FAR = \frac{\text{quantity of fraudulent acceptances}}{\text{quantity of impostor tries}} \quad (1)$$

2. False rejection rate (*FRR*): This indicator denotes the likelihood that the system erroneously denies access to an authentic user. *FRR* is computed as:

$$FRR = \frac{\text{number of false rejections}}{\text{number of legitimate attempts}} \quad (2)$$

3. Equal error rate (*EER*): This is the point at which the *FAR* and *FRR* are equivalent. A reduced *EER* signifies superior overall system performance. The system's judgment threshold is adjusted until the *FAR* equals the *FRR*. *EER* is computed using the accompanying formula:

$$EER = \frac{FAR + FRR}{2} \quad (3)$$

where $|FAR + FRR|$ is the smallest value.

4. Accuracy: This measure denotes the comprehensive correctness of the authentication system. It is computed as:

$$\text{Accuracy} = \frac{\text{true positives} + \text{true negatives}}{\text{total number of attempts}} \quad (4)$$

4. Experiments and Results

This section outlines the investigations to evaluate the presented SE-DeepConvNet model for continuous authentication. We evaluate the model's effectiveness using a publicly known dataset incorporating data from accelerometer, gyroscope, and magnetometer sensors. We offer insights on assessment criteria, comparisons with baseline models, parameter environments, and accuracy studies across diverse sensing modalities. The significant results provide advanced authentication rates, supporting the successful integration of SE blocks into deep CNNs for the dependable identification of users from movement sequences obtained from wearable appliances.

4.1. Experimental Setting

This study is performed using Python on Google Colab Pro+ and a Tesla V100 GPU to accelerate simulations. The evaluations compare the suggested SE-DeepConvNet model with traditional deep learning architectures, including regular CNNs and LSTM networks, particularly for continuous sensor data authentication. The comparison results measure improvements in identification attained by integrating SE blocks into our deep convolutional network.

We established a systematic evaluation process for thorough cross-user validation. For each user *i*-th in the dataset, we performed authentication trials in which that person's sensor data were classified as valid. In contrast, data from all other users were regarded as imposters. This method guarantees a comprehensive assessment of the model's capacity to differentiate between authentic users and imposters across various user groupings. The cross-user validation technique was uniformly implemented across the HMOG dataset (100 users) and the USC-HAD (14 users), yielding a comprehensive evaluation of the model's efficacy in distinguishing between authentic users and imposters throughout varied populations.

Acknowledging that this high-performance equipment was employed solely during the study and training phase is essential. In actual applications, the trained model functions on conventional server infrastructure, whereas wearable devices are exclusively tasked with data collection and transmission. This deployment model assures that computational

demands do not encumber resource-limited wearable devices, as they are solely responsible for sensor data collection and safe transmission to the authentication servers where the processing transpires.

4.2. Experimental Results

The following part provides a thorough examination of the results of experimentation from our SE-DeepConvNet model and compares its efficiency with standard deep learning methods. Our assessment includes two separate datasets: the HMOG dataset, which examines smartphone user behavior, and the USC-HAD, which records various walking behaviors. We evaluate the models' efficacy through critical parameters, including EER and accuracy indicators, offering insights into their capacity to authenticate users via behavioral biometrics. The subsequent subsections examine the distinct effectiveness findings for each dataset, emphasizing the advantages of our SE-DeepConvNet model in tackling the issues of continuous authentication through wearable sensor data. These findings provide evidence for the robustness and superiority of our proposed strategy across diverse real-world circumstances.

4.2.1. Performance Analysis on HMOG Dataset

The current section presents and analyzes the effectiveness of our SE-DeepConvNet model on the HMOG dataset, which records smartphone user behavior across different tasks. We evaluate our model against standard CNN and LSTM methodologies across three scenarios: Read_Walk, Write_Walk, and Map_Walk. We assess the models' efficacy in user authentication by employing EER and accuracy as primary measures, focusing on behavioral patterns exhibited during the standard use of smartphones. This investigation seeks to illustrate the efficacy and competitiveness of SE-DeepConvNet for continuous authentication in practical portable device engagements. The findings from the experiment are summarized in Table 1.

Table 1. Performance metrics of baseline deep learning models including the proposed SE-DeepConvNet using MHOG dataset.

Gait-Based Activity	CNN		LSTM		SE-DeepConvNet	
	EER	Accuracy	EER	Accuracy	EER	Accuracy
Read_Walk	0.75%(±2.67%)	99.51%(±1.73%)	0.60%(±1.81%)	99.60%(±1.21%)	0.38%(±1.13%)	99.78%(±0.67%)
Write_Walk	1.33%(±2.86%)	99.09%(±1.86%)	1.55%(±2.79%)	98.97%(±1.82%)	1.26%(±2.32%)	99.13%(±1.55%)
Map_Walk	1.24%(±4.73%)	99.08%(±4.25%)	0.77%(±1.44%)	99.48%(±0.96%)	0.83%(±1.40%)	99.43%(±0.98%)

Table 1 presents the effectiveness of the SE-DeepConvNet model for ongoing authentication tasks using the MHOG dataset, comparing its performance against standard CNN and LSTM models. The SE-DeepConvNet consistently outperforms in three specific activities—Read_Walk, Write_Walk, and Map_Walk—demonstrating its capability by achieving the lowest EER and highest accuracy rates, particularly for Read_Walk (0.38% EER, 99.78% accuracy) and Write_Walk (1.26% EER, 99.13% accuracy). For Map_Walk, SE-DeepConvNet nearly matches the best performance seen with the LSTM model. Each model achieves high accuracy (over 98.9%) across all activities, with Read_Walk being the easiest to authenticate and Write_Walk presenting the most challenges. The slight differences in performance suggest that each model is effective; nonetheless, SE-DeepConvNet's leading results across multiple scenarios indicate that including SE blocks within the deep convolutional network enhances ongoing authentication through wearable sensor data. These findings underscore the robustness and efficiency of the SE-DeepConvNet model for behavior-based user authentication.

4.2.2. Performance Analysis on USC-HAD

The following part provides a detailed examination of the effectiveness of our SE-DeepConvNet model on the USC-HAD, which includes various walking behaviors. We

evaluate the model we suggest against conventional CNN and LSTM methodologies across five diverse walking scenarios: Walking Forward, Walking Left, Walking Right, Walking Upstairs, and Walking Downstairs. We evaluate each model's capacity to authenticate users based on their gait patterns in different tasks employing EER and accuracy as the significant criteria. This investigation intends to illustrate the adaptability and efficacy of SE-DeepConvNet in detecting nuanced variations in walking manners, highlighting its prospect for reliable continuous authentication in wearable appliance applications. The results are presented in Table 2.

Table 2. Performance metrics of baseline deep learning models including the proposed SE-DeepConvNet using USC-HAD dataset.

Gait-Based Activity	CNN		LSTM		SE-DeepConvNet	
	EER	Accuracy	EER	Accuracy	EER	Accuracy
Walking Forward	7.37%(±3.99%)	94.81%(±2.62%)	5.46%(±2.30%)	95.68%(±1.71%)	0.07%(±0.25%)	99.97%(±0.12%)
Walking Left	11.78%(±8.15%)	92.66%(±5.95%)	5.47%(±3.85%)	95.62%(±3.76%)	0.00%(±0.00%)	100.00%(±0.00%)
Walking Right	6.01%(±7.08%)	96.38%(±4.77%)	2.18%(±1.58%)	98.66%(±0.92%)	0.00%(±0.00%)	100.00%(±0.00%)
Walking Upstairs	14.11%(±7.70%)	90.95%(±4.97%)	12.98%(±10.15%)	89.39%(±9.43%)	0.00%(±0.00%)	100.00%(±0.00%)
Walking Downstairs	19.20%(±10.70%)	86.03%(±9.82%)	21.76%(±13.40%)	81.32%(±11.81%)	0.00%(±0.00%)	100.00%(±0.00%)

Table 2 details the performance metrics of baseline deep learning models, including the proposed SE-DeepConvNet, as applied to the USC-HAD. Results reveal a significant improvement in authentication accuracy across various walking activities when using SE-DeepConvNet compared to traditional CNN and LSTM models.

For the Walking Forward activity, SE-DeepConvNet achieves an impressively low equal error rate (EER) of 0.07% and a high accuracy rate of 99.97%. These results surpass those of the CNN (EER: 7.37%, accuracy: 94.81%) and LSTM (EER: 5.46%, accuracy: 95.68%) models, highlighting SE-DeepConvNet's capability to distinguish unique gait patterns during forward movement effectively.

SE-DeepConvNet demonstrates perfect authentication with 0% EER and 100% accuracy for both actions in the Walking Left and Walking Right activities. This is a marked improvement over the CNN and LSTM models, which display significantly higher EERs and lower accuracy scores. For Walking Left, CNN shows an EER of 11.78% with 92.66% accuracy, while LSTM performs better, achieving an EER of 5.47% and an accuracy of 95.62%. The outstanding results of SE-DeepConvNet in these activities suggest its effectiveness in capturing subtle directional gait distinctions.

In more complex movements like ascending and descending Stairs, SE-DeepConvNet also achieves flawless performance (0% EER, 100% accuracy). In contrast, CNN and LSTM models struggle, displaying significantly higher EERs and reduced accuracy levels. For instance, in the Walking Downstairs activity, the CNN records an EER of 19.20% and an accuracy of 86.03%, while LSTM's performance is lower, with an EER of 21.76% and an accuracy of 81.32%. This clear performance gap emphasizes SE-DeepConvNet's ability to handle complex gait patterns effectively.

Overall, the findings highlight SE-DeepConvNet's outstanding performance across all tested walking behaviors in the USC-HAD. Its ability to achieve near-perfect or flawless authentication in diverse walking scenarios, including challenging activities like stair climbing, underscores its robustness and efficiency for continuous authentication based on gait analysis. This substantial improvement over traditional deep learning models indicates that SE-DeepConvNet's hybrid structure, combined with SE blocks, is advantageous for distinguishing unique gait features in wearable sensor data.

5. Discussion

5.1. Performance Analysis Across Different Behavioral Activities

Our experimental results illustrate the strong efficacy of the SE-DeepConvNet model in managing various patterns of behavior for continuous user authentication using wearable

sensor data. The model demonstrates outstanding effectiveness on the HMOG and USC-HAD datasets, highlighting its adaptability in user authentication across diverse daily tasks.

In the HMOG dataset, which reflects authentic smartphone usage patterns, SE-DeepConvNet exhibits improved efficiency relative to conventional CNN and LSTM structures. The model attains remarkable outcomes in the Read_Walk movement, exhibiting an EER of 0.38% and an accuracy of 99.78%. This outstanding achievement in a typical real-world situation—reading while walking—underscores the model's practical utility. The excellent efficiency in Write_Walk and Map_Walk actions further corroborates the model's capacity to authenticate users across various interaction patterns, indicating its efficacy in practical mobile device utilization contexts.

The results obtained from the USC-HAD are awe-inspiring, as SE-DeepConvNet attains flawless authentication measurements (0% EER, 100% accuracy) across diverse walking activities. The model sustains its outstanding achievement even under demanding situations like ascending and descending stairs, where conventional CNN and LSTM models exhibit considerable capacity decline. The significant efficiency disparity can be ascribed to the SE blocks' capacity to weight various sensor channels adaptively. This enables the model to discern nuanced differences in gait patterns under diverse walking settings.

The sustained superior results across all datasets indicate that SE-DeepConvNet proficiently identifies and utilizes unique behavioral traits in detailed interactions (smartphone usage) and broad motor activity (walking patterns). This adaptability renders it especially appropriate for practical applications where consumers participate in diverse activities while utilizing their devices.

5.2. Practical Applications

Although our SE-DeepConvNet model demonstrates outstanding accuracy in distinguishing between authentic users and impostors, we recognize that practical applications require a more sophisticated method for authentication determinations. We suggest adding a third uncertain type when the model's confidence is below a specified threshold. This allows for a seamless transition to alternate authentication methods, such as personal identification numbers or biometric identification. This is especially significant during abrupt alterations to bodily action, such as shifting from walking to running, where sensor data patterns may momentarily diverge from existing baseline levels. The system can be engineered to employ adaptive authentication by continuously modifying its decision thresholds based on different variables, such as contextual understanding (location and time), user activity adjustments, the quality of signals from wearable sensors, and past authentication arrangements. This approach facilitates the application of varying security policies according to the context, wherein high-security applications necessitate elevated confidence thresholds and increased secondary authentication frequency.

In contrast, less sensitive applications may uphold more permissive thresholds. In order to successfully implement this improved decision structure, several essential aspects must be handled, including determining suitable confidence thresholds through empirical analysis, facilitating seamless transitions between authentication techniques, preserving a positive user experience by eliminating superfluous secondary authentication requests, and consistently tracking and assessing ambiguous situations to enhance the effectiveness of the model. This triadic decision process offers a more resilient and pragmatic method for continuous authentication in practical applications, recognizing and mitigating the intrinsic variability in individual conduct and sensor data quality, thereby presenting a more sophisticated and efficient solution for the real-world implementation of behavioral authentication systems.

5.3. Limitations

Although our analysis reveals encouraging outcomes with the SE-DeepConvNet model, different constraints must be recognized. While the HMOG and USC-HAD datasets encompass a variety of actions taken by users, they may only comprehensively reflect some

real-world situations. The datasets were gathered under controlled circumstances and may not encompass the complete spectrum of environmental variables that could influence sensor readings in real-world applications. Moreover, our experimental data are derived from gadgets in accurate, consistent locations. In contrast, in practical applications, individuals might use or transport their gadgets variably, which could influence sensor readings and the precision of authentication. A further issue is that our datasets fail to consider temporal variations in user behavior, including long-term alterations in movement patterns resulting from tiredness, injury, or elderly users. The present research needs to thoroughly examine the influence of varying sensor quality and specifications among different gadgets that are worn, which may affect the device's efficacy in practical applications.

These constraints indicate possibilities for potential studies on aspects such as data acquisition across varied circumstances and sensor placements, examination of the model's adaptability to various sensor arrangements, and creation of strategies to address long-term alterations in user behavior patterns while preserving authentication accuracy.

5.4. Privacy Considerations in Continuous Authentication

Although continuous behavioral authentication provides improved security, it has considerable privacy issues that require further examination. The continuous accumulation of data collected by sensors on worn gadgets generates a comprehensive digital footprint of individuals' daily actions and habits, possibly disclosing sensitive information regarding their routines, physical activities, and wellness issues.

To mitigate these privacy points, multiple preventative strategies must be introduced. Data processing should be conducted locally whenever feasible, reducing unprocessed behavioral data transmission. The authentication system must utilize robust encryption techniques for data transfer and preservation, establish explicit data retention regulations, and offer consumers direct control over their data. Moreover, privacy-preserving methodologies like data anonymization and feature extraction at the edge can safeguard user privacy while ensuring authentication efficacy. These procedures guarantee that the system can authenticate individuals successfully while safeguarding their privacy privileges. The subsequent implementations of behavioral authentication methods must meticulously balance the trade-off between authentication precision and privacy protection.

6. Conclusions and Future Works

This work presents SE-DeepConvNet, an innovative hybrid deep learning structure for continuous user authentication utilizing wearable sensor data. Our methodology, incorporating SEblocks within a CNN framework, has improved efficiency across many tasks, continuously surpassing conventional CNN and LSTM models. The model's resilience throughout many scenarios, from smartphone utilization to intricate walking behaviors, signifies its applicability in real-world contexts.

Despite the encouraging results, subsequent research should concentrate on several critical domains: enhancing real-time implementation on resource-limited devices, creating adaptive learning systems to address gradual shifts in user behavior, examining multi-modal fusion and privacy-preserving strategies, assessing adversarial robustness, executing larger-scale investigations, and formulating context-aware authentication techniques. As we further refine and expand this methodology, SE-DeepConvNet signifies a substantial advancement toward achieving genuinely secure, unobtrusive, and user-friendly authentication systems for the digital era, responding to the increasing demand for improved security in the pervasive environment of mobile and wearable devices.

Author Contributions: Conceptualization, S.M. and A.J.; methodology, S.M.; software, A.J.; validation, A.J.; formal analysis, S.M.; investigation, S.M.; resources, A.J.; data curation, A.J.; writing—original draft preparation, S.M.; writing—review and editing, A.J.; visualization, S.M.; supervision, A.J.; project administration, A.J.; funding acquisition, S.M. and A.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the University of Phayao; the Thailand Science Research and Innovation Fund (Fundamental Fund 2025, Grant No. 5014/2567); the National Science, Research and Innovation Fund (NSRF); and King Mongkut's University of Technology North Bangkok (contract no. KMUTNB-FF-68-B-03).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: To clarify, our research utilizes a pre-existing, publicly available dataset. The dataset has been anonymized and does not contain any personally identifiable information. We have cited the source of the dataset in our manuscript and have complied with the terms of use set forth by the dataset provider.

Data Availability Statement: The original data presented in the study are openly available for the HMOG dataset at <https://hmog-dataset.github.io/hmog/> (accessed on 9 September 2024) and the USC-HAD of the University of Southern California at <https://sipi.usc.edu/had/> (accessed on 9 September 2024).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Shuwandy, M.L.; Jouda, A.; Ahmed, M.; Salih, M.M.; Al-Qaysi, Z.; Alamoodi, A.; Garfan, S.; Albahri, O.; Zaidan, B.; Albahri, A. Sensor-based authentication in smartphone: A systematic review. *J. Eng. Res.* 2024, *in press*. [CrossRef]
2. Fúster, J.; Solera-Cotanilla, S.; Pérez, J.; Vega-Barbas, M.; Palacios, R.; Álvarez-Campana, M.; Lopez, G. Analysis of security and privacy issues in wearables for minors. *Wirel. Netw.* 2024, *30*, 5437–5453. [CrossRef]
3. Hernández-Álvarez, L.; de Fuentes, J.M.; González-Manzano, L.; Hernández Encinas, L. Privacy-Preserving Sensor-Based Continuous Authentication and User Profiling: A Review. *Sensors* 2021, *21*, 92. [CrossRef] [PubMed]
4. Amin, R.; Gaber, T.; ElTaweel, G.; Hassanien, A.E. Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues. In *Bio-Inspiring Cyber Security and Cloud Services: Trends and Innovations*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 423–446. [CrossRef]
5. Malik, M.N.; Azam, M.A.; Ehatisham-Ul-Haq, M.; Ejaz, W.; Khalid, A. ADLAuth: Passive Authentication Based on Activity of Daily Living Using Heterogeneous Sensing in Smart Cities. *Sensors* 2019, *19*, 2466. [CrossRef]
6. Vaghasiya, J.V.; Mayorga-Martinez, C.C.; Pumera, M. Wearable sensors for telehealth based on emerging materials and nanoarchitectonics. *NPJ Flex. Electron.* 2023, *7*, 26. [CrossRef]
7. Chhibbar, L.D.; Patni, S.; Todi, S.; Bhatia, A.; Tiwari, K. Enhancing security through continuous biometric authentication using wearable sensors. *Internet Things* 2024, *28*, 101374. [CrossRef]
8. Pritee, Z.T.; Anik, M.H.; Alam, S.B.; Jim, J.R.; Kabir, M.M.; Mridha, M. Machine learning and deep learning for user authentication and authorization in cybersecurity: A state-of-the-art review. *Comput. Secur.* 2024, *140*, 103747. [CrossRef]
9. Shende, S.W.; Tembhumne, J.V.; Ansari, N.A. Deep learning based authentication schemes for smart devices in different modalities: Progress, challenges, performance, datasets and future directions. *Multimed. Tools Appl.* 2024, *83*, 71451–71493. [CrossRef]
10. Sigcha, L.; Borzi, L.; Amato, F.; Rechichi, I.; Ramos-Romero, C.; Cárdenas, A.; Gascó, L.; Olmo, G. Deep learning and wearable sensors for the diagnosis and monitoring of Parkinson's disease: A systematic review. *Expert Syst. Appl.* 2023, *229*, 120541. [CrossRef]
11. Kang, S.; Paul, A.; Jeon, G. Reduction of mixed noise from wearable sensors in human-motion estimation. *Comput. Electr. Eng.* 2017, *61*, 287–296. [CrossRef]
12. Zhai, B.; Elder, G.J.; Godfrey, A. Challenges and opportunities of deep learning for wearable-based objective sleep assessment. *npj Digit. Med.* 2024, *7*, 85. [CrossRef] [PubMed]
13. Zhang, S.; Li, Y.; Zhang, S.; Shahabi, F.; Xia, S.; Deng, Y.; Alshurafa, N. Deep Learning in Human Activity Recognition with Wearable Sensors: A Review on Advances. *Sensors* 2022, *22*, 1476. [CrossRef] [PubMed]
14. Jiang, N.; Mück, J.E.; Yetisen, A.K. The Regulation of Wearable Medical Devices. *Trends Biotechnol.* 2020, *38*, 129–133. [CrossRef] [PubMed]
15. Tesema, W.; Jimma, W.; Khan, M.I.; Stiens, J.; da Silva, B. A Taxonomy of Low-Power Techniques in Wearable Medical Devices for Healthcare Applications. *Electronics* 2024, *13*, 3097. [CrossRef]
16. Kim, E. Interpretable and Accurate Convolutional Neural Networks for Human Activity Recognition. *IEEE Trans. Ind. Inform.* 2020, *16*, 7190–7198. [CrossRef]
17. Agrawal, V.; Hazratifard, M.; Elmiligi, H.; Gebali, F. Electrocardiogram (ECG)-Based User Authentication Using Deep Learning Algorithms. *Diagnostics* 2023, *13*, 439. [CrossRef]
18. Abuhamad, M.; Abuhmed, T.; Mohaisen, D.; Nyang, D. AUToSen: Deep-Learning-Based Implicit Continuous Authentication Using Smartphone Sensors. *IEEE Internet Things J.* 2020, *7*, 5008–5020. [CrossRef]
19. Hu, J.; Shen, L.; Sun, G. Squeeze-and-Excitation Networks. In Proceedings of the 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–23 June 2018; pp. 7132–7141. [CrossRef]

20. Mekruksavanich, S.; Jitpattanakul, A. Elevating Wearable Sensor Authentication with Hybrid Deep Learning and Squeeze-and-Excitation. In Proceedings of the Computational Science and Its Applications—ICCSA, Hanoi, Vietnam, 1–4 July 2024; Gervasi, O., Murgante, B., Garau, C., Taniar, D., Rocha, A.M.A.C., Faginas Lago, M.N., Eds.; Springer: Cham, Switzerland, 2024; pp. 186–197.
21. Shuwandy, M.L.; Zaidan, B.; Zaidan, A.; Albahri, A.; Alamoodi, A.; Albahri, O.; Alazab, M. mHealth Authentication Approach Based 3D Touchscreen and Microphone Sensors for Real-Time Remote Healthcare Monitoring System: Comprehensive Review, Open Issues and Methodological Aspects. *Comput. Sci. Rev.* **2020**, *38*, 100300. [[CrossRef](#)]
22. Mekruksavanich, S.; Jitpattanakul, A. Identifying Smartphone Users Based on Activities in Daily Living Using Deep Neural Networks. *Information* **2024**, *15*, 47. [[CrossRef](#)]
23. Osman, T.; Mannan, M.; Hengartner, U.; Youssef, A. AppVeto: Mobile application self-defense through resource access veto. In Proceedings of the 35th Annual Computer Security Applications Conference, New York, NY, USA, 9–13 December 2019; ACSAC '19; pp. 366–377. [[CrossRef](#)]
24. Gehrman, C.; Rodan, M.; Jönsson, N. Metadata filtering for user-friendly centralized biometric authentication. *EURASIP J. Inf. Secur.* **2019**, *2019*, 7. [[CrossRef](#)]
25. Shukla, D.; Wei, G.; Xue, D.; Jin, Z.; Phoha, V.V. Body-Taps: Authenticating Your Device Through Few Simple Taps. In Proceedings of the 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, 22–25 October 2018; IEEE Press: Piscataway, NJ, USA, 2018; pp. 1–8. [[CrossRef](#)]
26. Permatasari, J.; Connie, T.; Ong, T.S.; Teoh, A.B.J. Adaptive 1-dimensional time invariant learning for inertial sensor-based gait authentication. *Neural Comput. Appl.* **2023**, *35*, 2737–2753. [[CrossRef](#)]
27. Abdrabou, Y.; Sherif, O.; Eisa, R.M.; Elmougy, A. Human-based fraudulent attempts on gait based profiles. In Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities, New York, NY, USA, 3–7 December 2018; AfriCHI '18. [[CrossRef](#)]
28. Lee, W.H.; Lee, R.B. Implicit Smartphone User Authentication with Sensors and Contextual Machine Learning. In Proceedings of the 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Denver, CO, USA, 26–29 June 2017; pp. 297–308. [[CrossRef](#)]
29. Shen, C.; Chen, Y.; Guan, X. Performance evaluation of implicit smartphones authentication via sensor-behavior analysis. *Inf. Sci.* **2018**, *430–431*, 538–553. [[CrossRef](#)]
30. Jorquera Valero, J.M.; Sánchez Sánchez, P.M.; Fernández Maimó, L.; Huertas Celdrán, A.; Arjona Fernández, M.; De Los Santos Vílchez, S.; Martínez Pérez, G. Improving the Security and QoE in Mobile Devices through an Intelligent and Adaptive Continuous Authentication System. *Sensors* **2018**, *18*, 3769. [[CrossRef](#)] [[PubMed](#)]
31. Yang, Q.; Peng, G.; Nguyen, D.T.; Qi, X.; Zhou, G.; Sitová, Z.; Gasti, P.; Balagani, K.S. A multimodal data set for evaluating continuous authentication performance in smartphones. In Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems (SenSys '14), New York, NY, USA, 3–6 November 2014; pp. 358–359. [[CrossRef](#)]
32. Zhang, M.; Sawchuk, A.A. USC-HAD: A daily activity dataset for ubiquitous activity recognition using wearable sensors. In Proceedings of the Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12), New York, NY, USA, 2012; pp. 1036–1043. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.