Computers, Materials & Continua
DOI: 10.32604/cmc.2023.035173
Article

Tech Science Press

Continuous Mobile User Authentication Using a Hybrid CNN-Bi-LSTM Approach

Sarah Alzahrani[1], Joud Alderaan[1], Dalya Alatawi[1] and Bandar Alotaibi[1,2,*]

[1]Department of Information Technology, University of Tabuk, Tabuk, 71491, Saudi Arabia
[2]Sensor Networks and Cellular Systems Research Center, University of Tabuk, Tabuk, 71491, Saudi Arabia
*Corresponding Author: Bandar Alotaibi. Email: b-alotaibi@ut.edu.sa
Received: 10 August 2022; Accepted: 19 November 2022

Abstract: Internet of Things (IoT) devices incorporate a large amount of data in several fields, including those of medicine, business, and engineering. User authentication is paramount in the IoT era to assure connected devices' security. However, traditional authentication methods and conventional biometrics-based authentication approaches such as face recognition, fingerprints, and password are vulnerable to various attacks, including smudge attacks, heat attacks, and shoulder surfing attacks. Behavioral biometrics is introduced by the powerful sensing capabilities of IoT devices such as smart wearables and smartphones, enabling continuous authentication. Artificial Intelligence (AI)-based approaches introduce a bright future in refining large amounts of homogeneous biometric data to provide innovative user authentication solutions. This paper presents a new continuous passive authentication approach capable of learning the signatures of IoT users utilizing smartphone sensors such as a gyroscope, magnetometer, and accelerometer to recognize users by their physical activities. This approach integrates the convolutional neural network (CNN) and recurrent neural network (RNN) models to learn signatures of human activities from different users. A series of experiments are conducted using the MotionSense dataset to validate the effectiveness of the proposed method. Our technique offers a competitive verification accuracy equal to 98.4%. We compared the proposed method with several conventional machine learning and CNN models and found that our proposed model achieves higher identification accuracy than the recently developed verification systems. The high accuracy achieved by the proposed method proves its effectiveness in recognizing IoT users passively through their physical activity patterns.

Keywords: Human activity recognition; recurrent neural network (RNN); internet of things (IoT); machine learning (ML)

1 Introduction

Smartphones are widely used for an extensive range of activities, from accessing social networks to conducting banking transactions. Smartphones process confidential and sensitive data during these tasks, which are vulnerable to attacks, as they may expose sensitive and confidential information [1]. Typical authentication approaches include pin codes, passwords, and biometrics-based methods, which involve one-time use authentication approaches with user authorization provided only at the start of the session. In contrast, continuous authentication mechanisms provide access control during the entire work session, where the user is authenticated continuously, confirming their identity. Continuous authentication helps manage access during the work session [2]. With the advances in sensor technologies adopted in mobile devices, employing motion behavior as an authentication method has become possible. Moreover, with the recent developments in deep learning and machine learning (ML) algorithms, it is also possible to process and analyze large datasets. Therefore, this study focuses on user authentication using human activities and artificial intelligence approaches [3].

To improve the IoT devices' security and present prospective solutions to current challenges in user authentication, researchers proposed various approaches based on behavioral biometrics. These behavioral biometrics-based methods utilize behavioral traits when IoT interact with their IoT devices and create a way to authenticate different IoT users in passive and continuous manners. Xiaofeng et al. [4] used keystrokes dynamics as a behavioral biometrics methodology and utilized a hybrid deep learning model to authenticate users continuously. Keystroke dynamics-based approaches authenticate users continuously while typing characters through a keyboard, so the authentication continuity of these approaches is bound to the user actions (i.e., typing movement). However, these approaches depend on the activity (e.g., walking, sitting) performed by the user while typing on the keyboard; every activity requires different training to build the patterns of the appropriate predictive model. Li et al. [5] investigated the consistency of touch movement and its applicability to identifying and authenticating IoT devices; the authors extracted the touch features and examined various supervised learning algorithms. However, this kind of approach relies on touch operations which differ among various applications and therefore affect the performance of the prediction model. Papavasileiou et al. [6] proposed a continuous authentication method based on gait cycles extracted from sensor measurements and fed into a hybrid model of autoencoder and SVM. However, gait-based authentication approaches are conducted in labs using burdensome prototypes and high-priced hardware. These approaches are also gaited activity-dependent.

There is vast interest in the research on human activity recognition because it can be employed in various practical uses in real-world applications. The main contribution of this paper is to introduce a new passive and continuous authentication approach that relies on features extracted from IoT devices' built-in sensors (i.e., accelerometer, gyroscope, and magnetometer) and fed into a novel BiLSTM and CNN model to recognize users performing different activities. Unlike the approaches mentioned above [4–6], our method authenticates users passively, is not activity-reliance, relies on the built-in sensors in the IoT devices rather than the applications, and does not require specialized hardware. This study develops an efficient and reliable authentication system based on human activity recognition methods by combining a novel convolutional neural network (CNN) with a recurrent neural network (RNN) model. Our model has been tested using an efficient activity dataset named MotionSense, where at the first stage, a training phase is conducted using the MotionSense dataset. Then, several experiments are conducted to assess the efficiency of the developed user authentication system.

The rest of the paper is organized as follows: Section 2 discusses the recently developed human activity authentication systems and the recent human activity dataset. In Section 3, we discuss

the system implementation, including the project concept and the selected human activity dataset, whereas Section 4 presents the results obtained from several actual experiments conducted to assess the proposed authentication system. In Section 5, we discuss the obtained results and provide a comparison with the recently developed human activity authentication systems. Finally, Section 6 concludes the work presented in this paper.

2 Related Works

This section discusses the currently developed human activity recognition systems. We present the recently collected human activity datasets, which have been employed in human activity authentication systems. Centeno et al. [7] proposed an authentication system based on Siamese CNN to acquire the signatures of motion patterns from different users using a human activity dataset presented in the study by Yang et al. [8] and obtained a verification accuracy reaching 97.8%. The authors found that the proposed algorithm is not sensitive to the sampling frequency and sequence length. The work presented by Shen et al. [9] includes an investigation of the reliability and applicability of employing motion sensors, including the gyroscope, accelerometer, gravity, and magnetometer behavior for active and continuous smartphone authentication across numerous operational scenarios. A systematic evaluation of the behavior's distinctiveness and persistence properties was also presented. The authors showed that motion-sensor behavior reveals appropriate discriminability and stability for the active and continuous authentication and offers a false-acceptance rate of 3.98%, and a false rejection rate of 5.03%.

Abuhamad et al. [10] developed an AUToSen deep-learning-based active authentication system, which exploits the data from sensors in consumer-grade smartphones to authenticate users. AUToSen is based on identifying distinct user behavior from the smartphone-embedded sensors. The authors investigated three diverse deep learning architectures for modeling and capturing the users' behavioral patterns. They revealed that AUToSen operates ideally using the readings of only three sensors: the gyroscope, magnetometer, and accelerometer. The obtained result of the F1-score was ∼98%, with a 6.67% false rejection rate. Ehatisham-ul-Haq et al. [11] proposed a novel authentication system based on smartphone users' behavioral traits by employing embedded sensors in smartphone devices, including a gyroscope, magnetometer, and accelerometer. They used the human activity dataset presented in [12,13]. The developed system also offers a multi-class smart user authentication platform that provides diverse levels of access to a wide range of smartphone users.

A two-step authentication framework was presented by Wu et al. [14], based on an own-built fingertip sensor device that can track physiological and motion data. The dataset was adopted from [15]. The developed framework can recognize a user's identity if the user is wearing the fingertip device. Extensive experiments were executed to validate the effectiveness of the proposed framework, where authors achieved a 98.5% accuracy with an F1 score of 86.67%. Moreover, the work presented by Malik et al. [16] includes the design and development of a heterogenous framework named ADLAuth for passive authentication of the user employing either wearable sensors or smartphone's built-in sensors through analyzing the physical activity patterns of the participants. The authors used multi-class ML models to verify the user identity. In addition, the authors tested three different datasets consisting of heterogeneous sensors for various activities. The employed dataset is presented in [17–19].

Mekruksavanich et al. [20] introduced a new continuous authentication system called Deep-Authen, which identifies smartphone users based on their physical activity patterns measured with

gyroscope, magnetometer, and accelerometer sensors. The employed human activity dataset is presented in [21,22]. In addition, the authors proposed a deep learning classification network named DeepConvLSTM and evaluated it using three different datasets. The results demonstrated that integrating motion-sensor data can achieve high classification accuracy. Volaka et al. [23] investigated the impact of touchscreen-based and sensor-based features with the employment of deep learning methods. HMOG dataset was adopted, which consists of 100 users over 24 sessions. The obtained results include 88% classification accuracy and 15% EER values, including binary classification with several data types.

Centeno et al. [24] present a deep learning autoencoder-based continuous authentication approach with an error rate of 2.2%. The presented system relies on accelerometer data with no requirement for a high number of features, thus minimizing the computational burden. The authors discussed the balance between the number of dimensional features and the re-authentication time, which minimizes as the number of dimensions increases. Verma et al. [25] proposed an algorithm to balance behavioral biometrics with multi-factor authentication by introducing a two-step user verification algorithm that verifies the user's identity using motion-based biometrics. Table 1 shows recent human activity datasets employed in the studies mentioned above. Each dataset has been analyzed by noting the number of participants and employed features (user activity).

Table 1: The recent human activity datasets

Reference	Number of participants	Number of features
[8,23,24]	100	24
[12,13]	10	Six different activities
[15]	40	Five different motions
Human Activity Recognition (HAR) [17]	30	Six different activities
Physical Activity Monitoring (PAMAP2) [18]	9	Eight different activities
MobiAct [19]	59	Nine different activities
WISDM-HARB [21]	51	18 different tasks
Hand Movement, Orientation and Grasp (HMOG) [22]	100	Six different activities
[25]	51	43

3 System Implementation

This project aims to develop an efficient user authentication system based on human activity recognition. This section discusses the human activity dataset's main features and categories and the architectures for the designed RNN and CNN. The proposed user authentication system is based on the human activity recognition function, where the user identity is identified based on human activities collected from each user. The following section discusses the MotionSense human activity dataset.

3.1 MotionSense Dataset

In this project, we employ the MotionSense dataset for the training phase. The MotionSense dataset includes many missing and incomplete data; therefore, we performed several processes to clean and recover the dataset. An efficient human activity dataset is adopted to train the model,

the MotionSense dataset [26]. The MotionSense dataset consists of time-series data produced by gyroscope and accelerometer sensors (gravity, user acceleration, attitudes, and rotation rate).

The MotionSense dataset was collected using an iPhone 6s smartphone that collects information from the Core Motion framework on iOS devices. The MotionSense dataset includes data of 24 participants who performed six different activities through 15 trials in the same environment and conditions: upstairs, downstairs, jogging, walking, sitting, and standing. The collected dataset files consist of two main sections:

- Short-trials: each activity lasted approximately 30 s to 1 min. The sit-down activity dataset is the largest, with 100,031 records, whereas the downstairs activity dataset is the smallest dataset, with a total number of 21,385 records. Therefore, it is crucial to study the effect of each activity on the user identification issue. Fig. 1 presents the distribution of the short- and long-activity datasets.
- Long-trails: each activity lasted approximately 2 to 3 min. The walk-activity dataset is the largest, with 266,752 records, whereas the Jog dataset is the smallest dataset, with 99,984 samples. Therefore, it is crucial to study the effect of each activity on the user identification issue.

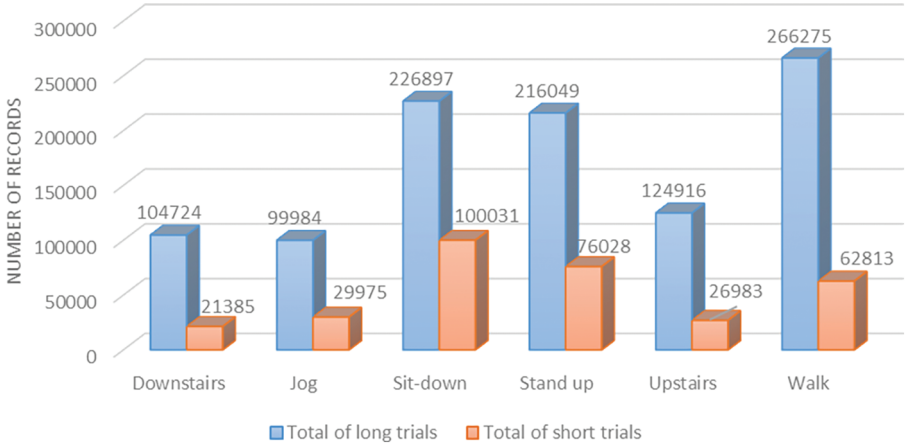

Figure 1: Distribution of records in long and short-trails datasets

The MotionSense dataset has been employed in several studies [27–30], which shows the importance of such a dataset. Therefore, the MotionSense dataset is employed in the training process by adopting several ML models. As presented above, each activity trail was stored in a single excel file. Therefore, we merged the activities into a single file to process the training and testing phases.

3.2 Preprocessing of MotionSense Dataset

The preprocessing function is essential for the employed MotionSense dataset. The MotionSense dataset consists of more than 100 unlabeled individual data files collected from 24 participants. Therefore, it was necessary to label the individual data files and merge them to produce a reliable dataset. The final merged dataset file consists of 1,039,322 records, which is considered a reliable data size for our experimental testbed.

MotionSense is a time-series dataset generated by the accelerometer and gyroscope sensors collected by iPhone 6s mobile phone. Therefore, to adapt the produced MotionSense dataset file with

our proposed architecture integrating the CNN and RNN models, an additional preprocessing stage must be accomplished, which is the injection of the timestamp feature to the MotionSense dataset. The timestamp feature injection process is considered a significant task to complete the training process. Fig. 2 shows the preprocessing functions conducted to produce a reliable dataset, which will be easily adaptable to our proposed model.

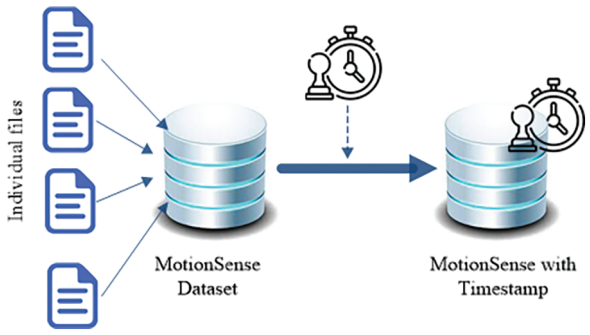

Figure 2: The main concept of preprocessing functions

3.3 Human Activity Authentication System

We designed a new human activity authentication system based on adopting CNN with RNN deep neural networks. Fig. 3 shows the main architecture of the proposed human activity authentication system.

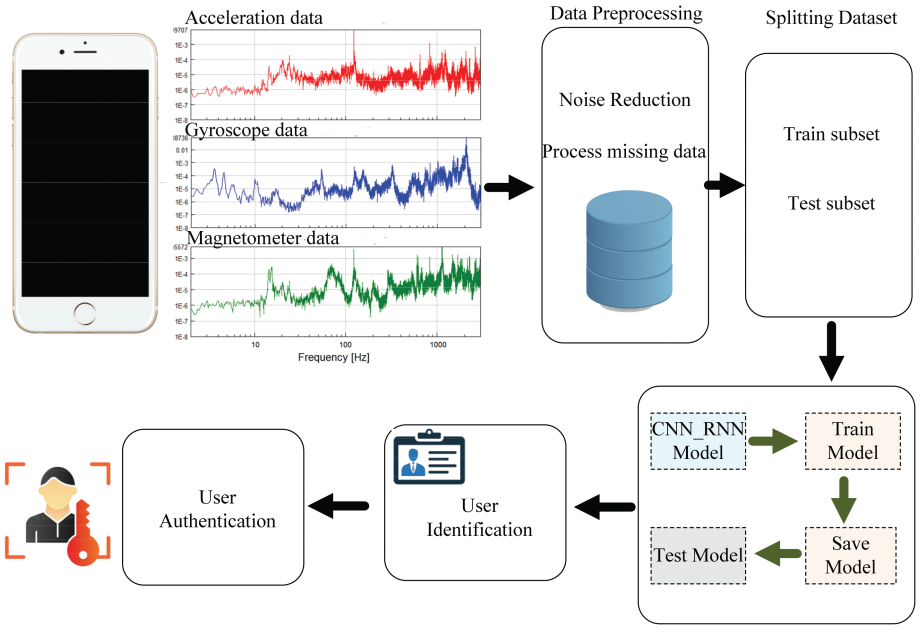

Figure 3: Proposed human activity authentication system

Human activity records are time-series data that reflect several human activities during a period of time. Although CNN has extreme computational efficiency, it is more suitable for spatial data, such as images. RNN, on the other hand, is more sensitive to sequential time-series data. Therefore, in this

study, we discuss the design of two deep neural networks: a CNN model and a novel CNN with an RNN model. CNN is a class of deep neural networks, where CNN is a multilayer perceptron, which means that the network is fully connected. In any layer, each neuron is connected to all neurons in the following layer. CNN uses a mathematical operation named convolution, which is a specialized type of linear operation.

3.4 CNN Architecture Overview

CNN models were mainly designed for image classification problems, where the CNN model studies an internal representation of 2D input in a feature learning process. However, the same procedure can be employed with 1D data sequences, as the model learns to extract features from sequences of observations. The main benefit of using CNN for sequence classification is that it can learn from the raw time-series data directly and hence does not require domain expertise to manually engineer the input features. The designed CNN model is presented in Fig. 4.

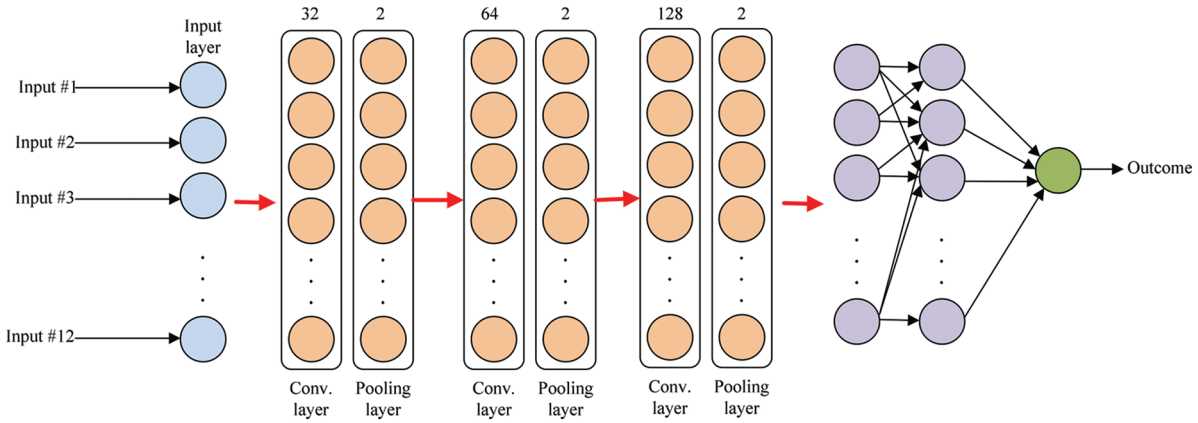

Figure 4: Structure of employed CNN model

3.5 Proposed Architecture Overview

We designed an efficient CNN with an RNN model presented in Fig. 5. RNN is a class of artificial neural networks where connections between nodes are either directed or not directed along a temporal variable-length sequence of inputs. RNN is usually adapted to work with time-series data that involves sequences, such as human activity data. The designed RNN model includes a convolution layer, which enhances classification accuracy by detecting significant features without human intervention.

CNN and RNN are considered the most popular categories of deep neural network architectures. Our model is efficient in terms of its reliability to the adopted human activity dataset, as in our case, the developed CNN and RNN models complement each other. The developed CNN model automatically detects the most significant features without any human supervision. In contrast, the developed RNN model remembers each piece of information throughout time, which is very useful in our approach. Therefore, integrating the above two models achieves better classification accuracy over the CNN and ML models.

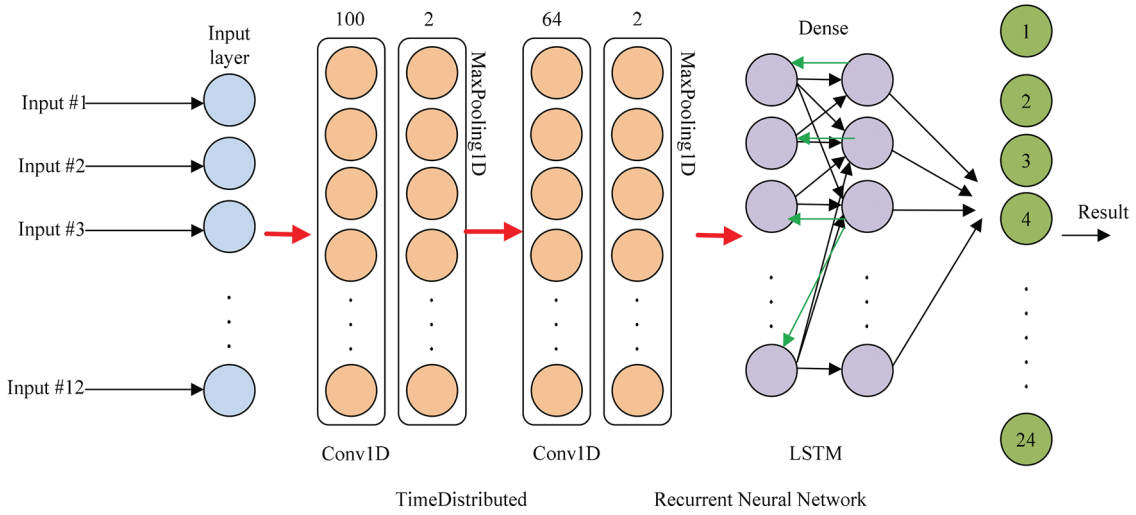

Figure 5: Structure of our developed model

As presented above, the proposed architecture consists of two main parts: a CNN and RNN. First, the human activity raw time data series was employed as an input into the CNN model to extract the sequence of features. Second, we used these features as inputs into the RNN model to perform the user identity classification task.

The CNN model consists of two consecutive 1D convolutional layers and a 1D max pooling function to down-sample the input representation by taking the maximum value over a spatial window of a pool size equal to two. After the feature extraction by the CNN layers with human activity raw data, the features were input to the designed RNN layer for classification purposes. The developed RNN model consists of a two-layer bidirectional long short-term memory (bi-LSTM), where each layer's dimension equals 60.

4 Experimental Results

This section presents and discusses the results of several experiments using the MotionSense dataset. We first discuss the results obtained from adopting five different ML models for each human activity. The human activities datasets were merged into six primary datasets (one dataset for each activity), and all datasets were merged into a single file.

4.1 Results of Employing ML Models with MotionSense Human Activity Dataset

To analyze and compare the results of our developed model, we first discuss the obtained results by employing five ML models with each human activity. Fig. 6 presents the results obtained for every human activity through five ML models. First, it was necessary to study the classification accuracy for each human activity for every user to assess its impact on identifying the user.

As mentioned above, walk and upstairs activities achieved the best testing accuracy (97%), whereas the LightGB and CatBoost models offer the best accuracy. Furthermore, the downstairs activity yields the worst accuracy.

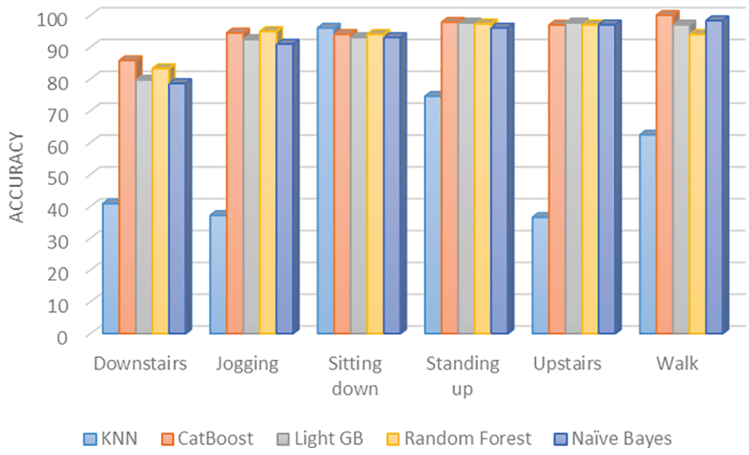

Figure 6: Results for 5 ML models on six activities

4.2 Results of Employing ML Models with Merged MotionSense Dataset

The human activity datasets obtained for 24 users were merged to produce a rich dataset file, improving the training process, and achieving better classification accuracy. The final dataset file comprises 1,039,322 records distributed among 24 users and six activities. The merged dataset has been divided into training and testing to validate the human activity classification system. Table 2 presents general statistics on the combined dataset file.

Table 2: General statistics on the merged dataset

Dataset type	Dataset size	Training records	Testing records
Merged dataset	1,039,322	727,525	311,797

For evaluation purposes, we implemented five different ML models with the merged dataset file to assess the efficiency of human activity classification systems. As indicated in Table 3, KNN and random forest classifiers offer the best training accuracy with 100.0%, whereas the latter achieves the best human identification accuracy with 92.44%. The obtained testing result for the employed random forest classifier is reasonable; however, there is a great demand for human authentication systems to obtain high classification accuracy to protect human identity. Fig. 7 shows the training and testing accuracy through adopting five machine learning models with the merged MotionSense dataset.

Table 3: ML model accuracy for the entire dataset

No.	Machine learning model	Training accuracy	Testing accuracy
1.	KNN	100.0%	90.51%
2.	CatBoost	88.02%	86.41%
3.	Light GB	81.61%	80.31%
4.	Random forest	100.0%	92.44%
5.	Naïve Bayes	51.24%	50.79%

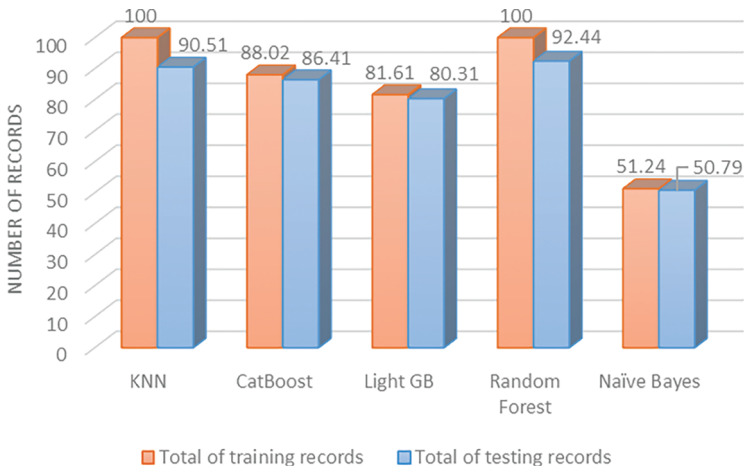

Figure 7: Training and testing accuracy for five ML models using the entire dataset

4.3 Results of Employing the CNN with MotionSense Dataset

Employing ML algorithms for user identification using the human activity dataset yields reasonable human identification accuracy. However, in some examples, the accuracy is low, indicating the low efficiency of the human activity authentication system. Therefore, considering novel approaches, like deep neural networks, is essential to enhance authentication accuracy and improve efficiency. For the developed CNN model, the training parameters are presented in Table 4, where the number of epochs was set to 180, and the batch size was set to 120.

Table 4: Training parameters for CNN model

# of epochs	Batch size
180	120

For evaluation purposes, we tested the proposed CNN model with three human activity datasets, as follows:

- Short-trials human activity dataset includes short durations of six different activities.
- Long-trials human activity dataset involves longer durations of six different activities.
- Merged short- and long-trials human activity dataset combines the short and long human activities dataset for six different activities.

This study evaluates the classification accuracy for these three datasets. Fig. 8 shows the training and testing accuracy for applying the presented CNN model with three datasets (short, long, and merged human activity datasets).

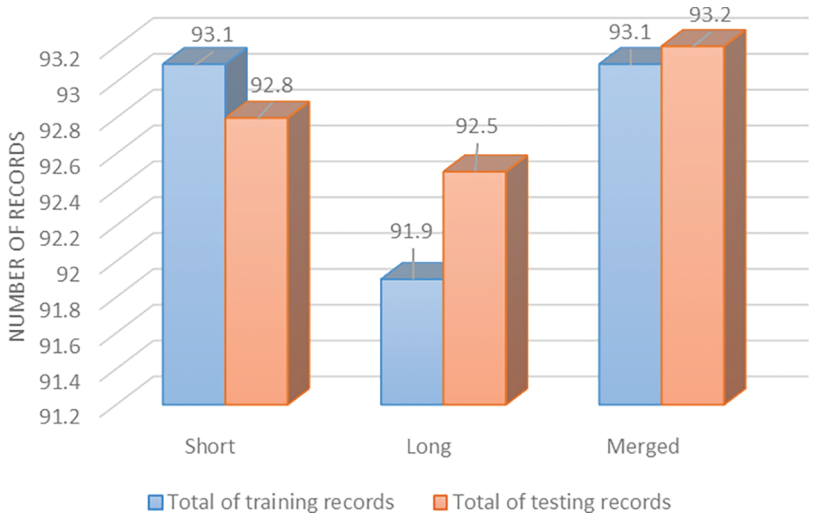

Figure 8: CNN training and testing accuracy for three human activity datasets

The merged human activity dataset offers the best training and testing classification accuracy. However, the accuracy needs further improvement to provide an efficient human activity authentication system.

4.4 Results of Employing Our Model Using MotionSense Dataset

Previous ML and CNN models offered reasonable classification accuracy for the human activity classification problem. However, human activity classification systems require high accuracy to protect the user's identity from eavesdroppers. Therefore, this section discusses the results obtained by employing our model to enhance human activity classification accuracy. Table 5 lists the training parameters for our model.

Table 5: The training parameters for our model

# of epochs	Batch size
150	120

After conducting the training and testing phases using our developed model, the overall classification accuracy achieved ~98.42%, whereas the data loss equaled 5.71%. Therefore, combining CNN with the RNN model offers the best classification accuracy. The precision, recall, and F1 scores were assessed for every user to examine the efficiency of our proposed architecture. Table 6 lists each user's precision, recall, and F1-score metrics.

Table 6: Precision, recall, and F1 score for each user

User identity	Precision	Recall	F1-score
1	98.00%	99.00%	99.00%
2	99.00%	99.00%	99.00%

(Continued)

Table 6: Continued

User identity	Precision	Recall	F1-score
3	99.00%	98.00%	99.00%
4	99.00%	99.00%	99.00%
5	98.00%	98.00%	98.00%
6	99.00%	99.00%	99.00%
7	99.00%	98.00%	99.00%
8	98.00%	99.00%	99.00%
9	99.00%	99.00%	99.00%
10	98.00%	98.00%	98.00%
11	99.00%	98.00%	98.00%
12	99.00%	98.00%	98.00%
13	97.00%	97.00%	97.00%
14	98.00%	99.00%	98.00%
15	98.00%	99.00%	98.00%
16	98.00%	98.00%	98.00%
17	100.0%	98.00%	99.00%
18	98.00%	96.00%	97.00%
19	98.00%	99.00%	99.00%
20	99.00%	98.00%	98.00%
21	98.00%	99.00%	98.00%
22	98.00%	98.00%	98.00%
23	99.00%	98.00%	99.00%
24	99.00%	99.00%	98.00%

Precision refers to the ratio of actually correct identifications. The precision accuracy for more than ten users was more than 98%. The overall precision ratio was high when our model was adopted. Fig. 9 shows the precision metric for 24 users.

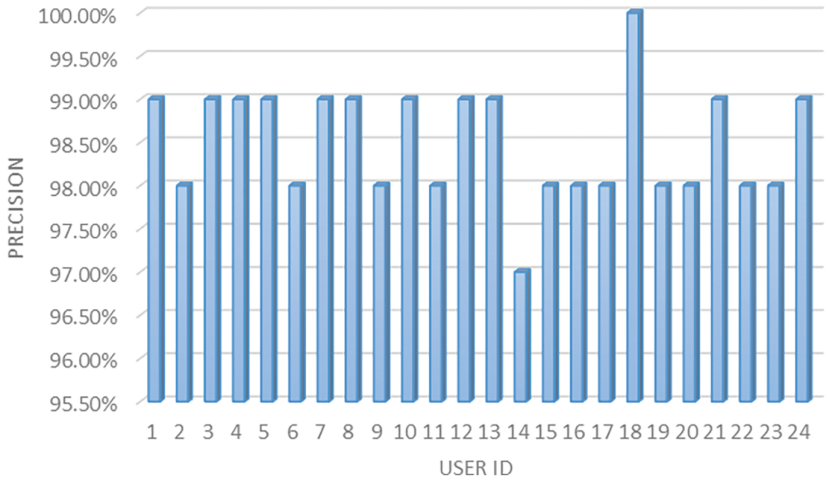

Figure 9: Precision accuracy for 24 users using our model

We assessed the recall metric for 24 users. Fig. 10 shows the results. Recall refers to the ratio of actual correct identifications. As presented, more than 16 users achieved high recall values. Finally, the F1-score metric was evaluated for 24 users. Fig. 11 illustrates the recall metric for 24 users. The F1-score conveys the balance between recall and precision for 24 users.

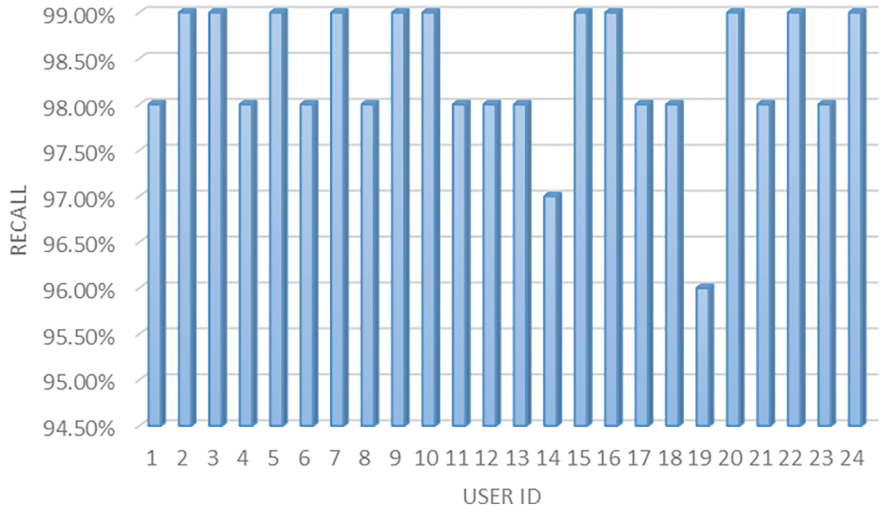

Figure 10: Recall results for 24 users using our model

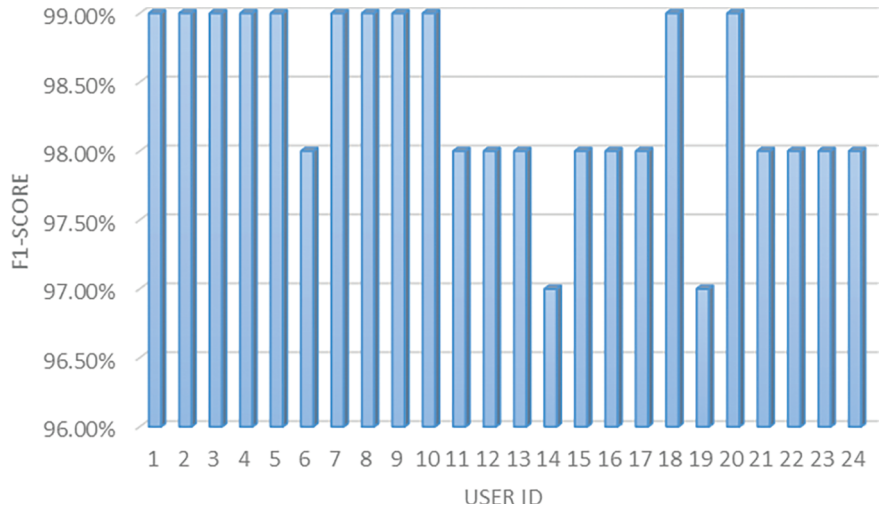

Figure 11: F1-score results for 24 users using our model

5 Discussion

We discuss the results of multiple experiments adopting several ML models, CNN, and our proposed model. Further, we compare the results obtained from previous studies with our proposed model. First, we measured the authentication accuracy for each human activity to evaluate the performance of user activity prediction based on a single human activity. According to the obtained results, the walk, standing up, and upstairs human activities offer the best classification accuracy,

whereas the Light GB and random forest models achieve high classification accuracy. Second, we measured the authentication performance using a developed CNN model. The CNN model was tested using the whole human activity dataset, where all individual human activity datasets were merged into a single file. According to the obtained results, CNN offers reasonable classification accuracy, like the ML models. However, human activity authentication systems require a high level of accuracy.

Finally, we developed an efficient CNN with RNN model to be employed with the human activity dataset. Our model offers the best classification accuracy using the human activity dataset. The developed CNN with RNN model achieves the best precision, recall, and F1 score for the 24 participants. Table 7 compares the developed machine learning models, CNN, and our proposed model. The KNN and random forest classifiers achieve the best training accuracy (100.0%), whereas they over less accuracy using the testing subset, with 95.51% and 92.44% accuracies for the KNN and RF classifiers, respectively. Our model achieves an efficient training accuracy of 99.89% and offers the best accuracy using the testing subset at 98.40%. This indicates that the developed classifier is more efficient and reliable than the ML and CNN models.

Table 7: Comparison among developed ML, CNN, and RNN models

Developed model	Training accuracy	Testing accuracy
KNN	100.0%	95.51%
CatBoost	88.02%	86.41%
LightGB	83.61%	80.30%
Random forest	100.0%	92.44%
Naïve Bayes	51.24%	50.75%
CNN	93.10%	93.20%
Our model	99.89%	98.40%

We compare the results achieved in other recent studies with our model. Table 8 shows a comparison among the recently developed human activity-based authentication systems. Our developed model is superior to most existing human activity authentication systems in terms of reliability and efficiency.

Table 8: Comparison among the recent developed human-activity-based authentication systems

Research work	Employed algorithm	Dataset	Accuracy
[7]	Siamese CNN	[8]	97.8
[9]	Hidden markov model	Online data	FAR: 3.98% FRR: 5.03
[10]	AUToSen deep learning	Their own dataset with 84 participants	98%
[11]	Bayes net classifier	[12,13]	95%
[14]	KNN, Autoencoder neural network, and support vector machine	[15]	98.3%

(Continued)

Table 8: Continued

Research work	Employed algorithm	Dataset	Accuracy
[16]	Decision tree, support vector machine, and random forest	[17–19]	97.3%
[20]	DeepConvLSTM	[21,22]	98%
Our model	CNN-RNN model	MotionSense	98.4%

6 Conclusion and Future Studies

User authentication is necessary for diverse applications because it is imperative to establish the user's identity. Continuous and passive authentication methods address several limitations in traditional user authentication systems. This paper developed a new passive and continuous authentication technique that takes advantage of features generated from IoT devices' sensors. This approach utilized users' behavioral traits and employed an activity recognition technique powered by a hybrid BiLSTM and CNN model. We validated the performance of our proposed method using a public dataset that consists of 24 users performing six different activities (i.e., sitting, walking, jogging, walking upstairs, walking downstairs, and standing). Our model achieves high identification accuracy above 98.4%. We compared our method with traditional machine learning algorithms and state-of-the-art solutions and found that our method achieved superior performance in terms of accuracy. Moreover, the results obtained from the proposed system were compared to the recently developed systems and achieved better classification performance in terms of accuracy. One limitation of the proposed approach is the lack of covering all possible activities. Also, the proposed approach does not investigate the sudden change in the user's behavior. In future research, we aim to integrate more sensors and evaluate every possible activity to recognize users in a comprehensive manner. Furthermore, we aim to develop an unsupervised learning phase to deal with the sudden change in the user's behavior.

Funding Statement: This work was partly supported by the Sensor Networks and Cellular Systems (SNCS) Research Center, University of Tabuk, Saudi Arabia, under Grant 1443-001.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Hameed, F. I. Khan and B. Hameed, "Understanding security requirements and challenges in internet of things (IoT): A review," *Journal of Computer Networks and Communications*, vol. 2019, pp. 1–14, 2019.
[2] S. Pal, M. Hitchens, T. Rabehaja and S. Mukhopadhyay, "Security requirements for the internet of things: A systematic approach," *Sensors (Basel)*, vol. 20, no. 20, pp. 5897, 2020.
[3] S. Jin, B. Sun, Y. Zhou, H. Han, Q. Li *et al.,* "Video sensor security system in IoT based on edge computing," in *2020 Int. Conf. on Wireless Communications and Signal Processing (WCSP)*, Nanjing, China, 2020.
[4] L. Xiaofeng, Z. Shengfei and Y. Shengwei, "Continuous authentication by free-text keystroke based on CNN plus RNN," *Procedia Computer Science*, vol. 147, pp. 314–318, 2019.
[5] W. Li, W. Meng and S. Furnell, "Exploring touch-based behavioral authentication on smartphone email applications in IoT-enabled smart cities," *Pattern Recognition Letters*, vol. 144, pp. 35–41, 2021.
[6] I. Papavasileiou, Z. Qiao, C. Zhang, W. Zhang, J. Bi *et al.,* "GaitCode: Gait-based continuous authentication using multimodal learning and wearable sensors," *Smart Health*, vol. 19, pp. 100162, 2021.

[7] M. P. Centeno, Y. Guan and A. van Moorsel, "Mobile based continuous authentication using deep features," in *Proc. the 2nd Int. Workshop on Embedded and Mobile Deep Learning*, Munich, Germany, pp. 19–24, 2018.
[8] Q. Yang, G. Peng, D. T. Nguyen, X. Qi, G. Zhou *et al.,* "A multimodal data set for evaluating continuous authentication performance in smartphones," in *Proc. the 12th ACM Conf. on Embedded Network Sensor Systems*, New York, United States, pp. 358–359, 2014.
[9] C. Shen, Y. Li, Y. Chen, X. Guan, R. A. *et al.,* "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.
[10] M. Abuhamad, T. Abuhmed, D. Mohaisen and D. Nyang, "AUToSen: Deep-learning-based implicit continuous authentication using smartphone sensors," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5008–5020. 2020.
[11] M. Ehatisham-ul-Haq, M. A. Azam, J. Loo, K. Shuang, S. Islam *et al.,* "Authentication of smartphone users based on activity recognition and mobile sensing," *Sensors*, vol. 17, no. 9, pp. 2043, 2017.
[12] M. Shoaib, H. Scholten and P. J. M. Havinga, "Towards physical activity recognition using smartphone sensors," in *Proc. the 2013 IEEE 10th Int. Conf. on Ubiquitous Intelligence & Computing and 2013 IEEE 10th Int. Conf. on Autonomic & Trusted*, Vietri sul Mere, Italy, pp. 80–87, 18–21 December 2013.
[13] M. Shoaib, S. Bosch, O. Durmaz Incel, H. Scholten and P. J. M. Havinga, "Fusion of smartphone motion sensors for physical activity recognition," *Sensors*, vol. 14, no. 6, pp. 10146–10176. 2014.
[14] G. Wu, J. Wang, Y. Zhang and S. Jiang, "A continuous identity authentication scheme based on physiological and behavioral characteristics," *Sensors*, vol. 18, no. 1, pp. 179, 2018.
[15] W. G. Nan, W. Jian, Z. Y. Rong and J. Shuai, "J, sensor data for identity recognition," 2022. [Online]. Available: http://pan.baidu.com/s/1dE9Shwd.
[16] M. N. Malik, M. A. Azam, M. Ehatisham-Ul-Haq, W. Ejaz and A. Khalid, "ADLAuth: Passive authentication based on activity of daily living using heterogeneous sensing in smart cities," *Sensors*, vol. 19, no. 11, pp. 2466, 2019.
[17] D. Anguita, A. Ghio, L. Oneto, X. Parra and J. L. Reyes-Ortiz, "A public domain dataset for human activity recognition using smartphones," in *Proc. the European Symp. on Artificial Neural Networks (ESANN)*, Bruges, Belgium, pp. 24–26, April 2013.
[18] A. Reiss and D. Stricker, "Introducing a new benchmarked dataset for activity monitoring," in *Proc. the 2012 16th Int. Symp. on Wearable Computers (ISWC)*, Heidelberg, Germany, pp. 108–109, 12–16, September 2012.
[19] C. Chatzaki, M. Pediaditis, G. Vavoulas and M. Tsiknakis, "Human daily activity and fall recognition using a smartphone's acceleration sensor," in *Proc. the Int. Conf. on Information and Communication Technologies for Ageing Well and e-Health*, Rome, Italy, pp. 100–118 21–22, April 2016.
[20] S. Mekruksavanich and A. Jitpattanakul, "Deep learning approaches for continuous authentication based on activity patterns using mobile sensing," *Sensors*, vol. 21, no. 22, pp. 7519, 2021.
[21] G. M. Weiss, K. Yoneda and T. Hayajneh, "Smartphone and smartwatch-based biometrics using activities of daily living," *IEEE Access*, vol. 7, pp. 133190–133202, 2019.
[22] Q. Yang, G. Peng, D. T. Nguyen, X. Qi, G. Zhou *et al.,* "A multimodal data set for evaluating continuous authentication performance in smartphones," in *Proc. the 12th ACM Conf. on Embedded Network Sensor Systems*, Memphis, TN, USA, 3–6 November 2014; SenSys'14; Association for Computing Machinery: New York, NY, USA, pp. 358–359, 2014.
[23] H. C. Volaka, G. Alptekin, O. E. Basar, M. Isbilen and O. D. Incel, "Towards continuous authentication on mobile phones using deep learning models," *Procedia Computer Science*, vol. 155, pp. 177–184, 2019.
[24] M. P. Centeno, A. V. Moorsel and S. Castruccio, "Smartphone continuous authentication using deep learning autoencoders," in *2017 15th Annual Conf. on Privacy, Security and Trust (PST)*, Calgary, Canada, pp. 147–1478, August 2017.

[25] A. Verma, V. Moghaddam and A. Anwar, "Data-driven behavioural biometrics for continuous and adaptive user verification using smartphone and smartwatch," *Sustainability*, vol. 14, no. 12, pp. 7362, 2022.
[26] M. Malekzadeh, R. G. Clegg, A. Cavallaro and H. Haddadi, "Mobile sensor data anonymization," in *Proc. the Int. Conf. on Internet of Things Design and Implementation*, Montreal Quebec, Canada, pp. 49–58, April 2019.
[27] N. Agrawal, A. Shahin Shamsabadi, M. J. Kusner and A. Gascón, "QUOTIENT: Two-party secure neural network training and prediction," in *Proc. the 2019 ACM SIGSAC Conf. on Computer and Communications Security*, London, United Kingdom, pp. 1231–1247, November 2019.
[28] M. Batool, A. Jalal and K. Kim, "Sensors technologies for human activity analysis based on SVM optimized by PSO algorithm," in *2019 IEEE Int. Conf. on Applied and Engineering Mathematics (ICAEM)*, Taxila, Pakistan, pp. 145–150, August 2019.
[29] I. Klein, "Smartphone location recognition: A deep learning-based approach," *Sensors*, vol. 20, no. 1, pp. 214, 2019.
[30] B. Bordel, R. Alcarria, T. Robles and M. S. Iglesias, "Data authentication and anonymization in IoT scenarios and future 5G networks using chaotic digital watermarking," *IEEE Access*, vol. 9, pp. 22378–22398, 2021.