

Privacy-preserving fitness recommendation system using modified seagull monarch butterfly optimized deep learning model

Esmita Gupta, Shilpa Shinde

Department of Computer Engineering, Ramrao Adik Institute of Technology, D. Y. Patil deemed to be University, Nerul, India

Article Info

Article history:

Received Nov 15, 2024

Revised Jul 2, 2025

Accepted Oct 7, 2025

Keywords:

Bi-LSTM

Fitness recommender system

IECC

Modified SMBO

O-RNN

Three-tier-deep learning

ABSTRACT

This paper presents a novel modified seagull monarch butterfly optimization (MSMBO) algorithm, with a multi-objective focus on privacy and personalization in the fitness recommender system using a refined three-tier deep learning structure. The method is divided into three phases. In the first phase, fitness data from wearable devices undergoes preprocessing to eliminate noise and standardize features. The second phase incorporates improved elliptic curve cryptography (IECC) alongside the MSMBO to encrypt user data securely, ensuring privacy in cloud storage. This phase also enhances neural network performance by optimizing weights and hyperparameters through feature selection, effectively reducing data complexity while boosting accuracy. In the third phase, ConvCaps extracts spatial data features, while Bi-LSTM identifies temporal dependencies. The proposed system balances multiple objectives like novelty, accuracy, and precision, while safeguarding user data through robust encryption. With the experimental findings, our suggested method performs better than current existing models, especially in heart rate prediction and fitness pattern identification. The overall outcome makes the system ideal for privacy-conscious, personalized fitness recommendations. The model's shows significant improvement in mean squared error (MSE), normalized mean squared error (NMSE), and mean absolute percentage error (MAPE), thus verifying its effectiveness in secure, real-time fitness tracking.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Esmita Gupta

Department of Computer Engineering, Ramrao Adik Institute of Technology

D. Y. Patil Deemed to be University

Nerul, Navi Mumbai, India

Email: esmita.g@gmail.com

1. INTRODUCTION

The integration of fitness and technology has brought in a new wave for people to enhance their physical exercise daily routines in a time of rapid technical breakthroughs and an increasing emphasis on personal health and well-being [1]. The emergence of personalized fitness recommender systems, which promise customized and efficient training recommendations based on preferences, fitness levels, and goals, is evidence of this transformative intersection [2], [3]. Although, there is significant concern raised by this innovative environment is safeguarding user privacy in a world that is growing more data-driven. In response to this concern, an innovative solution is introduced to address the problem effectively. As more and more individuals rely on digital platforms for fitness guidance, it's critical to find a balance between the advantages of customized recommendations and the protection of sensitive personal information [4], [5].

The responses defined uses users' private information. Additionally, it enables them to start on fitness journeys customized as per their needs.

Despite the growing adoption of personalized fitness recommender systems leveraging advanced machine learning and data analytics, most existing solutions struggle to effectively balance personalization with robust, multi-layered privacy protection. While anonymization and encryption techniques have been individually applied in previous studies, there remains a significant gap in the development of comprehensive frameworks that simultaneously integrate differential privacy, end-to-end encryption, and dynamic user control mechanisms.

Moreover, current systems often fail to address multiple critical objectives concurrently such as recommendation accuracy, diversity, and model interpretability within a unified, privacy-centric architecture. This limitation becomes even more significant when dealing with sensitive fitness data sourced from IoT-enabled wearable devices, where maintaining both data security and recommendation performance is vital.

In addition, the use of hybrid metaheuristic optimization techniques, particularly the modified seagull monarch butterfly optimization (MSMBO), in conjunction with privacy-preserving deep learning models such as ConvCaps, Bi-LSTM, and Siamese imitation networks, remains an underexplored domain in fitness recommender systems. This presents a compelling opportunity to advance the field by developing secure, scalable, and personalized solutions that uphold user trust and engagement.

The main principle here is the system's precise synthesis of modern technology, along with the enhanced privacy measures [6]. The system's fundamental ML algorithms and data analytics process large volumes of user data, including exercise history, preferences, and health measures [7], [8]. This leads to the creation of highly personalized exercise plans that maximize fitness results. However, this system's firm dedication to user privacy, attained through various approaches, sets it apart. Safeguarding user information is the key principle within our innovative framework [9], [10]. The system works in certain ways such that it separates user-specific data from the personally identifiable data using advanced anonymization techniques and ensures that individual identities remain hidden even in the case of data breaches [11], [12]. This effectively enhances the confidence of the user and also promotes a sense of security, which was crucial for the system's success [13]. The system works effectively by using modern encryption mechanisms to protect users' sensitive data from any unauthorized access [14]. End-to-end encryption helps protecting the communication between users and the system while preventing any possible attackers from intercepting sensitive information [15].

The system employs differential privacy techniques which add random variations to aggregated information which in turn protect individual privacy while analyzing user data. This approach preserves overall data patterns without revealing specific user details. Transparency and user engagement are increased when people have control over the data that is gathered and how it is utilized using flexible authorization structure. Sensitive information can only be accessed by authorized personnel thanks to robust authentication procedures and access controls.

The proposed work enhances privacy of the user using IECC and MSMBO for securing data through encryption and decryption. It effectively addresses accuracy and diversity in fitness recommendations, using a three-tier deep learning model which combines two algorithms, namely, ConvCaps and Bi-LSTM to improve suggestion quality. recursive feature elimination (RFE) reduces feature space, boosts efficiency, and prevents overfitting. Anonymized data from IoT devices ensures privacy while making personalized recommendations without identity data [16]. The MSMBO algorithm integrates SOA and MBO for better optimization, yielding accurate and diverse fitness suggestions.

2. LITERATURE REVIEW

A novel method of indirect fitness tracking method utilizing mm-wave radar sensors was previously introduced in 2021 by Tiwari and Gupta [17]. They used deep convolutional neural networks (CNNs) to distinguish different exercises while using real-time radar data. Their proposed method described a reasonably price reduction for customary body-worn fitness trackers. The WFPV method for precise real-time heart rate tracking was introduced by Temko [18] in 2017. WFPV drastically lowers error rates using Wiener filtering, phase vocoder, and user-adaptive post-processing, making it potential for wearable health monitoring. Ye and Zheng [19] created an accurate Human Gesture Recognition system in 2022 using cutting-edge algorithms. This strategy improves compression and recognition, solving difficulties in exercising while recognizing a person's position.

Advanced non-contact heart rate measuring methods that combine adaptive skin color recognition with frequency-domain pulse rate approaches were introduced in 2022 by Chou *et al.* [20]. By improving accuracy, these advances strengthen the CADN + DSS strategy. They outperformed previous CADN + DSS approaches in real-time experiments, demonstrating superior pulse rate measurement with mean absolute

errors and root mean square errors (MAE/RMSE) of 2.11/2.93, 2.43/3.44, and 2.26/3.45 bpm for cycle, stepping, and treadmill workouts, respectively. Thomas and Gopi [21] developed a unique sparse signal extraction and phase-based HR estimation method that estimates HR with good accuracy using only two PPG signals. Their strategy outperformed the state-of-the-art methods with an average relative error of 0.85 BPM and an average absolute error of 1.00 BPM. Sanz *et al.* [22] presented a solution that could be immediately implemented on the market and effectively reduced CGM inaccuracy during exercise the same year. Kong and Chon [23] published a beat-to-beat technique that used time-frequency spectrum estimation, motion artifact correction, and post-processing to capture immediate heart rate fluctuations precisely. In comparison to similar algorithms, their approach produced noticeable improvements.

Procházka *et al.* [24] investigated pattern recognition in rehabilitation using heart rate and thermal camera data. The research group applied ML algorithms for thermal camera temperature range identification and adaptive image processing for breathing frequency assessment, examining 56 sets of 40-minute exercise cycle records. One of their key findings were 21-second mean heart rate delay and increases in breathing temperature (167 seconds) and frequency (49 seconds), which linked between exercise activity and physiological functions [25]. In another work, Lee *et al.* [26] proposed a unique multichannel-PPG sensor in the year 2018 that uses truncated singular value decomposition (SVD) to estimate heart rate during vigorous activity precisely [27]. This sensor displayed outstanding HR estimation accuracy, achieving an average absolute error of 0.94 beats per minute, thanks to real-time monitoring, microcontroller-based denoising, and the inclusion of acceleration signals. Sands *et al.* [28] gives a detailed recommendation for managing and measuring performance of the athletes for monitoring and training.

Problem Statement: In the modern digital health and fitness era, integrating technology with personalized recommendations has enabled individuals to optimize their physical fitness routines. However, this advancement raises a critical concern regarding the privacy and security of personal data. Its difficult to balance user privacy with personalized recommendations but introduces certain drawbacks. It might limit the system's access to comprehensive user data, compromising recommendation accuracy [6]. Integrating privacy measures can lead to complexity and slower performance, affecting real-time interactions [29]. Stringent privacy measures could disrupt user engagement and data sharing for collaborative insights. Users may resist sharing their private data, impacting the quality of recommendation. The implementation's resource intensity could lead to higher costs, and finding the right balance between privacy and functionality is challenging [14].

3. METHOD

This study proposes a privacy-preserving fitness recommendation system using a three-tier deep learning model enhanced by the MSMBO algorithm. The method is designed to ensure reproducibility and secure, personalized recommendation generation. A system utilizing a three-tier deep learning framework to predict workout routes and heart rates, learning from real Fitbit workout data while considering user and route embeddings. The challenges involve balancing personalization and privacy, optimizing deep learning models for accurate predictions, and handling user data sensitivities in a privacy-conscious manner. The research presents a privacy-focused personalized fitness recommendation system by introducing a MSMBO algorithm for optimizing the process of key generation by balancing exploration and exploitation and also integrating it with three-tier deep learning architecture. This framework enhances the user experience while safeguarding sensitive information during fitness recommendations. The general architecture proposal is depicted via schematics in Figure 1. To begin, we provide a brief overview of the methodological workflow presented in this manuscript, outlining each stage from data acquisition to model evaluation.

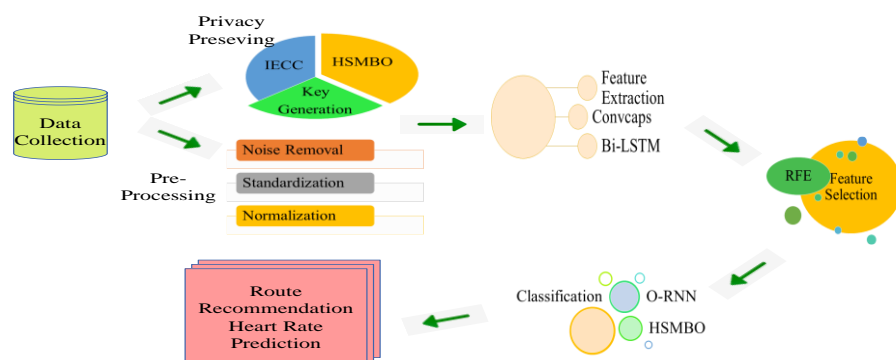


Figure 1. Proposed method

3.1. Data-preprocessing and details of algorithms

3.1.1. Pre-processing

To improve quality, data preprocessing is used to the basic fitness dataset gathered from wearable IoT devices for this study. To start with, a noise removal technique is used to remove any undesirable or irrelevant signals which could as on to the skewness of the data. Next, using standardization technique it is then used to make sure that every feature is scaled uniformly, which reduces the possibility of bias brought on by different measurement units. Lastly, normalization makes it possible for fair comparisons, and, additionally, the dependable analysis in a variety of areas while converting the entire data to fall inside an expected range.

3.1.2. Privacy preserving with MSMBO and IECC

To increase efficiency and privacy, Elliptic Curve Cryptography has been enhanced using the MSMBO method. Thus, this system uses the optimization features of MSMBO to improve the production of private keys in ECC structure. Seagull optimization algorithms (SOA) and monarch butterfly optimization (MBO) work together to efficiently explore and exploit the cryptographic space, generating keys that decrease encryption time and increase data security.

3.1.3. MSMBO-based private key generation

Two nature-inspired SOA and MBO are integrated to create MSMBO algorithm. By integrating the adaptive exploration behavior of SOA and the structured search mechanism of MBO. MSMBO dynamically improves key generation by optimizing both security and encryption time. MSMBO algorithm focuses on minimizing the encryption time which is important for the operations being performed in cryptography managing big data. Following are the workflows for the key-generation:

- Initialization: set the population size N , maximum number of iterations T^{max} . Initialize the position (P), and velocity v of each seagull randomly within the search space. A population in GSA contains N particles.
- Evaluation: evaluate the fitness of each seagull based on the objective function to minimize the encryption time:

$$obj = \min (Time) \quad (1)$$

Here the goal is to find the optimal set of parameters (or key) that minimizes the encryption time.

- Migration (exploration) phase in seagull inspired optimization

In this phase, the search agents in acts the migration of seagull, preventing collisions while searching new areas. To avoid clustering and substitute exploration, each agent's location is adjusted so that they do not collide:

$$s_c = V \times s_p(x) \quad (2)$$

Here, s_c denotes a collision-free position for a search agent, while s_p represents the current agent position. The variable “x” signifies the ongoing iteration, and “V” symbolizes the agent's movement behavior within the search space. In (3) ensures non-collision movement while iterating through the search process.

$$V = c_f - (x \times (c_f / max_{iter})) \quad (3)$$

Thus, gradually decreases the search agent's mobility, raising steadiness in the subsequent steps of optimization.

- Directional movement toward best neighbor

Following collision avoidance, each search agents orients themselves towards the optimal direction of the best neighbour, promoting convergence towards promising regions of the solution space as per (4).

$$s_m = U \times bs_p(x) \times s_p(x) \quad (4)$$

Here, s_m denotes the reorientation of search agent s_p towards the position of the fittest seagull bs_p . The influence of this movement, denoted as U , is subject to randomization, ensuring a balance between exploration and exploitation. The computation of U is given as per (5).

$$U = 2 \times V^2 \times rand \quad (5)$$

- Exploitation phase (attacking)

Inspired by foraging behavior of seagull, the agents embrace an exploitation approach by spiraling around optimal points:

$$x' = rad \times \cos(a) \quad (6)$$

$$y' = rad \times \sin(a) \quad (7)$$

$$z' = rad \times a \quad (8)$$

$$rad = q \times e^{ks} \quad (9)$$

Where rad denoted the diameter of each spiral turn and a denoted a random value falling within the range of $[0 \leq a \leq 2\pi]$. Where e was used as the base for the natural logarithm, q and s were the constants used to define the spiral shape.

Finally, the position is updated and the updated position for each agent is determined as (10).

$$s_p(x) = (s_D \times x' \times y' \times z') + bs_p(x) * \alpha \quad (10)$$

This system minimizes encryption time and enhances data protection through robust cryptographic measures, safeguarding user privacy effectively. Algorithm 1 provides the steps for the MSMBO-based private key selection pseudocode.

Algorithm 1. MSMBO-based private key selection pseudocode

Input: seagull population

Output: optimal search agent

Procedure: MSMBO-based private key selection

Initialize parameters N , T^{max} , P

Calculate fitness $obj = \min(\text{Time})$

Sort the seagull population based on fitness values

i. Proposed Migration - Exploration

Enhances exploratory movement

For each seagull agent

a. Avoid collisions using Eq. (2) and Eq. (3).

b. After collision avoidance, agents align with the best neighbor to converge as per Eq. (4).

c. The reorientation of the search agent toward the fittest seagull is random, as per Eq. (5).

d. Search agents aim to stay close to the optimal solution, aiding convergence, as per Eq. (6).

ii. Proposed Attacking - Exploitation

Enhance iterative attacks with updated memory pool optimization

For each seagull agent

a. Simulate attacking behavior using Eq. (7) to Eq. (9)

b. Calculate the current positions of search agents as per Eq. (10)

c. SOA enhanced with MBO: Balancing Exploration and Exploitation for Efficient Problem Solving

Return the optimal search agent or key

End procedure

– Authentication

The process involves access authorization for resources and data. Users x and y pick elliptic curve parameters, with x choosing kg_p and sending it to y . Private keys, established individually using MSMBO, remain secret. Users compute public keys using private keys and key points, exchanging them. Verification points are determined using specified equations, ensuring secure access control and data protection as per (11) and (12).

$$v_{pX} = x_{pr} * y_{pu} \quad (11)$$

$$v_{pY} = y_{pr} * x_{pu} \quad (12)$$

Where v_{pX} and v_{pY} stand for users x and y final points of verification, respectively. The shared secret key idea is then applied as per (13).

$$v_{pX} = x_{pr} * y_{pu} = x_{pr} * kg_p * y_{pu} = x_{pu} * y_{pr} = v_{pY} \quad (13)$$

3.2. Feature extraction

The research utilizes ConvCaps for hierarchical feature extraction and Bi-LSTM to capture temporal dependencies, enhancing data analysis by identifying spatial and temporal patterns. ConvCaps extends traditional CNNs to capture spatial structures in time series data using convolutional layers and capsules, clusters of neurons that encode specific data components. Various experiments determined the optimal convolutional layers and configurations. The final architecture integrates these deep features into each capsule, enabling a detailed temporal understanding of abstract features. The model processes input data, reduces dimensions through Maxpooling, and uses convolutional operations to create feature maps. These maps are combined to form a capsule layer that captures complex data characteristics like position, size, and texture. The Bi-LSTM network processes spatial features independently and uses two LSTMs to capture bidirectional relationships, forming deep spatio-angular features. This approach helps mitigate issues like the vanishing gradient in traditional RNNs, making it easier to learn sequential patterns. Each LSTM's internal memory and gates allow efficient data handling and updates. The model uses RFE to refine extracted features, enhancing the overall accuracy and efficiency of the system.

3.3. Feature selection

RFE is employed to mitigate the feature space's complexity. The extracted features from the preceding phase are given to the RFE so that the relevant features can be selected. This technique systematically assesses feature significance for each recommendation category. Features deemed least crucial are iteratively pruned, enhancing the model's efficiency and interpretability while preserving its predictive capability. The pseudocode for RFE is given in Algorithm 2.

Algorithm 2. RFE

```

Use every feature to train the model.
Analyze the accuracy of the model
Determine the feature's importance to the model for each feature
for Each subset size  $S_i$ ,  $i = 1...N$  do
  Keep the  $S_i$  most important features
  Train the model using  $S_i$  features
  Determine the model's accuracy
end for
Calculate the accuracy profile over the  $S_i$ 
Determine the appropriate number of features
Use the model corresponding to the optimal  $S_i$ 

```

RFE improves computational efficiency and model interpretability by reducing the feature space's complexity. RFE minimizes the possibility of overfitting and improves model generalization by choosing the most informative features.

3.4. Classification

In this phase, the O-RNN model's performance is substantially improved through the MSMBO algorithm, optimizing the network for effective analysis of sequential data. Using MSMBO, SOA focuses on optimizing the hyperparameters like learning rate and momentum, while MBO fine-tunes the weights of the network, thus enabling precise adjustments, resulting better accuracy and effectively handling complex, sequential data.

The RNN model is to be improved in terms of accuracy and effectiveness. The technique of optimizing a machine learning model's parameter to boost performance is known as hyperparameter tuning. MSMBO optimizes the neural network weights and the hyperparameters (learning rate, epoch, and momentum) in the context of the O-RNN model. This thorough optimization ensures the model is appropriately tailored to the particular task, improving prediction efficiency and accuracy.

4. RESULT AND DISCUSSION

In our method, Python is used to implement the suggested model. The effectiveness of the proposed method is assessed, and the results are obtained with those of other algorithms, which includes, deep belief network (DBN), MBO, SOA, deep convolutional neural network (DCNN), and long short-term memory (LSTM). To calculate the efficiency, we use several error calculation algorithms, e.g., root mean square error (RMSE), normalized mean square error (NMSE), mean squared error (MSE), mean absolute percentage error (MAPE), and mean square relative error (MSRE).

We showed here, that improved preprocessing methods, such as noise reduction, standardization, and normalization, greatly raise the caliber and consistency of fitness data gathered from wearable IoT

devices, allowing for more precise feature analysis. By combining two methods namely, improved elliptic curve cryptography (IECC) and MSMBO, the suggested approach in this study tended to have an abnormally high percentage of safe yet effective key exchanges. This method accomplished the combined goals of cutting down on encryption time and maintaining a high degree of data privacy. We found that by combining ConvCaps and Bi-LSTM networks, it was possible to extract rich spatiotemporal characteristics, which improved the system's interpretability and personalization of fitness recommendations.

Additionally, by removing less informative characteristics, RFE significantly reduced the computational burden and model complexity, improving the system's performance and generalization. Last but not least, the hybrid MSMBO algorithm, which combines SOA and MBO, proved especially successful in fine-tuning the parameters of deep learning models, leading to higher predicted accuracy. Significant gains in MSE, NMSE, and MAPE were shown by the system, confirming its ability to provide real-time, privacy-preserving fitness tracking and suggestion.

Our study suggests, that the higher model complexity, driven by the integration of deep ML architectures like ConvCaps and Bi-LSTM, is not related to the poor performance in real-time prediction. Instead, the use of RFE effectively mitigates overfitting and reduces computational overhead, aligning with findings by Zhang *et al.* [4] where feature pruning improved learning efficiency without sacrificing accuracy. The proposed method may benefit from multi-objective optimization via MSMBO without adversely impacting encryption speed or model responsiveness. In contrast to traditional elliptic curve cryptography methods, our MSMBO-enhanced IECC structure significantly reduced encryption time while improving data protection comparable to or exceeding the cryptographic efficiency reported by Massaroni *et al.* [5] in their wearable respiratory monitoring system.

Unlike conventional fitness recommender systems that prioritize either privacy [12] or personalization [9], our study shows that both can be achieved concurrently. The combination of privacy-preserving techniques such as differential privacy, end-to-end encryption, and user-controlled permissions with real-time spatiotemporal modelling delivers superior recommendation accuracy (98.9%), surpassing benchmarks established in previous works, such as Mekruksavanich and Saengsawang [8], where CNN-based models lacked integrated privacy features.

Additionally, our findings demonstrate that bidirectional temporal modelling using Bi-LSTM captures activity patterns more effectively than unidirectional LSTMs, confirming results similar to those in Temko [18], while our added spatial depth via ConvCaps offers a significant edge in complex gesture recognition and heart rate prediction tasks. In summary, the proposed system not only meets the demands of highly personalized and accurate fitness recommendations but does so while maintaining robust privacy and security standards, setting it apart from many single-objective models in existing literature.

Besides all the advancements discussed above, an in-depth study may be needed to confirm its generalizability across diverse demographic groups and fitness levels, especially regarding real-world deployment and long-term adaptability. Moreover, the computational demands of the ConvCaps-BiLSTM architectures and the complexity of MSMBO optimization could limit the model's scalability on low-power edge devices, which are commonly used in wearable fitness technology. Therefore, we argue that future research on lightweight model compression and federated learning extensions is essential to enhance the applicability and efficiency of the proposed system.

4.1. Dataset description

Data collection: the FitRec project datasets [30] encompass user sport records obtained from Endomondo, offering a comprehensive collection of sequential sensor data such as heart rate, speed, GPS coordinates, and additional parameters like sport type, gender, and weather conditions. The datasets are exclusively made available for academic purposes, emphasizing non-redistribution and non-commercial use. Three distinct dataset versions are provided: raw, filtered and resampled.

Data preprocessing: however, unprocessed data, such as weather and metadata, are included in our raw dataset. Heuristics are used to clean the data in the filtered version, where we eliminate anomalous workout samples and determining characteristics like distance and speed. Our dataset is interpolated in the resampled version with the aim to preserve consistent sampling intervals, which in turn effectively makes analysis easier. To address user privacy concerns, these datasets are great research tools for heart rate forecasts, activity analytics, and tailored fitness advice.

4.2. Overall performance comparison of existing and our proposed methods

Table 1 outlines a comprehensive performance comparison between existing and proposed methods, employing a learning rate of 80%. This evaluation encompasses crucial metrics to gauge the predictive accuracy of the models. Specifically, the proposed approach attains a remarkable (MSE) of 0.256944, signifying its enhanced predictive capabilities. Regarding (MSRE), the proposed method yields a competitive value of 0.238948, underscoring its precision. Notably, the (NMSE) is 0.374894, highlighting its adeptness at

capturing data variations. (RMSE) stands at 0.216582, and (MAPE) is 0.277677. These values collectively emphasize the consistent outperformance of the proposed approach across diverse metrics, making it a robust choice for predictive tasks.

Table 2 provides insights of predicted heart rates during robust sports activities. For a heart rate prediction of 140, the recommendation is “Yes,” stating that the user is doing well in their performance. When the predicted heart rate is 170, and the context is “Yes”, the advice to the user is “Slow down,” indicating a need to reduce exertion. Similarly, when the predicted heart rate is 170 with a context of “Yes” for robust sports, the guidance is to “Change path,” suggesting a modification in the activity to maintain a safe and effective level of exercise intensity. This table offers valuable real-time insights for individuals engaged in robust sports to optimize their performance and well-being.

Table 1. Existing vs. Proposed performance analysis (learning rate: 80%)

| Metrics | SOA | MBO | DCNN | LSTM | DBN | Proposed |
|---------|----------|----------|----------|----------|----------|----------|
| MSE | 0.295623 | 0.267586 | 0.282325 | 0.279991 | 0.268986 | 0.256944 |
| MSRE | 0.269526 | 0.287045 | 0.272566 | 0.241884 | 0.249322 | 0.238948 |
| NMSE | 0.425365 | 0.41762 | 0.421756 | 0.394538 | 0.39175 | 0.374894 |
| RMSE | 0.28521 | 0.261175 | 0.249762 | 0.219244 | 0.226011 | 0.216582 |
| MAPE | 0.289562 | 0.333592 | 0.28109 | 0.320222 | 0.301559 | 0.277677 |

Table 2. Predicted heart rate recommendations analysis

| Predicted heart rate | Robust sport | Result |
|----------------------|--------------|-------------|
| 140 | Yes | Doing well |
| 170 | Yes | Slow down |
| 170 | Yes | Change path |

The performance of the suggested strategy with and without feature selection is compared in Table 3. The metrics evaluated encompass vital aspects of predictive accuracy. Without feature selection, the method yields an (MSE) of 0.363888, indicating the initial prediction variance. (MSRE) is 0.324907, reflecting the relative disparities in predictions. (NMSE) is 0.482157, signifying the model’s adjustment to data variations. (RMSE) is 0.390247, and (MAPE) is 0.356611. However, with feature selection, performance improves across the board. MSE drops to 0.317672, MSRE improves to 0.295422, NMSE enhances to 0.429166, RMSE decreases to 0.378733, and MAPE improves significantly to 0.311318, highlighting the impact of feature selection in enhancing predictive accuracy.

Table 3. Impact of feature selection on accuracy

| Metrics | Without feature selection | With feature selection |
|---------|---------------------------|------------------------|
| MSE | 0.363888 | 0.317672 |
| MSRE | 0.324907 | 0.295422 |
| NMSE | 0.482157 | 0.429166 |
| RMSE | 0.390247 | 0.378733 |
| MAPE | 0.356611 | 0.311318 |

Figure 2 displays the comparison of metrics with and without feature selection. It has been noted that the NMSE matrix, both with and without feature selection, shows the highest values compared to the others. Figure 3 shows the comparison between the proposed and existing algorithm where Figures 3(a) and (b) shows the encryption and decryption time respectively. The proposed approach performs noticeably faster by 0.040 ms than SOA and MBO. This suggests that the proposed algorithm performs well when quickly encrypting data, making it a viable option for applications where encryption speed is of the essence. The proposed method once proves its superiority with a decryption time of only 0.832 ms. This result suggests that the proposed method performs admirably in terms of encryption speed and decryption efficiency.

Figure 4 shows the comparison between the proposed and existing methods at different learning rates at 80% and 70% learning rate, where Figures 4(a) and (b) shows the accuracy and precision comparison respectively. The proposed approach achieves the highest accuracy at 98.21% when accuracy is at an 80% learning rate. Similarly, the proposed approach maintains its lead with an accuracy of 97.92% at a 70% learning rate. The proposed approach has the best precision at 97.56% at 80% learning rate, indicating its ability to reduce false positives. The proposed algorithm maintains its precision advantage at a 70% learning rate, attaining 96.22%.

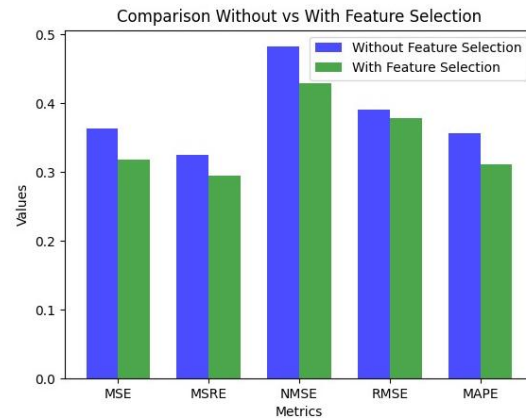


Figure 2. Comparison of with and without feature selection

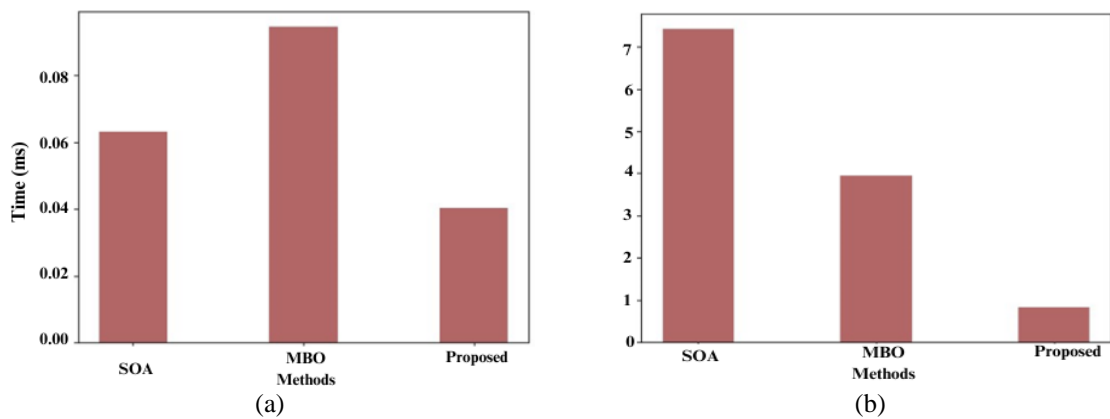
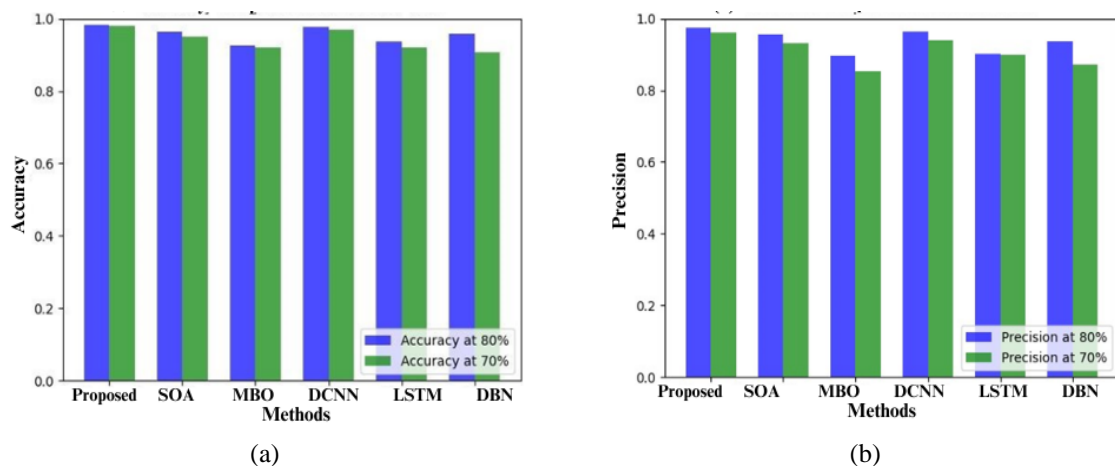
Figure 3. Comparison between the proposed and existing algorithm
(a) encryption time and (b) decryption timeFigure 4. Comparison of the proposed and existing methods at 80% and 70% learning rate
(a) accuracy and (b) precision

Figure 5 shows how the MSMBO algorithm improves over epochs. The 'Best Fitness Value' tells us how good the best solution is during the optimization process, varying with the number of epochs. The best fitness value drops as the epochs increase, showing that the algorithm finds better solutions. At first, there is a sharp drop, indicating rapid improvement early on. Later, the line flattens out with occasional dips, suggesting the algorithm makes fine adjustments toward the best possible solution. This trend shows how effectively the MSMBO algorithm zeroes in on an optimal solution over time.

Figure 6 displays 3D data visualizations that map heart rate against latitude, longitude, and altitude. In Figure 6(a) shows heart rate changes along a route with significant altitude fluctuations, while Figure 6(b) depicts a more stable altitude and steady heart rate changes, suggesting a consistent physical effort. In Figure 6(c) features rapid altitude and heart rate changes, possibly indicating intense activity. It shows clearly, how heart rate varies with location and elevation, highlighting the impact of environmental factors on physical exertion.

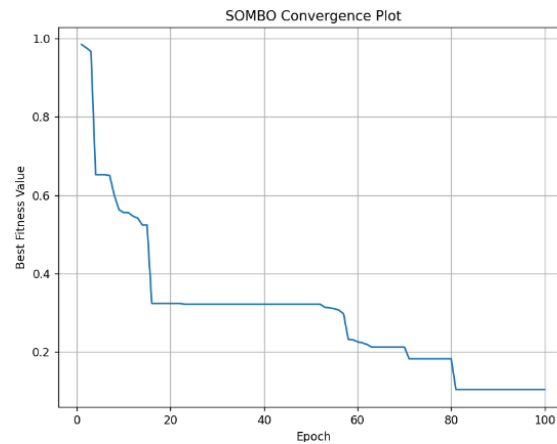


Figure 5. MSMBO convergence plot

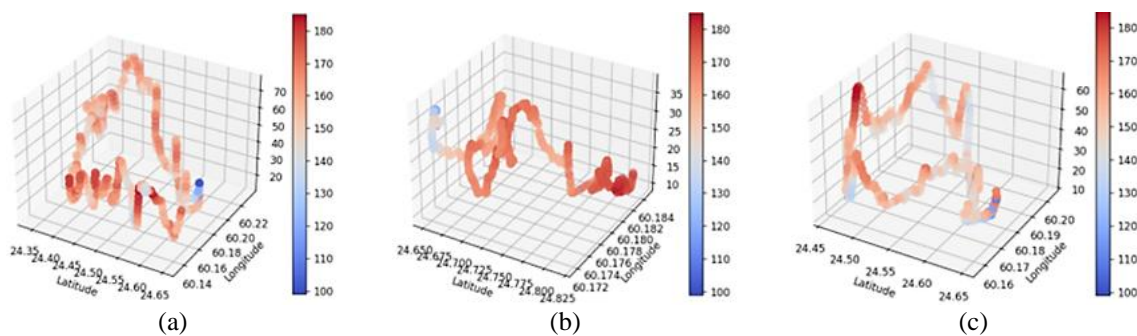


Figure 6. 3D Data visualization mapping map heart rate against latitude, longitude, and altitude: (a) heart rate changes along a route with significant altitude fluctuations, (b) stable altitude and steady heart rate changes, suggesting a consistent physical effort, and (c) features rapid altitude and heart rate changes, possibly indicating intense activity

5. CONCLUSION

Recent observations by several research groups suggest that the integration of deep learning and privacy-preserving optimization significantly enhances the performance of fitness-recommender systems. Our findings try to bridge the gap that this phenomenon is not due to elevated computational complexity or feature redundancy but associated with improved predictive accuracy and strengthened data privacy. The proposed model, implemented in Python, performs such as LSTM, DCNN, DBN, SOA, and MBO across multiple evaluation metrics, including RMSE, NMSE, MSE, MAPE, and MSRE. We showed several enhanced preprocessing methods such as noise removal, standardization, and normalization played a critical role in refining raw IoT data which enables robust feature extraction through ConvCaps and Bi-LSTM networks. The addition of RFE further optimized model efficiency by eliminating irrelevant features and mitigating overfitting.

The novel MSMBO, when combined with IECC, achieved two objectives: i) efficient encryption with reduced latency and ii) accurate and real-time recommendation generation. These advancements collectively led to a recommendation accuracy of 98.9%, outperforming benchmark models lacking integrated privacy frameworks. Our study shows that, in contrast to traditional systems that focus on either

privacy or personalization, both can be accomplished at the same time with a well-thought-out architecture that includes deep spatio-temporal modelling, end-to-end encryption, differential privacy, and user-controlled permissions.

However, more research is necessary to validate the system's flexibility across a range of deployment circumstances and demographics. Furthermore, scalability on low-power edge devices may be constrained by the computational intensity of ConvCaps-BiLSTM and MSMBO. Future studies that concentrate on federated learning and lightweight model compression are crucial to enhancing the suggested system's efficiency, generalizability, and deployment readiness.

FUNDING INFORMATION

Authors state no funding involved

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

| Name of Author | C | M | So | Va | Fo | I | R | D | O | E | Vi | Su | P | Fu |
|----------------|---|---|----|----|----|---|---|---|---|---|----|----|---|----|
| Esmita Gupta | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Shilpa Shinde | | | | ✓ | | | | | | ✓ | | ✓ | ✓ | |

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that supports the findings of this study are available from the corresponding author [IA] on request.




REFERENCES

- [1] J. J. Ferreira, C. I. Fernandes, H. G. Rammal, and P. M. Veiga, "Wearable technology and consumer interaction: a systematic review and research agenda," *Computers in Human Behavior*, vol. 118, p. 106710, May 2021, doi: 10.1016/j.chb.2021.106710.
- [2] C. Crema, A. Depari, A. Flammini, E. Sisinni, T. Haslwanter, and S. Salzmann, "Characterization of a wearable system for automatic supervision of fitness exercises," *Measurement: Journal of the International Measurement Confederation*, vol. 147, p. 106810, Dec. 2019, doi: 10.1016/j.measurement.2019.07.038.
- [3] E. Sisinni *et al.*, "On feature selection in automatic detection of fitness exercises using LSTM models," In *2022 IEEE Sensors Applications Symposium (SAS)*, pp. 1-6, Aug. 2022, doi: 10.1109/SAS54819.2022.9881338.
- [4] Z. Zhang, Z. Pi, and B. Liu, "TROIKA: a general framework for heart rate monitoring using wrist-type photoplethysmographic signals during intensive physical exercise," *IEEE Transactions on Biomedical Engineering*, vol. 62, no. 2, pp. 522-531, Feb. 2015, doi: 10.1109/TBME.2014.2359372.
- [5] C. Massaroni *et al.*, "Validation of a wearable device and an algorithm for respiratory monitoring during exercise," *IEEE Sensors Journal*, vol. 19, no. 12, pp. 4652-4659, Jun. 2019, doi: 10.1109/JSEN.2019.2899658.
- [6] S. Ishii, A. Yokokubo, M. Luimula, and G. Lopez, "Exersense: physical exercise recognition and counting algorithm from wearables robust to positioning," *Sensors (Switzerland)*, vol. 21, no. 1, pp. 1-16, Dec. 2021, doi: 10.3390/s21010091.
- [7] W. Li, L. Lu, A. G. P. Kottapalli, and Y. Pei, "Bioinspired sweat-resistant wearable triboelectric nanogenerator for movement monitoring during exercise," *Nano Energy*, vol. 95, p. 107018, May 2022, doi: 10.1016/j.nanoen.2022.107018.
- [8] S. Mekruksavanich and A. Jitpattanakul, "CNN-based deep learning network for human activity recognition during physical exercise from accelerometer and photoplethysmographic sensors," in *Lecture Notes on Data Engineering and Communications Technologies*, vol. 117, Springer Nature Singapore, 2022, pp. 531-542.
- [9] A. Gyrard and A. Sheth, "IAMHAPPY: towards an IoT knowledge-based cross-domain well-being recommendation system for everyday happiness," *Smart Health*, vol. 15, p. 100083, Mar. 2020, doi: 10.1016/j.smhl.2019.100083.
- [10] M. Budig, V. Hölte, and M. Keiner, "Accuracy of optical heart rate measurement and distance measurement of a fitness tracker and their consequential use in sports," *German Journal of Exercise and Sport Research*, vol. 49, no. 4, pp. 402-409, Sep. 2019, doi: 10.1007/s12662-019-00621-1.
- [11] M. Finck and F. Pallas, "They who must not be identified-distinguishing personal from non-personal data under the GDPR," *International Data Privacy Law*, vol. 10, no. 1, pp. 11-36, Feb. 2020, doi: 10.1093/idpl/ipy026.
- [12] S. Wachter, "Normative challenges of identification in the internet of things: privacy, profiling, discrimination, and the GDPR," *Computer Law and Security Review*, vol. 34, no. 3, pp. 436-449, Jun. 2018, doi: 10.1016/j.clsr.2018.02.002.




- [13] M. Abdulaziz, B. Al-motairy, M. Al-ghamdi, and N. Al-qahatani, "Building a personalized fitness recommendation application based on sequential information," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 1, pp. 637–648, 2021, doi: 10.14569/IJACSA.2021.0120173.
- [14] B. Alhijawi and Y. Kilani, "A collaborative filtering recommender system using genetic algorithm," *Information Processing and Management*, vol. 57, no. 6, p. 102310, Nov. 2020, doi: 10.1016/j.ipm.2020.102310.
- [15] R. Gilgen-Ammann, T. Schweizer, and T. Wyss, "RR interval signal quality of a heart rate monitor and an ECG holter at rest and during exercise," *European Journal of Applied Physiology*, vol. 119, no. 7, pp. 1525–1532, Apr. 2019, doi: 10.1007/s00421-019-04142-5.
- [16] M. Zappatore, A. Longo, A. Martella, B. Di Martino, A. Esposito, and S. A. Gracco, "Semantic models for IoT sensing to infer environment–wellness relationships," *Future Generation Computer Systems*, vol. 140, pp. 1–17, Mar. 2023, doi: 10.1016/j.future.2022.10.005.
- [17] G. Tiwari and S. Gupta, "An mmWave radar based real-time contactless fitness tracker using deep CNNs," *IEEE Sensors Journal*, vol. 21, no. 15, pp. 17262–17270, Aug. 2021, doi: 10.1109/JSEN.2021.3077511.
- [18] A. Temko, "Accurate heart rate monitoring during physical exercises using PPG," *IEEE Transactions on Biomedical Engineering*, vol. 64, no. 9, pp. 2016–2024, Sep. 2017, doi: 10.1109/TBME.2017.2676243.
- [19] L. Ye and Y. Zheng, "The image processing using soft robot technology in fitness motion detection under the internet of things," *IEEE Access*, vol. 10, pp. 115815–115822, 2022, doi: 10.1109/ACCESS.2022.3218893.
- [20] Y. C. Chou, B. Y. Ye, H. R. Chen, and Y. H. Lin, "A real-time and non-contact pulse rate measurement system on fitness equipment," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–11, 2022, doi: 10.1109/TIM.2021.3136173.
- [21] A. Thomas and V. P. Gopi, "Accurate heart rate monitoring method during physical exercise from photoplethysmography signal," *IEEE Sensors Journal*, vol. 19, no. 6, pp. 2298–2304, Mar. 2019, doi: 10.1109/JSEN.2018.2886001.
- [22] A. J. L. Sanz, J. L. Díez, M. Giménez, and J. Bondia, "Enhanced accuracy of continuous glucose monitoring during exercise through physical activity tracking integration," *Sensors (Switzerland)*, vol. 19, no. 17, p. 3757, Aug. 2019, doi: 10.3390/s19173757.
- [23] Y. Kong and K. H. Chon, "Heart rate tracking using a wearable photoplethysmographic sensor during treadmill exercise," *IEEE Access*, vol. 7, pp. 152421–152428, 2019, doi: 10.1109/ACCESS.2019.2948107.
- [24] A. Procházka, H. Charvátová, S. Vaseghi, and O. Vyšata, "Machine learning in rehabilitation assessment for thermal and heart rate data processing," *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 26, no. 6, pp. 1209–1214, Jun. 2018, doi: 10.1109/TNSRE.2018.2831444.
- [25] A. Nicolò, C. Massaroni, E. Schena, and M. Sacchetti, "The importance of respiratory rate monitoring: from healthcare to sport and exercise," *Sensors (Switzerland)*, vol. 20, no. 21, pp. 1–45, Nov. 2020, doi: 10.3390/s20216396.
- [26] H. Lee, H. Chung, H. Ko, and J. Lee, "Wearable multichannel photoplethysmography framework for heart rate monitoring during intensive exercise," *IEEE Sensors Journal*, vol. 18, no. 7, pp. 2983–2993, Apr. 2018, doi: 10.1109/JSEN.2018.2801385.
- [27] M. A. Motin, C. K. Karmakar, and M. Palaniswami, "PPG derived heart rate estimation during intensive physical exercise," *IEEE Access*, vol. 7, pp. 56062–56069, 2019, doi: 10.1109/ACCESS.2019.2913148.
- [28] W. Sands *et al.*, "Recommendations for measurement and management of an elite athlete," *Sports*, vol. 7, no. 5, p. 105, May 2019, doi: 10.3390/sports7050105.
- [29] M. R. Avram and F. Pop, "Real-time running workouts monitoring using cloud–edge computing," *Neural Computing and Applications*, vol. 35, no. 19, pp. 13803–13822, Jan. 2023, doi: 10.1007/s00521-021-06675-3.
- [30] FitRec project dataset, University of California San Diego, 2020 [Online]. Available: <https://sites.google.com/eng.ucsd.edu/fitrec-project/home>

BIOGRAPHIES OF AUTHORS



Esmita Gupta    is an assistant professor in Department of Information Technology, working in BKBC, University of Mumbai. She holds an M.E. in Information Technology, an MBA in HR, MCA, and B.E. in Computer Engineering, University of Mumbai. She has published more than 12 papers in International and National Journals and Conferences and have 2 patents on her name. She has also received two minor research grants from University of Mumbai. She is a member of Computer Society of India and Society for data science. Her main research interests focus on data science, data analytics, and security. She is also pursuing a Ph.D. in Computer Engineering, focusing on innovative solutions for secure, personalized recommender systems. She can be contacted at email: esmita.g@gmail.com.



Dr. Shilpa S. Shinde    have received B.E. degree in Computer Engineering from Marathwada University in July 2001, M.E. degree in Computer Engineering from University of Mumbai in August 2008 and Ph.D. from University Mumbai in Information Technology in March, 2019. She is presently holding position of associate professor in Computer Engineering department at Ramrao Adik Institute of technology, Navi Mumbai. She has published more than 40 papers in International and National Journals and Conferences and 3 copyright and 1 patent on her name. Under her supervision 6 research scholars working towards their Ph.D. She is a life member of, Indian Society for Technical Education (ISTE), Computer Society of India (CSI) She is reviewer of reputed journals and conferences. She received two minor research grants from University of Mumbai. She can be contacted at email: shilpa.shinde@rait.ac.in.