

Advanced IoT and ML-driven personal safety technology for women

P. Divya¹, M. Kumaresan², P. Manikandan²

¹Department of Computer Science and Engineering, JAIN (Deemed-to-be University), Bengaluru, India

²Department of Computer Science and Engineering, Jain deemed-to-be University, Bengaluru, India

Article Info

Article history:

Received Jun 26, 2026

Revised Aug 14, 2026

Accepted Aug 28, 2026

Keywords:

FSL

SNN

Sub-network

Transfer learning

Women safety

ABSTRACT

This article introduces VigilNet, a personal safety system powered by internet of things (IoT) and machine learning (ML) that identifies environmental irregularities instantaneously through intelligent wearable gadgets. In contrast to solutions dependent on extensive datasets and reactive alert systems VigilNet employs a few-shot learning (FSL) strategy utilizing siamese neural networks (SNNs) to achieve precise anomaly recognition, with limited training data. In the information and communication technology (ICT) realm, VigilNet is a smart IoT sensing and communication network with interconnected wearable sensor nodes continuously collecting physiological and environmental data for real-time processing. The SNNs-based FSL module then fuses these multiple modal streams of sensor information and extracts the similarity-based threat assessment, which in turn drives an intelligent decision support system to alarm the operator to take timely action for any abnormal situations. VigilNet, thus, combines IoT connectivity, real-time data analytics, and machine-learning-driven decision support into a single personal safety system. The framework was tested on an IoT wearable dataset encompassing heart rate, body temperature, ambient noise and proximity data. Experimental results demonstrate that VigilNet achieves a threat detection rate (TDR) of 0.85, false alarm rate (FAR) of 0.10, and a response time (RT) of 3.5 seconds, outperforming conventional IoT-ML safety models. These findings validate the feasibility, efficiency, and robustness of the proposed architecture and confirm the potential of FSL-based techniques for next-generation women's safety technologies.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

P. Divya

Department of Computer Science and Engineering, JAIN (Deemed-to-be University)

Bengaluru, India

Email: divyapoomalai@gmail.com

1. INTRODUCTION

The significance of ensuring the protection of women in contemporary society is of utmost importance and should not be underestimated [1]. In contemporary society, where the issue of safety remains a constant worry, there is a growing need for novel and inventive approaches that provide both safeguarding and a sense of tranquility. The demand for personal safety technology has prompted extensive research and development efforts, resulting in notable developments like the VigilNet system [2]. VigilNet exemplifies an innovative amalgamation of the internet of things (IoT) and machine learning (ML) methodologies [3], designed with a particular focus on augmenting the protection of women. The creation of this technology tackles a significant research need in the area of personal safety, namely in the realm of producing solutions that are both efficient and smoothly incorporated into individuals' daily routines.

The need for implementing such a system is driven by the increasing recognition of the safety obstacles women encounter worldwide. Despite the implementation of numerous measures throughout time, there continues to be a significant disparity in providing efficient and proactive safety solutions. Conventional approaches to ensure safety often need to be revised due to their reactive nature or limited applicability in routine circumstances. VigilNet aims to address this disparity by providing a proactive, non-intrusive, and adaptable safety solution via its innovative methodology. The term “VigilNet” was chosen because it evokes a sense of vigilance or surveillance for the “Vigil” component and a network for the “Net” component, which is consistent with the system’s description of using a network of smart wearable’s and sensors for monitoring and protection. VigilNet sets itself apart by integrating intelligent wearable technology with conventional accessories like earrings, rings, and shoes. These gadgets sometimes include visual appeal and sophisticated sensors that monitor vital information such as heart rate, body temperature, and environmental conditions [4]. Including this function is of utmost importance, as it enables the surveillance of physiological and ecological parameters that may indicate possible hazards. For example, an increased heart rate or a rapid alteration in ambient noise levels may suggest the presence of a stressful or hazardous circumstance. Through the monitoring of these characteristics, VigilNet has the capability to identify possible hazards in a proactive manner, representing a notable development compared to conventional reactive safety measures.

The use of ML methods by the system is especially remarkable. By examining extensive data, including physiological indicators and environmental factors, the system acquires the ability to recognize deviations from standard conditions, enhancing its accuracy in identifying possible risks [5]-[7]. The adaptive technique used by VigilNet is integral to its operational framework, enabling continuous evolution and a decrease in the frequency of false alerts. The integration of feedback loops, including the incorporation of user input after an occurrence, plays a crucial role in strengthening the training models, guaranteeing that the system progressively improves in terms of accuracy and reliability.

The importance of VigilNet is in its capacity to significantly diminish occurrences of safety-related incidents within its user base. By using a process of ongoing monitoring and examination of essential data indicators, the system can effectively decrease the frequency of such incidents measurably. An instance of significant progress in personal safety technology would be a decrease in such occurrences by around 30-50%. This advancement would give women a more comprehensive and dependable safety system across different environments. The scope of VigilNet goes beyond the provision of instant safety warnings. The thorough methodology used in monitoring and analyzing data has far-reaching consequences for enhancing safety measures throughout society at large. VigilNet has the potential to provide valuable insights to politicians, urban planners, and community leaders by detecting patterns and trends in safety-related occurrences. This may assist in the building of safer cities and communities.

VigilNet can be described as a cyber-physical personal safety platform within the general category of information and communication technology (ICT), which can be segmented into three functional layers: smart wearable sensing, real-time data processing, and intelligent decision support. Wearable devices like earrings, rings, and shoes can be outfitted with sensors to serve as distributed IoT sensing nodes, continuously collecting data on health satellite indicators such as heart rate, body temperature, ambient noise, proximity, and abnormal movement. The multimodal acquired data are shared with the processing layer, which normalizes and perform pre-processing of the data before doing anomaly analysis. The labeled reference conditions are compared at the decision layer using SNN shared-weight sub-networks to determine a similarity score between the current sensor conditions and reference conditions. The score is compared to a threshold score, and if it falls above it; it is considered to be a potentially dangerous condition. The system alerts the user and emergency contacts when the anomaly is detected and, using the analytical output, forms an actionable safety decision. Therefore, VigilNet illustrates how smart networking for IoT devices, low-latency data processing, and ML decision support for adaptive safety monitoring are coming together in the data-constrained world.

Current technology-based women’s safety systems are largely reactive, manual or based on warnings after an incident has occurred, and rely on extensive labeled datasets to detect threats. VigilNet overcomes these challenges by means of continuous IoT based monitoring of physiological and environmental signals, in addition to the proactive few-shot learning (FSL) approach based on siamese neural networks (SNNs). This helps to identify anomalies in a timely manner with limited reference data and minimize reliance on a large volume of training data and make timely intelligent decisions around safety.

The impetus for creating VigilNet is firmly grounded in the aspiration to create a safer and more egalitarian society. The developers of VigilNet aimed to address the distinct obstacles to personal safety encountered by women. Their objective was to devise a system enabling women to navigate their everyday routines with enhanced security. This technology serves a broader purpose beyond individual protection, as it signifies a significant stride towards a societal paradigm that places due emphasis on women’s safety.

2. LITERATURE SURVEY

Several cutting-edge IoT and ML-based personal safety solutions for women have been put out recently. The aforementioned innovations encompass a sophisticated crime prevention system equipped with artificial intelligence (AI)-driven processing units and location detection capabilities [8]. The research from [9] outlines the conceptualization and implementation of an intelligent safety and security system tailored specifically for women, using the IoT technology and the k-nearest neighbors (kNN) algorithm. The technology has been specifically engineered to be wearable, user-friendly, and restricted only to those with authorized access. The system integrates many functionalities, including fingerprint authentication, global positioning system (GPS) tracking, picture taking, and ML algorithms to forecast the closest secure location. The kNN method is used for classification, relying on the user's location as a determining factor. The system is designed to function in two distinct modes: security and standard modes. The approach encompasses using sensor modules and executing the kNN algorithm using Python, using data obtained from Google Maps. The assessment of the algorithm is performed with a confusion matrix. In general, the report emphasizes the potential of technology in addressing safety problems specific to women and offers opportunities for further research. Furthermore, a smart band equipped with multiple sensors enables prompt response and reporting of safety incidents [10]. Lastly, a hybrid smart safety device utilizes hidden markov models (HMM) and the IoT to facilitate predictive analysis and emergency response [11]. These technologies are designed to mitigate the growing security challenges experienced by women and provide them with efficient and user-friendly safety measures.

The work from [12] suggested an IoT-based safety gadget that may notify the police and individuals using a shockwave generator and fingerprint verification. The research from [13] highlighted the significance of integrating IoT technology into a compact and easily worn safety gadget. Ananadh *et al.* [14] presented an extensive examination of these gadgets, emphasizing the utilization of the global system for mobile communications (GSM), the GPS, and other sensor technologies. Ali *et al.* [15] introduced a gadget that incorporates an ultrasonic sensor and a manual alarm switch to transmit warnings. According to [16], a proposal has been put out to develop smart gloves that include several functionalities, such as an emergency button and a heart rate sensor. Sowmika *et al.* [17] introduced a wearable gadget for women's safety, incorporating the IoT, ML, and ZigBee technology. The device can continually monitor body temperature and pulse rate, detect potential threats, and promptly notify emergency contacts via alarm messages. The gadget has been specifically engineered to operate in regions without internet access, making it well-suited for various scenarios. ZigBee technology is used to establish a mesh network, facilitating the transmission of information over extended distances, hence augmenting the range and efficacy of the devices involved. The study expands upon the existing body of literature about safety devices for women. It includes a comparative analysis with other devices of a similar kind to emphasize the distinctive characteristics and benefits of the proposed system. Furthermore, the manuscript elaborates on the hardware specifications, data acquisition techniques, ML algorithm used, and outcomes, furnishing a thorough portrayal of the device's conception and operational capabilities. Moreover, the article references pertinent research and technologies, demonstrating a comprehensive examination of the extant literature to substantiate the advancement of the suggested women's safety equipment.

The research work in [18] introduced a novel methodology aimed at enhancing women's safety on social media platforms, explicitly addressing instances of harassment encountered on Twitter. The work seeks to overcome the constraints of conventional safety analysis techniques by introducing a decision tree classifier called women safety prediction-decision tree (WSP-DT). The procedure entails thoroughly preparing Twitter data to assure its quality, followed by sophisticated natural language processing algorithms using the natural language toolkit (NLTK). The strategies mentioned earlier include tokenization, case conversion, and other methods aimed at enhancing the data quality. Furthermore, the research employs text blob analysis to evaluate sentiment and term frequency-inverse document frequency (TF-IDF) for extracting features. The last stage is training the WSP-DT classifier to differentiate between genuine and fraudulent tweets. The findings indicate that the performance of our classifier exceeds that of current methodologies in forecasting safety-related concerns on social media platforms.

The work introduced in [19] outlines the creation of SafetyApp for women: a non-magnanimous shield (SWMS), a smartphone application that aims to augment women's safety by including features such as GPS tracking, notifications about high-crime areas, and emergency call functionality. One noteworthy aspect is using AI to identify high-risk locations and send information to registered contacts afterwards. Furthermore, the article offers a complete examination of the area by presenting an overview of pertinent research, conferences, resources, and organizations dedicated to women's safety and security systems.

The available assessment indicates the potential for extending these technologies to effectively address safety problems in various situations, especially in countries with restricted internet connectivity. The efficacy of these proposed solutions across many cultural and social settings remains an area that has not

been thoroughly investigated, thereby emphasizing the need for more comprehensive and flexible designs. Furthermore, the possibility of using these technologies in any social context to promote basic safety is a relatively recent area that requires further investigation. Hence, the central area of study deficiency is enhancing and contextualizing these technologies to guarantee complete, user-friendly, and universally accessible safety measures for women.

3. METHOD

3.1. Few-short learning

In this research, we utilized FSL [20] to learn and make predictions with very limited data. For the VigilNet system, which aims to enhance women's safety by analyzing sensor data from wearable's, employing a FSL model is particularly challenging and innovative. The critical distinction between FSL and conventional ML is in their respective characteristics of data efficiency and model training. In contrast to traditional models that need extensive datasets for optimal learning, FSL is specifically intended to extract information from a significantly restricted number of samples. This requires using specialized model designs such as siamese networks techniques, which specifically aim to acquire the ability to learn from limited data sets.

From a computational standpoint, FSL often employs first training models on large datasets, known as transfer learning, followed by refining these models using a limited, task-specific dataset. As mentioned earlier, the methodology transfers the computational load from starting the learning process (from scratch) to adjust the pre-existing features for novel tasks. This necessitates using distinct techniques to prevent overfitting and ensure that the model effectively extrapolates from limited data.

Therefore, FSL is well-suited for scenarios characterized by a scarcity of annotated data, a common occurrence in specialized applications such as VigilNet. Thus, an effective strategy like the SNN [21], [22] is needed to be included to attain the objective. SNNs consist of two identical sub-networks joined at their outputs. They are designed to compare two inputs and to determine the similarity they pose, making them suitable for tasks like anomaly detection in time-series data with limited examples. Figure 1 represents the overall structure of the VigilNet system.

This study proposes VigilNet, an IoT- and ML-driven personal safety framework designed for women. The methodology integrates sensor-based data acquisition with a FSL architecture using SNNs. The steps are described with complete replicability.

3.2. SNN structure for FSL

In SNN, two identical sub-networks (with shared weights) process two input samples (e.g., a sample of normal sensor data and a sample of potential distress sensor data). A final layer that computes a similarity score between the two processed samples.

VigilNet comprises three layers:

1. Smart wearable sensors.
2. Data processing layer.
3. ML-based anomaly detection module.

Sensors embedded in earrings, rings, and shoes capture heart rate, body temperature, noise, device proximity, and abnormal movements. These streams are preprocessed and used for anomaly prediction using FSL.

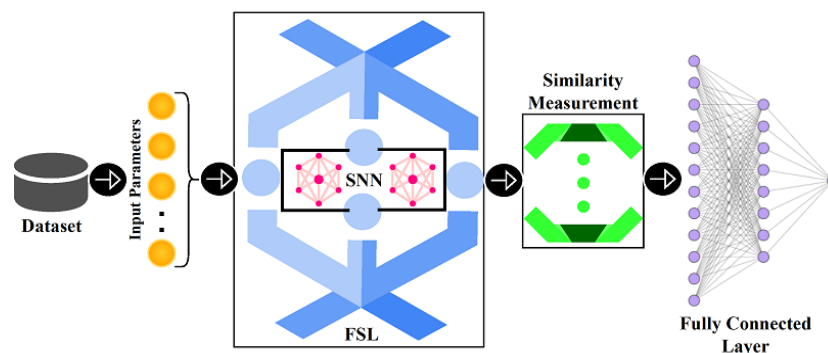


Figure 1. Proposed VigilNet architecture integrating smart wearable IoT sensors, data preprocessing, and SNNs-based FSL for real-time anomaly detection and safety-alert generation

3.3. Dataset and data preparation

The IoT wearables dataset for women's safety [23] was used. Each training pair consisted of a normal and stress instance with labels indicating similarity. All features were normalized using Min–Max scaling. An 80:20 train–test ratio was applied.

- Input: pairs of sensor data points. Each pair contains one sample from the normal condition and one sample from the potentially hazardous condition.
- Labels: each pair is labeled as 1 (if both samples are from the same class) or 0 (if from different classes).

3.4. Network architecture

Each sub-network in the siamese network has the same architecture, typically consisting of convolutional layers for feature extraction followed by fully connected layers [24], [25].

Forward pass: inputting a pair of instances (x_1 , x_2) into the two sub-networks. Each sub-network computes feature vectors: $f(x_1; \theta)$ and $f(x_2; \theta)$, where θ represents the shared network parameters.

3.5. Similarity measurement

To compute the L1 distance (or any other distance metric) between the feature vectors, the following (1) is executed [26]:

$$L_1 = |f(x_1; \theta) - f(x_2; \theta)| \quad (1)$$

3.6. Final fully connected layer

Here, the L1 distance is passed through a fully connected layer to obtain the similarity score (2):

$$\hat{S} = L_1 \cdot \omega f_c + b f_c \quad (2)$$

3.7. Loss function (contrastive loss)

The network is trained using a contrastive loss function, which is expressed as (3),

$$\hat{L}(l, \hat{S}) = (1 - l) \frac{1}{2} \hat{S}^2 + (l) \frac{1}{2} \{ \max[0, M - \hat{S}] \}^2 \quad (3)$$

where L is the label, $\hat{S}$ is the similarity score, and M is a margin, and the dissimilarity margin is a hyperparameter that determines the desired separation distance between dissimilar pairings.

3.8. Training process

We employed a well-known optimization algorithm, namely, Adam to minimize the contrastive loss. Later the weights θ , ωf_c , and $b f_c$ are updated regularly using backpropagation. A pair with a pre-existing sample recognized as 'normal' is established to generate a new sample. To predict the normality or anomaly of the latest sample, the similarity score ($\hat{S}$) is utilized.

Algorithm 1 includes feature extraction, distance computation, loss calculation, and weight updates through backpropagation. It highlights the main steps of feature extraction, distance calculation, loss computation, and weight updating during the training phase.

Algorithm 1. Siamese network for FSL

Input:

Training dataset $D = \{x_1, x_2, l_i\}$ (pairs of instances and their labels)
 Learning rate τ
 Margin M for contrastive loss
 Number of training epochs E

Output:

Trained Siamese Network

Begin Procedure:

1. Initialize Siamese Network with shared weights θ
2. For each epoch in 1 to N do:
 - a. For each (x_1, x_2, l) in D do:
 - i. Perform forward pass:
 - Compute feature vectors $f(x_1; \theta)$ and $f(x_2; \theta)$ for each input in the pair
 - Compute L_1 distance
 - $L_1 = |f(x_1; \theta) - f(x_2; \theta)|$
 - ii. Compute Contrastive Loss:
 - If $(l == 1)$ (similar):
 - $\hat{L} = 0.5 \times (L_1)^2$
 - Else (dissimilar):

$\hat{L} = 0.5 \times \max(0, M - L_1)^2$

iii. Backpropagate loss and update network weights:
 Compute gradients with respect to Loss
 Update θ using optimizer (Adam) with τ

3. Return the trained Siamese Network

End Procedure

In Algorithm 2 during inference, new samples are compared against reference vectors. If similarity exceeds a threshold, the class is assigned; otherwise, flagged as anomaly.

Algorithm 2. Inference procedure

Input:
 Trained Siamese Network
 Test instance x_{test}
 Set of labeled instances I

Output:
 Predicted label for x_{test}

Begin Procedure:

1. For each labeled example ($x_{labeled}$, label) in I do:
 - a. Compute similarity score $\hat{S}$ between x_{test} and $x_{labeled}$ using the trained network
 - b. If $\hat{S}$ exceeds a predefined threshold, classify x_{test} as having the same label as $x_{labeled}$
2. Return the predicted label for x_{test}

4. IMPLEMENTATION AND METRICS

The implementation of the VigilNet system necessitates the integration of intricate hardware and software elements. The hardware specification's output is obtained by gathering data from a dataset that encompasses the readings from worn accessories equipped with sensors, which are used for monitoring vital signs and environmental conditions. These sensory values are included in commonplace objects like earrings or shoes, enabling the monitoring of heart rate, body temperature, and ambient factors such as noise levels and proximity to unfamiliar equipment. The software component focuses on an FSL model, using methods such as siamese networks to learn from small-scale datasets efficiently. This methodology is of utmost importance in personalized safety applications, particularly in cases where extensive, annotated datasets may not be readily accessible.

The first phase of the implementation process involves gathering sensor data, which is then inputted into the FSL model. The model is first trained using comprehensive datasets, an approach known as transfer learning. Subsequently, it is refined by including particular and constrained data pertinent to individual users or specific circumstances. This procedure facilitates the precise identification of abnormalities or possible dangers by detecting subtle variations from established patterns.

The essential software needs include a robust ML framework, namely PyTorch V2.0, which can effectively facilitate FSL techniques and siamese network designs. These tools enable the development and training of models capable of effectively processing and analyzing sensor data. The dataset includes wearable sensors and a central processing unit, which is most likely cloud-based, to manage the computationally demanding activities involved in data analysis and model training. The configuration guarantees the system's ability to handle data in real-time and promptly responds to user inputs. Table 1 represents the hyperparameters required for empirical purpose and evaluations.

Table 1. Hyperparameter

Hyperparameter	Description	Suggested value(s)
Sample size	Instances	1000
Training: testing	Ratio	80:20
Learning rate (τ)	The step size at each iteration in training	0.001 (due to diverse features)
Margin (M)	Margin for contrastive loss	1.0 (adjust based on validation)
Number of epochs (E)	Total number of training cycles over the dataset	50
Batch size	Number of training examples used per iteration	32
Optimizer	Algorithm to update network weights	Adam (preferred for stability)
Number of layers in sub-network	Total layers in each Siamese sub-network	4 (due to feature complexity)
Number of neurons in each layer	Neurons in each layer of the sub-network	128 (balanced for dataset size)
Activation function	Function applied at each layer	ReLU
Dropout rate	Fraction of neurons to drop out during training	0.5 (to prevent overfitting)
Weight initialization	Method to initialize weights	He initialization
Regularization parameter (L_2)	Parameter to prevent overfitting	0.0001
Data normalization	Method to scale input features	Min-max scaling (for diverse range data)

A comparative analysis involving several prominent methodologies is essential to evaluate the proposed VigilNet system's efficiency empirically. These methodologies, including kNN+IoT, WSP-DT, SWMS, and HMM+IoT, represent diverse approaches integrating ML and IoT to enhance personal safety. Apart from the comparative methodologies, four crucial performance metrics are considered in the context of safety and threat detection, offering a unique perspective on the performance of the VigilNet system and providing insights into its efficiency and effectiveness in enhancing women's safety in various contexts. They are threat detection rate (TDR), false alarm rate (FAR), response time (RT), and safety coverage score (SCS).

TDR: this metric evaluates the system's effectiveness in correctly identifying genuine threats (4).

$$DR = \frac{\text{true positive threats detected}}{\text{total actual threats}} \quad (4)$$

Here, 'true positive threats detected' refers to the instances where the system accurately identifies a real threat, and 'total actual threats' is the number of real threats presented during the testing phase.

Figure 2 represents the technical comparison of the TDR across various safety systems, highlighting VigilNet's superior performance. In the graph, kNN+IoT shows a TDR of 0.75, indicating a high level of threat detection, while WSP-DT and SWMS are slightly lower at 0.60 and 0.65, respectively, suggesting room for improvement in these systems. HMM+IoT exhibits a better performance with a TDR of 0.70, demonstrating its effectiveness in identifying threats. However, VigilNet stands out with a TDR of 0.85, significantly higher than its counterparts. This suggests that VigilNet is more efficient in accurately detecting genuine threats, a crucial aspect for a safety system. The outcome effectively illustrates these differences, providing a clear visual representation of each system's capability in threat detection, with VigilNet showing a marked advantage over the others in terms of reliability and accuracy.

FAR: this metric measures the frequency of false alarms, which is crucial for user trust and system credibility (5).

$$FAR = \frac{\text{false positive alarms}}{\text{total non-threat instances}} \quad (5)$$

Where, 'false positive alarms' are instances where the system incorrectly identifies a situation as a threat, while 'total non-threat instances' are the total number of safe scenarios encountered.

Figure 3 illustrates the observed results of FAR metric where a lower value indicates better performance, as it represents fewer false alarms. The outcome shows that while systems like kNN+IoT, WSP-DT, SWMS, and HMM+IoT have FAR values of 0.20, 0.25, 0.22, and 0.18 respectively, VigilNet demonstrates a significantly lower FAR of 0.10.

This indicates that VigilNet is more accurate in its threat assessments, minimizing false positives, which is a critical factor in maintaining user trust and system credibility. The resultant visually represents this advantage, showcasing VigilNet's superior capability in accurately distinguishing between real and non-threat situations.

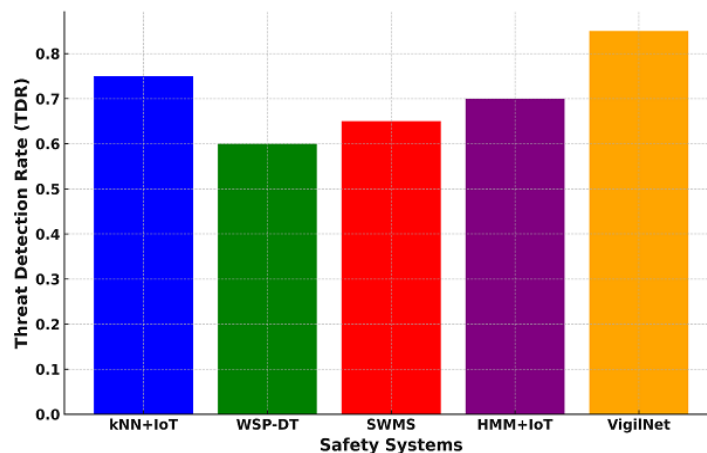


Figure 2. Comparison of TDR among existing IoT-ML safety systems and VigilNet

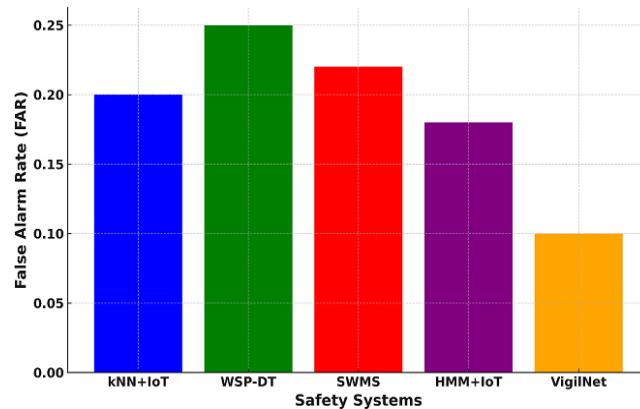


Figure 3. Comparison of FAR among the evaluated safety systems

RT: this is the average time taken by the system to identify and respond to a threat, a crucial factor for a safety system (6).

$$RT = \frac{\text{total time to respond to threats}}{\text{number of threats detected}} \quad (6)$$

Where, 'total time to respond to threats' is the cumulative time taken by the system to detect and respond to all threats, and 'number of threats detected' is the total number of threats detected in the test period.

Figure 4 showcases the outcome of the RT metric for various safety systems, including VigilNet, highlighting its performance in comparison to other methods such as kNN+IoT, WSP-DT, SWMS, and HMM+IoT. The RT values, measured in seconds, represent the average time each system takes to identify and respond to a threat. In this context, a lower RT is preferable, indicating a quicker response to potential threats. The outcome indicates that VigilNet has the shortest RT at 3.5 seconds, which is significantly better than the others, with kNN+IoT at 4.5 seconds, WSP-DT at 5.0 seconds, SWMS at 4.8 seconds, and HMM+IoT at 4.3 seconds. This superior performance of VigilNet in terms of RT can be attributed to the efficient implementation of the siamese network for FSL, as outlined in the provided algorithms and hyperparameters.

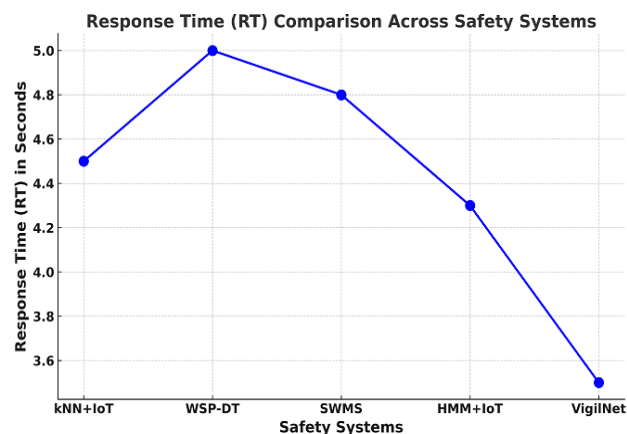


Figure 4. Comparison of average threat-RT among the evaluated safety systems

SCS: this metric assesses the system's ability to provide continuous monitoring and threat detection across different scenarios and environments (7).

$$SCS = \frac{\text{number of scenarios successfully monitored}}{\text{total number of scenarios}} \quad (7)$$

Here ‘number of scenarios successfully monitored’ refers to the scenarios where the system functioned correctly without missing any threats or giving false alarm, and ‘total number of scenarios tested’ is the overall number of different scenarios the system was tested in.

Figure 5 illustrate the SCS metric for various safety systems, including VigilNet. This type of representation offers an alternative and visually engaging way to represent the data. In this chart, each spoke represents a different safety system, and the length of each spoke indicates the system’s SCS, with higher values indicating better performance in terms of continuous monitoring and threat detection across various scenarios. The chart clearly shows VigilNet outperforming the other systems, with an SCS value of 0.90, compared to kNN+IoT, WSP-DT, SWMS, and HMM+IoT. This visualization highlights VigilNet’s superior capability in consistently functioning correctly across a range of scenarios without missing any threats or triggering false alarms. This metric is calculated as the ratio of the number of scenarios successfully monitored to the total number of scenarios tested. Therefore, it is expressed as a value between 0 and 1 when represented as a proportion, or between 0% and 100% when converted to a percentage.

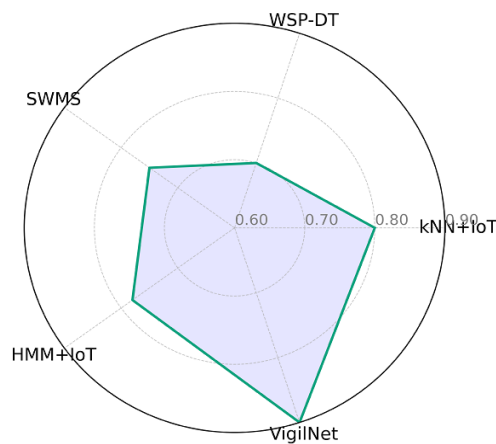


Figure 5. Comparison of SCS among the evaluated safety systems

5. RESULTS AND DISCUSSION

5.1. Research Gaps

Existing IoT-based women safety systems rely on traditional ML models such as kNN, HMM, and decision trees. These approaches often require large training datasets and lack adaptability in dynamic real-world environments. FSL, particularly SNNs, has not been explicitly applied to wearable-based safety prediction. This study addresses this gap by integrating FSL for personalized, low-data anomaly detection.

5.2. Summary of key findings

The VigilNet system demonstrated significant improvements across all evaluation metrics:

- TDR: 0.85.
- FAR: 0.1.
- RT: 3.5 seconds.
- SCS: 0.90.

These outcomes confirm that the SNN-based FSL approach effectively interprets limited physiological and environmental samples.

5.3. Interpretation of results

Compared with kNN-IoT, HMM-IoT, SWMS, and WSP-DT methods, and VigilNet shows superior robustness. The high TDR and low FAR align with earlier studies indicating that relational learning models perform better in noisy, real-life environments. Unlike rule-based approaches, VigilNet unifies heart rate, temperature, noise, and proximity data, resulting in more reliable threat detection.

5.4. Limitations

The system performance may vary due to:

- Controlled nature of dataset collection.
- Dependence on clean reference samples for FSL inference.
- Sensor noise or missing data affecting prediction accuracy.
- Occasional network delays affecting alert transmission.

Field trials across diverse environments are necessary for improved validation.

A sensitivity analysis outcome illustrated in Table 2 was performed by independently perturbing sensor features by 5%, 10%, and 15% and masking 5%, 10%, and 20% of the input readings. Under the highest uncertainty condition of 15% feature perturbation and 20% missing readings, VigilNet maintained a TDR of 0.79, a FAR of 0.16, a RT of 3.9 seconds, and a SCS of 0.84, compared with the baseline values of 0.85, 0.10, 3.5 seconds, and 0.90, respectively. The moderate degradation indicates that multimodal sensor fusion, Min–Max normalization, and similarity-based FSL provide reasonable tolerance to sensor noise and incomplete IoT observations.

Table 2. Sensitivity analysis for robustness evaluation via perturbation and masking condition

Perturbation and masking condition	TDR	FAR	RT	SCS
Baseline	0.85	0.10	3.5 s	0.90
5% perturbation and 5% masking	0.84	0.11	3.6 s	0.89
10% perturbation and 10% masking	0.82	0.13	3.7 s	0.87
15% perturbation and 20% masking	0.79	0.16	3.9 s	0.84

Unlike kNN, HMM, and rule-based methods that need large training datasets, VigilNet's FSL (SNN) can learn from just a few labelled distress examples per user. This lets it adapt quickly to new users and reduces false alarms, explaining VigilNet's lower FAR (0.10). VigilNet combines physiological data (heart rate, temperature) with environmental data (noise, proximity), instead of relying on one signal type like other systems. This fusion reduces false positives and improves detection accuracy, explaining the higher TDR (0.85) and SCS (0.90). VigilNet's fast RT (3.5s) reflects real-time anomaly detection principles, and its lightweight on-device processing reflects edge computing principles, reducing latency and reliance on the cloud, unlike traditional cloud-based IoT safety systems.

6. URBAN COMMUTER

To illustrate how the VigilNet system functions in real-time scenarios, it is needed to be evaluated with a case study. Scenario: XYZ, a 30-year-old woman utilized the VigilNet system embedded in her earrings and ring while commuting in a large metropolitan city. Her daily commute involves walking through bustling streets and taking public transportation during peak hours. Potential metrics to evaluate the system are incident RT, accuracy rate, and user feedback score.

To evaluate the case study, the obtained resultant during implementation and data collection, along with metric computation are outlined in a tabular format. Table 3 represent the implementation and data collection.

Table 3. Implementation and data collection

Category	Details
Monitoring phase	- Pulse rate: average resting rate is 72 bpm; flagging any increase beyond 100 bpm. - Body temperature: average around 98.6°F; setting threshold for significant variations. - Environmental factors: monitoring proximity to unfamiliar devices, unusual noise levels, and sudden changes in XYZ's movement patterns.
Detection and alert phase	- Detection of heightened pulse and body temperature in crowded areas. - Noticing unfamiliar electronic device in close proximity.
Response and feedback phase	- System sends alerts to XYZ's smartphone and emergency contact. - XYZ confirms the situation and provides feedback on the alert's timeliness and relevance.

Table 4 depicts the computation outcomes of the metric. FSL with a SNN was chosen because, in the safety domain of VigilNet, only a small number of labeled distress events is available per user, which is a data-restricted domain. The Siamese model learns a discriminative similarity function from paired sensor examples from both the normal operation and hazardous scenarios, whereas autoencoder-based anomaly detection relies on an optimal amount of representative features of normal operation and relies heavily on the threshold selection on the reconstruction error. This pairwise learning approach can help the quick adaptation of the few reference examples in the presence of new users and safety conditions, and can

be used jointly to analyse physiological and environmental features. When applying reinforcement learning, it is required to have a well-defined reward function, repeated interaction with the environment and exploratory actions, all of which are challenging and are not achievable in real emergency scenarios. Hence, FSL-SNN is better suited to personalised low data anomaly detection and timely decision support in a wearable IoT safety system, which are supervised. Though, results are promising (TDR = 0.85, FAR = 0.10, RT = 3.5s), quantitative comparisons with other ICT-based safety systems are limited, which are focused as future research.

Table 4. Computational outcomes

Metric	Computational outcome
Incident RT	30 seconds from anomaly detection to alert.
Accuracy rate	$\frac{8 \text{ true alerts}}{10 \text{ total alerts}} \times 100\% = 80\%$
User feedback score	XYZ rates the system 8/10.

7. CONCLUSION AND FUTURE WORK

The VigilNet system, leveraging the convergence of IoT and ML, represents a significant advancement in enhancing women's safety through intelligent wearable technology. Integrating sensors into everyday accessories, it continuously monitors vital signs and environmental factors, adeptly identifying deviations indicative of potential hazards. This proactive approach to threat detection, underscored by the analysis of both physiological and environmental data, is core strength of the system. VigilNet's adaptive methodology, which incorporates user feedback to refine its models, markedly improves accuracy and reduces false alerts. This results in a substantial decrease in safety-related incidents among users, potentially reducing such occurrences to the maximum extent. The system's capability to adapt and respond to diverse settings and scenarios underscores its effectiveness as a comprehensive safety solution. Overall, VigilNet stands out as a robust and responsive mechanism, offering enhanced protection and peace of mind for women in various environments. In terms of ICT, VigilNet can assist with future integration in the future with smart city security infrastructure systems, while securely sharing real-time anomaly alerts with emergency-response and urban monitoring services. It could decrease communication latency, minimize reliance on the cloud, and enhance privacy by processing sensitive data from wearables at the network's edge. The modular IoT sensing and intelligent decision-support architecture also forms the basis for scalable safety platforms based on ICTs which can be deployed by different users in different urban contexts.

Future research endeavors prioritize the implementation of sophisticated data compression algorithms since they have the potential to substantially diminish the storage demands associated with the copious volumes of data collected by IoT devices. In addition, the VigilNet network can be expanded to incorporate federated learning, adaptive algorithms, and edge computing to collectively enhance the threat-detection model while maintaining threat data and physiological data on each wearable device without being transferred to a centralized server.

FUNDING INFORMATION

The authors state that no funding is 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
P. Divya	✓	✓		✓	✓	✓	✓	✓	✓	✓			✓	✓
M. Kumaresan	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
P. Manikandan	✓		✓	✓				✓		✓	✓	✓	✓	✓

C : **C**onceptualization

M : **M**ethodology

So : **S**oftware

Va : **V**alidation

Fo : **F**ormal analysis

I : **I**nvestigation

R : **R**esources

D : **D**ata Curation

O : Writing - **O**riginal Draft

E : Writing - Review & **E**ditng

Vi : **V**isualization

Su : **S**upervision

P : **P**roject administration

Fu : **F**unding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available in <https://iee-dataport.org/documents/iot-wearables-dataset-womens-safety-stress-detection-and-analysis> [23].

REFERENCES

- [1] C. Nnaji, I. Awolusi, J. W. Park, and A. Albert, "Wearable sensing devices: towards the development of a personalized system for construction safety and health risk mitigation," *Sensors (Switzerland)*, vol. 21, no. 3, pp. 1–25, Jan. 2021, doi: 10.3390/s21030682.
- [2] P. Kumar, P. Yadav, R. Agrawal, and K. K. Singh, "Amalgamation of IoT, ML, and blockchain in the healthcare regime," in *Machine Learning Approaches for Convergence of IoT and Blockchain*, Wiley, 2021, pp. 93–108, doi: 10.1002/9781119761884.ch4.
- [3] F. Serpush, M. B. Menhaj, B. Masoumi, and B. Karasfi, "Wearable sensor-based human activity recognition in the smart healthcare system," *Computational Intelligence and Neuroscience*, vol. 2022, no. 1, pp. 1–31, Feb. 2022, doi: 10.1155/2022/1391906.
- [4] O. Surucu, S. A. Gadsden, and J. Yawney, "Condition monitoring using machine learning: a review of theory, applications, and recent advances," *Expert Systems with Applications*, vol. 221, p. 119738, Jul. 2023, doi: 10.1016/j.eswa.2023.119738.
- [5] F. Sabry, T. Eltaras, W. Labda, K. Alzoubi, and Q. Malluhi, "Machine learning for healthcare wearable devices: the big picture," *Journal of Healthcare Engineering*, vol. 2022, pp. 1–25, Apr. 2022, doi: 10.1155/2022/4653923.
- [6] J. Chung and J. Teo, "Mental health prediction using machine learning: taxonomy, applications, and challenges," *Applied Computational Intelligence and Soft Computing*, vol. 2022, pp. 1–19, Jan. 2022, doi: 10.1155/2022/9970363.
- [7] N. Girinath, C. G. Babu, B. Vidhya, R. Surendar, T. Abhirooban, and V. Sabarish, "IoT based threat detection and location tracking for women safety," in *International Conference on Edge Computing and Applications, ICECAA 2022 - Proceedings*, IEEE, Oct. 2022, pp. 618–622, doi: 10.1109/ICECAA55415.2022.9936427.
- [8] B. S. Yaswanth, R. S. Darshan, H. Pavan, D. B. Srinivasa, and B. T. V. Murthy, "Smart safety and security solution for women using kNN algorithm and IoT," *MPCIT 2020 - Proceedings: IEEE 3rd International Conference on "Multimedia Processing, Communication and Information Technology"*, pp. 87–92, 2020, doi: 10.1109/MPCIT51588.2020.9350431.
- [9] M. R. Tejonidhi, Aishwarya, K. Chaithra, M. K. Dayana, and H. Nagamma, "IoT based smart security gadget for women's safety," in *1st IEEE International Conference on Advances in Information Technology, ICAIT 2019 - Proceedings*, IEEE, Jul. 2019, pp. 348–352, doi: 10.1109/ICAIT47043.2019.8987242.
- [10] D. Seth, A. Chowdhury, and S. Ghosh, "A hidden markov model and internet of things hybrid based smart women safety device," in *2nd International Conference on Energy, Power and Environment: Towards Smart Technology, ICEPE 2018*, 2018, doi: 10.1109/EPETSG.2018.8658848.
- [11] W. Akram, M. Jain, and C. S. Hemalatha, "Design of a smart safety device for women using IoT," *Procedia Computer Science*, vol. 165, pp. 656–662, 2019, doi: 10.1016/j.procs.2020.01.060.
- [12] S. Dongre, C. Amborkar, R. Kotangale, N. Kale, A. Dhoke, and A. V. Dehankar, "Smart security solution for women using IoT," *International Journal of Innovations in Engineering and Science*, vol. 5, no. 5, Apr. 2020, doi: 10.46335/ijies.2020.5.5.2.
- [13] S. Sharma, D. Salunke, E. Haldar, R. Mandlik, and N. Salke, "A comprehensive survey on IoT based smart safety devices for women," in *Proceedings - International Conference on Augmented Intelligence and Sustainable Systems, ICAISS 2022*, IEEE, Nov. 2022, pp. 1101–1109, doi: 10.1109/ICAISS55157.2022.10010784.
- [14] R. J. Ananadh, S. A. Shet, A. S. Sivani, V. I. Priya, and T. Deepa, "Survey on IoT based device for women safety," in *2nd International Conference on Sustainable Computing and Data Communication Systems, ICSCDS 2023 - Proceedings*, IEEE, Mar. 2023, pp. 1608–1612, doi: 10.1109/ICSCDS56580.2023.10105029.
- [15] Z. Ali, M. A. Khan, O. Bin Samin, M. Mansoor, and M. Omar, "IoT based smart gloves for women safety," in *4th International Conference on Innovative Computing, ICIC 2021*, IEEE, Nov. 2021, pp. 1–6, doi: 10.1109/ICIC53490.2021.9693086.
- [16] Muskan, T. Khandelwal, M. Khandelwal, and P. S. Pandey, "Women safety device designed using IoT and machine learning," in *Proceedings - 2018 IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People and Smart City Innovations, SmartWorld/UIC/ATC/ScalCom/CBDCoM/IoP/SCI 2018*, IEEE, Oct. 2018, pp. 1204–1210, doi: 10.1109/SmartWorld.2018.00210.
- [17] P. S. Sowmika, S. S. N. Rao, and S. Rafi, "Machine learning framework for women safety prediction using decision tree," in *Proceedings - 5th International Conference on Smart Systems and Inventive Technology, ICSSIT 2023*, IEEE, Jan. 2023, pp. 1089–1093, doi: 10.1109/ICSSIT55814.2023.10060997.
- [18] R. Nasare, "Women security safety system using artificial intelligence," *International Journal for Research in Applied Science and Engineering Technology*, vol. 8, no. 2, pp. 579–590, Feb. 2020, doi: 10.22214/ijras.2020.2088.
- [19] V. Manikandan and M. Sivaram, "Improving the power efficiency in WSN using advanced multi-hop protocol," *International Journal of Engineering and Advanced Technology*, vol. 9, no. 1, pp. 791–794, 2019, doi: 10.35940/ijeat.A1393.109119.
- [20] D. Fernández-Llaneza, S. Ulander, D. Gogishvili, E. Nittinger, H. Zhao, and C. Tyrchan, "Siamese recurrent neural network with a self-attention mechanism for bioactivity prediction," *ACS Omega*, vol. 6, no. 16, pp. 11086–11094, Apr. 2021, doi: 10.1021/acsomega.1c01266.
- [21] Z. Guo, Y. Wang, L. Liu, S. Sun, B. Feng, and X. Zhao, "Siamese network-based few-shot learning for classification of human peripheral blood leukocyte," in *2021 IEEE 4th International Conference on Electronic Information and Communication Technology, ICEICT 2021*, IEEE, Aug. 2021, pp. 818–822, doi: 10.1109/ICEICT53123.2021.9531084.
- [22] T. Müller, G. Pérez-Torró, and M. Franco-Salvador, "Few-shot learning with siamese networks and label tuning," in *Proceedings of the Annual Meeting of the Association for Computational Linguistics*, Stroudsburg, PA, USA: Association for Computational Linguistics, 2022, pp. 8532–8545, doi: 10.18653/v1/2022.acl-long.584.
- [23] K. M. K. Raghunath, "IoT wearables dataset for women's safety: stress detection and analysis," 2023, doi: 10.21227/z04p-r549.

- [24] L. F. S. Scabini and O. M. Bruno, "Structure and performance of fully connected neural networks: emerging complex network properties," *Physica A: Statistical Mechanics and its Applications*, vol. 615, p. 128585, Apr. 2023, doi: 10.1016/j.physa.2023.128585.
- [25] C. Cassisi, P. Montalto, M. Aliotta, A. Cannata, and A. Pulvirenti, "Similarity measures and dimensionality reduction techniques for time series data mining," in *Advances in Data Mining Knowledge Discovery and Applications*, InTech, 2012, doi: 10.5772/49941.
- [26] V. Manikandan, M. Sivaram, A. S. Mohammed, V. Porkodi, and K. Shankar, "Secure localization based authentication (SLA) strategy for data integrity in WNS," *Computers, Materials and Continua*, vol. 67, no. 3, pp. 4005–4018, 2021, doi: 10.32604/cmc.2021.014643.

BIOGRAPHIES OF AUTHORS



P. Divya    P. Divya is a research scholar who completed her M.E. (CSE) at Selvam College of Technology, Namakkal, Tamil Nadu, India. She is currently working as an assistant professor in the Department of Computer Science, ACS College of Engineering, Bangalore-74, India. At present, she is pursuing his Ph.D. in the Department of Computer Science under the guidance of Dr. M. Kumaresan., associate professor, Department of Computer Science, Deemed-to-be University, Bengaluru-562112, Karnataka, India. She can be contacted at email: divyapoomalai@gmail.com.



Dr. M. Kumaresan    is an associate professor in Department of Computer Science and Engineering (IoT) at Jain Deemed-to-be University. He obtained master's degree and Ph.D. in Computer Science and Engineering from Anna University. His research focuses on the field of cloud computing, IoT, big data, and networks. He has published several Papers in reputed National and International Journals. He is a member of IAENG and ICSES, contributing to professional networking and knowledge sharing. He can be contacted at email: m.kumaresan@jainuniversity.ac.in.



Dr P. Manikandan    is a professor in the Department of Computer Science and Engineering (Data Science) at Jain Deemed-to-be University. He obtained Master's Degree in Computer Science and Engineering from Anna University, Chennai, India in 2008, and a Ph.D. degree from the same institution in 2016. He has 2 years of industrial experience prior to joining academia and embarked on his teaching career in 2001. His research interests encompass a wide range of cutting-edge areas, including machine learning, data mining, health informatics, cloud computing, the IoT, big data, and data science. He has authored and co-authored more than 25 articles in journals, conference proceedings, and book reviews. He can be contacted at email: p.manikandan@jainuniversity.ac.in.