Wireless Personal Communications
https://doi.org/10.1007/s11277-024-11429-0

Smart Security Solution for Women and Children Using Wearable IOT Systems

Nanda R. Wagh[1] · **Sanjay R. Sutar**[2] · **Anant S. Yadav**[3]

Accepted: 19 June 2024

Abstract
In recent years, the rapid advancement of technology has paved the way for innovative solutions aimed at enhancing personal safety and security. Among these, wearable Internet of Things (IoT) devices have emerged as a significant development, particularly in safeguarding vulnerable groups such as women and children. This paper introduces a smart security solution that leverages wearable IoT systems to provide real-time monitoring and protection. The increasing incidence of crimes against women and children highlights the urgent need for effective safety measures. Traditional security approaches often fall short in offering immediate assistance or preventive measures. However, wearable IoT devices, equipped with sensors and connectivity features, offer a proactive approach to security. These devices can monitor various physiological and environmental parameters, detect potential threats, and trigger timely alerts to guardians or authorities Our proposed smart security solution integrates advanced IoT technologies with user-friendly wearable devices designed specifically for women and children. This system encompasses several critical components, including GPS tracking, real-time communication, health monitoring, and emergency alert mechanisms. By harnessing the power of IoT, this solution aims to provide continuous protection, enhance situational awareness, and facilitate rapid response in case of emergencies. In this paper, we will explore the design, functionality, and potential impact of wearable IoT devices in improving the safety and security of women and children. We will also discuss the challenges and considerations in implementing such systems, including privacy concerns, data security, and the need for reliable connectivity. Through this comprehensive examination, we aim to demonstrate the viability and importance of IoT-based wearable technology in fostering a safer environment for vulnerable populations.

Keywords Smart security · Women's safety · Children's safety · Wearable IoT devices · Real-time GPS tracking · Emergency response · Heart rate monitoring · Evidence collection · Safety monitoring · Personal safety devices · IoT-based security solutions · Wearable technology

Extended author information available on the last page of the article

Published online: 12 September 2024

1 Introduction

The increasing concern for the safety of women and children in both urban and rural environments necessitate innovative and effective security solutions. With advancements in technology, especially the IoT, there is an unprecedented opportunity to enhance personal security through smart, wearable devices. These devices, integrated with IoT systems, offer real-time monitoring, emergency response capabilities, and comprehensive safety features designed to protect vulnerable populations. Smart Security Solutions for women and children using wearable IoT systems represent a significant leap forward in personal safety. These devices are equipped with a range of sensors and communication technologies, including GPS, accelerometers, and biometric sensors, which can detect distress signals and unusual movements. By connecting to a centralized monitoring system, these wearables can alert authorities, family members, or guardians in case of an emergency, ensuring a swift and appropriate response. However the increasing concern for the safety of women and children necessitates the development of innovative security solutions. This paper proposes a smart security system utilizing wearable Internet of Things (IoT) devices designed specifically for women and children. These wearable devices, such as smartwatches, smart jewelry, and smart clothing, are embedded with advanced sensors and communication technologies. Key features include real-time GPS tracking, accelerometers for detecting sudden movements, heart rate monitors, and integrated microphones and cameras for evidence collection and two-way communication. The system leverages connectivity options like Bluetooth, Wi-Fi, and cellular networks to ensure continuous monitoring and immediate response during emergencies. By integrating these technologies, the proposed solution aims to provide a reliable, real-time safety net that can alert guardians or authorities, share precise location data, and record crucial evidence, thereby enhancing the overall security for vulnerable populations. The effectiveness of this solution lies in its ability to provide seamless, proactive, and reactive measures to safeguard women and children in various scenarios.

Moreover, wearable IoT devices provide a discreet and convenient means of maintaining security without impeding daily activities. They can be integrated into everyday items such as watches, bracelets, or pendants, making them an unobtrusive yet powerful tool for safeguarding individuals. This integration not only helps in continuous tracking and monitoring but also empowers users with a sense of security and confidence as they go about their daily lives. In this paper, we explore the design, functionality, and impact of wearable IoT systems tailored specifically for enhancing the safety of women and children. We will examine the technological components, system architecture, and practical applications of these devices. Additionally, we will discuss the broader societal implications and the potential for these technologies to foster a safer and more secure environment for at-risk populations. Through a comprehensive analysis, we aim to highlight the transformative potential of wearable IoT security solutions and their role in building a safer future.

2 Review of Literature

The integration of wearable IoT devices into security solutions for women and children is a burgeoning field of research, combining advances in wearable technology, IoT, and safety applications. This literature survey reviews the current state of knowledge and technological

advancements in this domain, highlighting key studies and developments. The literature on smart security solutions for women and children using wearable IoT systems spans multiple fields, including IoT technology, wearable devices, personal safety, and emergency response systems. This survey aims to provide a comprehensive overview of the key developments, existing solutions, and research advancements in this domain.

2.1 Wearable Technology and IoT in Personal Safety

Wearable technology has seen significant growth, driven by advancements in miniaturization, sensor technology, and wireless communication. Research by [1] highlighted the potential of wearable devices in health monitoring, noting that these technologies can be adapted for personal safety applications. The incorporation of IoT further enhances these capabilities, allowing for real-time data transmission and analysis [2]. Wearable IoT devices have gained significant traction due to their portability and advanced functionalities. These devices typically integrate various sensors, communication modules, and power-efficient components to monitor and transmit data. Studies by [3, 4] highlight the evolution of wearable health monitors, focusing on their applications in continuous health tracking and emergency detection. These foundational works demonstrate the potential of wearables to extend beyond health monitoring into broader safety applications.

2.2 Wearable Devices for Women's Safety

Many studies have explored wearable devices designed specifically for women's safety. Numerous technologies developed a wearable device equipped with GPS and GSM modules, capable of sending emergency alerts with location information. Similarly, a study by [5] introduced a smart bracelet that integrates an SOS button and real-time tracking features, demonstrating significant potential in improving personal security for women. The use of wearables for personal safety has been explored extensively. For example, [6] reviewed various wearable devices designed to enhance personal security, including panic buttons, GPS trackers, and communication tools. Their work underscores the critical need for reliable and discreet security solutions, particularly for vulnerable groups. Similarly, a study by [7] analyzed the effectiveness of wearable devices in emergency situations, finding that rapid alert systems integrated with wearables can significantly reduce response times.

2.3 Child Safety Solutions Using Wearable Technology

For children, wearable IoT devices have been investigated primarily for tracking and monitoring purposes. The work of [8] introduced a wearable device for children that uses GPS and GSM technologies to provide real-time location updates to parents. Another notable study by [9] proposed a multi-functional wearable device for children, incorporating features such as geofencing, health monitoring, and emergency alerts. Women's safety has been the focus of several innovative wearable technologies. A notable example is the work by [10], which explores wearable devices designed to send alerts and location data to emergency contacts when a potential threat is detected. Additionally, research by [11] on wearable panic devices shows the effectiveness of these gadgets in empowering women to discreetly call for help during emergencies.

2.4 Biometric Monitoring and Advanced Sensing

Advanced sensing capabilities, including biometric monitoring, are critical for enhancing the functionality of wearable security devices. Research by [12] explored non-invasive biometric sensors for continuous monitoring of physiological parameters, which can detect signs of stress or distress. Similarly, [13] demonstrated how wearable devices could utilize heart rate variability and skin conductance to assess the wearer's emotional state, providing an additional layer of safety. Research by [14] on emergency response frameworks highlights the importance of real-time data transmission and analysis in improving response efficiency. Their work suggests that integrating IoT-enabled wearables with centralized monitoring systems can enhance situational awareness and facilitate quicker interventions. Another study by [15] demonstrated how IoT-based solutions could be used to create automated emergency response protocols, further improving the reliability and effectiveness of these systems.

2.5 Integration and Connectivity in IoT Systems

The seamless integration of wearable devices into a cohesive IoT system is crucial for effective real-time monitoring and response. The [16] reviewed the architecture of IoT systems, emphasizing the importance of interoperability, data security, and scalability. Their findings underline the need for robust communication protocols and secure data handling practices in wearable IoT applications. Specific research focused on children's safety, such as the study by [17], explores various wearable solutions tailored for children, including smartwatches and wristbands equipped with GPS and communication features. These devices not only help in tracking the location of children but also enable parents to set geofencing alerts to notify them if their child exits a predefined safe zone. Another notable study by [18] discusses the integration of biometric sensors in children's wearables to monitor vital signs and detect unusual patterns that might indicate distress.

2.6 User-Centric Design and Usability

Ensuring that wearable security devices are user-friendly and unobtrusive is essential for widespread adoption. A study by [19] on wearable design principles highlighted the importance of ergonomics and user comfort. Subsequent research by [20] reinforced these principles, showing that the effectiveness of wearable devices is significantly influenced by their design and usability. The integration of wearables with IoT platforms is critical for creating cohesive security systems. Studies like those by [21] emphasize the need for interoperability between different devices and systems to ensure seamless data flow and coordination. Moreover, future directions in this field, as discussed by [22], point towards the use of artificial intelligence (AI) and machine learning (ML) to analyze data from wearables in real time, predicting and preventing potential threats before they escalate.

2.7 Case Studies and Practical Implementations

Several real-world implementations provide valuable insights into the practical challenges and successes of wearable IoT security solutions. The Nirbhaya case in India prompted

numerous technological innovations aimed at women's safety, including smart wearables that have been piloted in various urban settings [23]. Additionally, pilot projects in schools have tested wearable devices for child safety, demonstrating their effectiveness in providing real-time tracking and emergency response [24, 25].

There are two ways of computing namely heterogeneous distributed computing systems and homogenous distributed computing systems approaches are used in design of distributed systems. In addition to server heterogeneity, depending on the basic applications, outstanding burden spreading over numerous cloud clients may require tremendously unique measure of resources (CPU, memory and capacity) [26] Neuro-fuzzy systems are widely used today to model various real-life problems. They have gained popularity among the scientific society because they efficiently combine the advantages of fuzzy logic and artificial neural networks. The fuzzy logic component takes care of the learning abilities, while the artificial neural network component takes the feature interpretation from fuzzy logic [27]. Wireless sensor networks represent one of the most crucial components of novel technologies, such as the internet of things and cloud computing [28]. Big Data combines large-scale computing with machine learning techniques to build predictive analytics for intrinsic information extraction [29]. In wireless sensor network (WSN), user authentication plays as a vital role in which data sensing, as well as sharing, will be spoiled by hackers. To enhance user security, user authentication must be focused [30].

The literature highlights the significant advancements and ongoing research in the field of wearable IoT systems for enhancing the safety of women and children. These studies collectively underscore the potential of integrating wearable technology with IoT to create effective, reliable, and user-friendly security solutions. Future research and development efforts should focus on enhancing the functionality, interoperability, and intelligence of these systems to ensure they can provide comprehensive protection in a wide range of scenarios.

3 Proposed System Design

The architecture used in this study for the Internet of Things (IoT) is as follows: The data collection process begins with sensors, namely a pulse sensor and a temperature sensor. These sensors gather the necessary information, which is then sent to a microcontroller unit, such as an Arduino. The microcontroller unit then transmits the collected data to a gateway. The whole system for communication constitutes a mesh network. The gateway transmits the data to the cloud, where it undergoes analysis using machine learning algorithms. Once all the calculations are completed on the cloud, the accuracy is obtained, indicating whether or not the woman is in danger.

The smart security solution for women's and children's safety using wearable IoT systems comprises various modules, each serving specific functions to ensure comprehensive protection and support. The smart security solution is designed to enhance the safety of women and children through the use of advanced wearable IoT devices. These devices integrate various sensors, communication modules, and software to provide real-time monitoring, alerting, and response capabilities. The system aims to offer peace of mind by ensuring constant connectivity, immediate assistance in emergencies, and comprehensive monitoring of the wearer's environment and health.

Wearable Devices Module These are small, lightweight devices designed to be worn by women and children. They can be in the form of wristbands, necklaces, or clips. These devices contain sensors for tracking location, detecting falls, monitoring vital signs, and activating alerts.

User Interface Module The IoT User Interface Module plays a crucial role in facilitating interaction between users and the smart security solution through intuitive and accessible interfaces. It provides a graphical interface for users to interact with the system via mobile applications or web portals and it allows users to configure settings, view real-time data, and trigger emergency alerts.

Authentication and Authorization Module Manages user authentication to ensure secure access to the system and validates user credentials and assigns appropriate permissions based on user roles.

Sensor Data Acquisition Module Collects data from sensors embedded in wearable devices, including GPS, accelerometers, gyroscopes, heart rate monitors, microphones, and cameras.

Data Preprocessing Module Filters, cleans, and preprocesses raw sensor data to remove noise and extract relevant information and performs data normalization and feature extraction to prepare the data for further analysis (See Fig. 1).

Communication Module Facilitates communication between wearable devices, mobile applications, cloud servers, and emergency response systems and utilizes wireless technologies such as Bluetooth Low Energy (BLE), Wi-Fi, and cellular networks for data transmission.

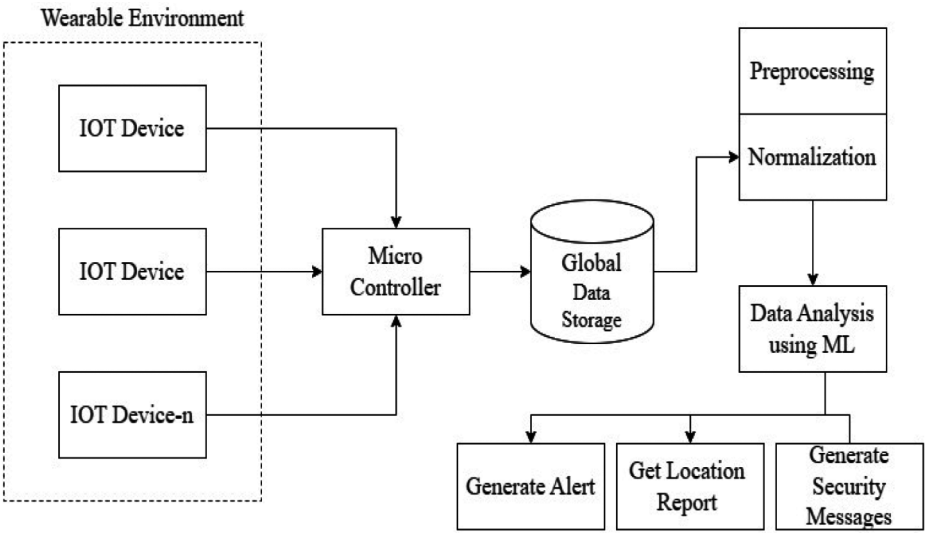

Fig. 1 Proposed system architecture for IoT based women and child security

Location Tracking Module Tracks the real-time location of wearable devices and users using GPS technology. It also implements geofencing capabilities to define virtual boundaries and trigger alerts when users enter or leave predefined areas.

Machine Learning and AI This module analyses sensor data to detect patterns or anomalies indicative of potential threats and improves the accuracy of fall detection and other safety features over time. It also provides personalized recommendations for enhancing safety based on usage patterns and environmental factors.

Emergency Alerting Module Monitors sensor data for signs of distress or emergency situations, such as sudden movements, abnormal heart rate patterns, or activated SOS buttons and generates and transmits emergency alerts to designated contacts, caregivers, or emergency response systems.

Emergency Response Coordination Module Coordinates emergency responses by contacting appropriate authorities (e.g., police, medical services) based on the nature and severity of the situation. and facilitates two-way communication between users in distress and emergency responders.

Data Storage and Management Module It stores sensor data, user profiles, system configurations, and historical records securely in a centralized database or cloud storage and implements data retention policies and ensures compliance with data protection regulations.

Security and Privacy Module this module provides end-to-end encryption to secure data transmission and storage and enforces user consent and privacy preferences regarding data sharing and usage. It also monitors system integrity and detects potential security threats or unauthorized access attempts.

By integrating these modules, the smart security solution aims to deliver a robust and scalable platform for enhancing the safety and well-being of women and children using wearable IoT systems. This smart security solution leverages the power of IoT to create a comprehensive and reliable system for safeguarding women and children, ensuring their safety and providing peace of mind to their loved ones.

4 Algorithm Design

In below algorithm Artificial Neural Network (ANN) and Support Vector Machine (SVM) utilized for analysis of structured data while Convolutional Neural Network (CNN) utilized for analysis of unstructured data.

1: Hybrid Machine Learning Algorithm (HML)

Input:

1. Input values for all parameters HashMap < Double Value, String class > which contains the all-attributes values such as {BP rates, Body Temperature, ECG data etc.} of training and testing data.

2. Set of Algorithms Algo-Names {ANN, SVM, CNN}

Output: predicted decision using above three combined machine learning classification algorithms.

Step 1 *for each all training data.*

$$Extracted\_Attribute\,[i]\,[j] \sum_{i=0,j=0}^{n} \left(a_{[i]}, a_{[j].....}a_{[n]}, a_{[n].}\right)$$

Step 2 *Generate instance for ANN as objANN.*

ANN_Rules[] $\leftarrow$ *objANN.Trainclassifier(*$Extracted_{Attribute[m][n]}$*)*

Step 3 *Generate instance for SVM as objSVM.*

SVM_Rules[] $\leftarrow$ *objSVM.Trainclassifier(*$Extracted_{Attribute[m][n]}$*)*

Step 4 *Generate instance for CNN as objCNN.*

CNN_Rules[] $\leftarrow$ *objCNN.Trainclassifier(*$Extracted\_Attribute\,[m]\,[n]$*)*

Step 5 *Add all training rules in single arraylist.*

Master_Training_List[] $\leftarrow$ *(DT_Rules[], PART_Rules[], J48_Rules[],)*
End for.

Step 6 *for each all testing data.*

$$Extracted\_Test\_Data\,[i]\,[j] \sum_{i=0,j=0}^{n} \left(a_{[i]}, a_{[j].....}a_{[n]}, a_{[n].}\right)$$

Step 7 *Apply all classifiers on test data using above training rules.*

Pred1[] $\leftarrow$ *ANN.Buildclassifier(*$Extracted_{Test_{Data[m][n]}}$*, Master_Training_List[])*
Pred2[] $\leftarrow$ *SVM.Buildclassifier(*$Extracted_{Test_{Data[m][n]}}$*, Master_Training_List[])*
Pred3[] $\leftarrow$ *CNN.Buildclassifier(*$Extracted_{Test_{Data[m][n]}}$*, Master_Training_List[])*

Step 8 *C_Matrix[]* $\leftarrow$ *Calc_Accuracy(Pred1[], Pred2[], Pred3[])*

Step 9 *Review C_Matrix[].*

5 Results and Discussions

This method will use the pulse rate and temperature of a woman to forecast if she is at risk or not. If she is in danger, the system will immediately initiate calls to the appropriate contacts. We devised a concept to minimize human engagement with mobile devices. The article used the Logistic Regression machine learning approach for the prediction aspect. The machine learning technique will extract characteristics such as pulse rate and temperature from an Excel sheet that is directly connected to an Arduino. To transfer parameters from Arduino to Excel, the researchers used Java software. The algorithm will execute calculations and provide plots for both the training and testing datasets.

In order to determine the effectiveness of the proposed approach, a number of investigations covering a wide range of topics were carried out. The data that is stored in the health care sector is extremely delicate, and as a result, the department requires a specialized system that is able to safeguard the data that is stored in the global dataset network. A number of different machines learning algorithms, including NB, RF, Adaboost, ANN, DT, and SVM, were evaluated alongside the HML Algorithm that was proposed.

After examining each of these methods side by side, the necessary components were chosen from among them. The data set has been divided up into two parts with a 70:30 split between them. The first 70% were assigned toward training, while the remaining 30% were used for testing.

From Table 1; Fig. 2, it is evident that the proposed hybrid machine learning algorithm used in this research is more accurate in predicting the disease than the machine learning (ML) Algorithms.

In another experiment, we use the real-time student dataset to demonstrate SVM (Sigmoid) classification accuracy. Figure 3 illustrates the outcomes of similar trials using various cross-validation techniques. According to the findings, 15-fold cross-validation has the highest average classification accuracy of 95.10%. The 5-fold cross validation also achieves 93.6% with SVM with sigmoid function. While Fig. 3 describes with 10-fold data cross validation. Both functions achieve around similar accuracy during module testing.

Figure 4 displays SVM classification accuracy using the Cleveland dataset; similar tests were carried out with different cross validation and the results are shown in below Fig. 4. According to our findings, 15-fold cross validation delivers the greatest average classification accuracy of 93.55% and 94.90% for SVM utilizing Tanh.

In this experiment, we examined ReLU's classification accuracy using a real-time dataset; comparable tests were conducted using varied cross validation, and the results are shown in Fig. 5. According to this study, 10-fold cross validation classification accuracy for SVMs is 95.30% and 97.10%, respectively. The Fig. 5 carried out 5-fold, 10-fold and 15-fold cross validation training of SVM (Tan h activation function).

Table 1 Comparative analysis of proposed algorithm with conventional ML

Classification Methods	Accuracy	Precision	Recall	F-Measure
HML	0.93	0.95	0.96	0.97
NB	0.80	0.85	0.91	0.89
RF	0.89	0.90	0.93	0.94
ADABOOST	0.91	0.93	0.94	0.95
ANN	0.90	0.92	0.93	0.94
DT	0.89	0.91	0.92	0.93
SVM	0.92	0.94	0.95	0.97

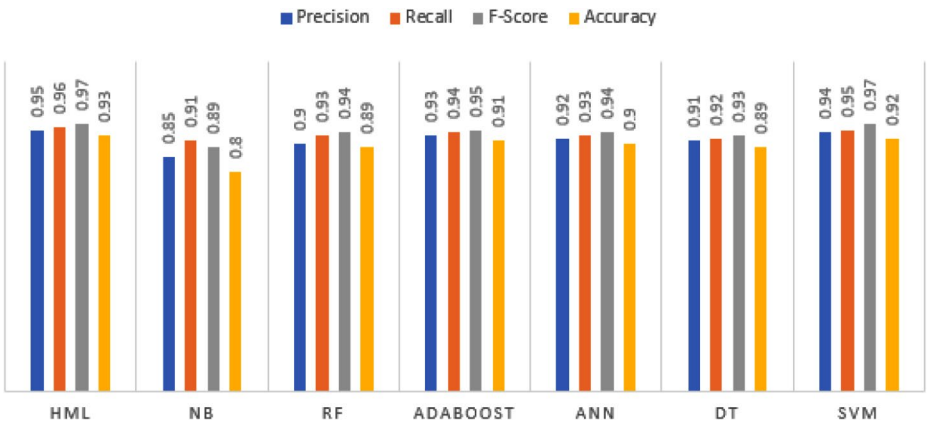

Fig. 2 Comparative analysis of proposed HML with traditional ML

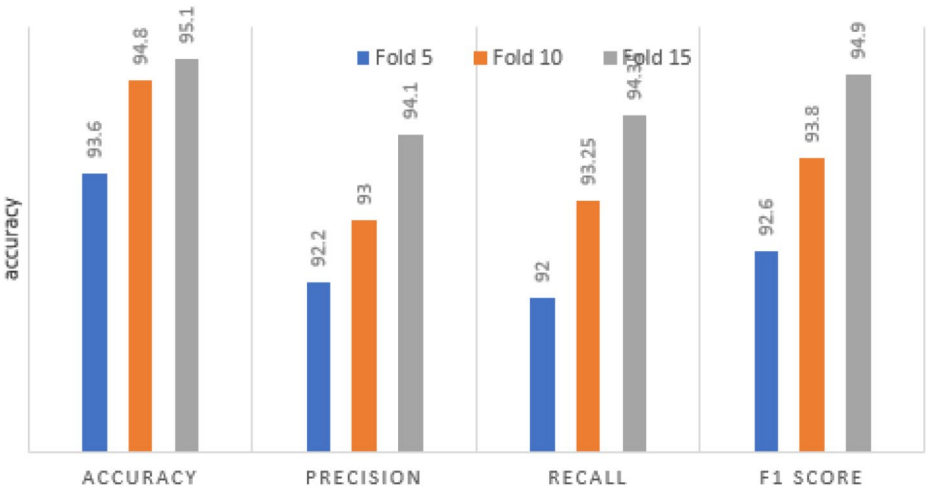

Fig. 3 System validation with various cross validation using SVM (sigmoid)

A proposed deep learning classification method utilizing a machine learning algorithm is shown in Fig. 5. The outcome of several cross-validation is shown in this diagram. For student performance prediction, we employed a minimum of three hidden layers. We infer that SVM with sigmoid delivers superior detection accuracy than the other three activation functions based on this experiment.

6 Conclusion

In an era where personal safety remains a pressing concern, particularly for vulnerable groups such as women and children, the integration of advanced technology into everyday life presents promising solutions. Smart security systems, enhanced by the IoT, offer

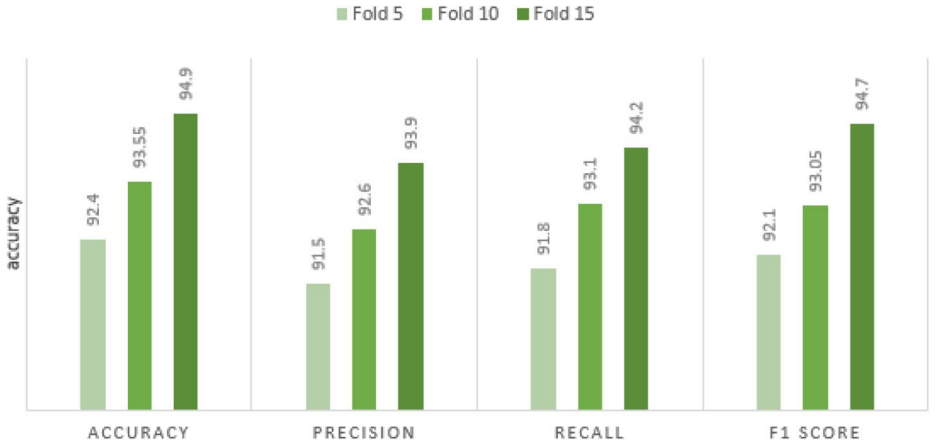

Fig. 4 System validation with various cross validation using SVM (Tanh)

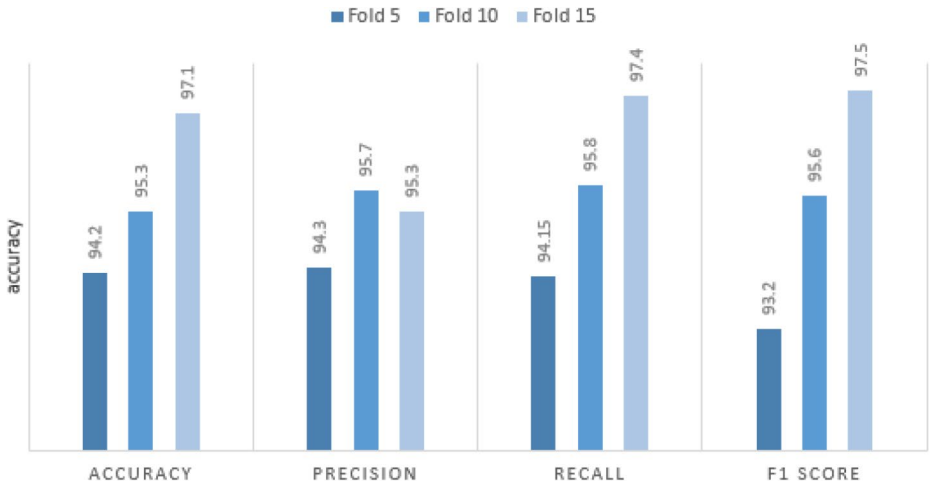

Fig. 5 System validation with various cross validation using SVM (ReLU)

innovative and effective ways to address these concerns. This paper introduces a comprehensive smart security solution specifically designed for women and children, leveraging wearable IoT devices to provide real-time monitoring, immediate response capabilities, and enhanced situational awareness. Wearable IoT devices are small, portable gadgets embedded with sensors and communication technologies that can be worn on the body. These devices are capable of collecting and transmitting data, enabling continuous monitoring of the wearer's environment and physiological status. By integrating these wearables into a cohesive security system, it becomes possible to offer a robust safety net that is proactive, reliable, and user-friendly. The proposed smart security solution encompasses various functionalities, including location tracking, emergency alerts, and biometric monitoring. These features work in tandem to ensure the wearer's safety in multiple scenarios, from everyday commuting to more perilous situations. For instance, location tracking allows for the pre-

cise pinpointing of an individual's position, which is crucial in emergencies. Emergency alerts can be automatically or manually triggered to notify authorities or predetermined contacts, ensuring swift response in critical situations. Biometric monitoring adds an extra layer of security by detecting physiological changes that may indicate distress. Moreover, the integration of IoT allows for seamless connectivity between the wearable devices and a central monitoring system. This connectivity ensures that data is continuously updated and analysed, enabling real-time decision-making and quick intervention when necessary. The system's design prioritizes user-friendliness and unobtrusiveness, ensuring that it does not interfere with the daily activities of the wearers while still providing a constant safety net. In conclusion, the development and deployment of a smart security solution utilizing wearable IoT devices represent a significant advancement in personal safety for women and children. By harnessing the power of modern technology, this solution offers a practical, efficient, and scalable way to enhance security and peace of mind for these vulnerable populations.

Author Contributions Nanda R. Wagh performed the conceptualization, methodology, data collection and writing the study. Sanjay R. Sutar worked as supervisor of this manuscript and performed analysis of the dataset and conceptualization in the study. Anant S. Yadav performed analysis of the dataset and revision of manuscript.

Funding No fund received for this project.

Data Availability Not Applicable.

Declarations

Conflict of Interest The authors declare that they have no conflict of interest.

References

1. Zheng, Y. L., Ding, X. R., Poon, C. C., Lo, B. P., Zhang, H., Zhou, X. L., Yang, G. Z., Zhao, N., & Zhang, Y. T. (2014). Unobtrusive sensing and wearable devices for health informatics. *IEEE Transactions on Biomedical Engineering*, *61*(5), 1538–1554.
2. Patel, V., Orchanian-Cheff, A., & Wu, R. (2021). Evaluating the validity and utility of wearable technology for continuously monitoring patients in a hospital setting: Systematic review. *JMIR mHealth and uHealth*, *9*(8), e17411.
3. Sharma, A., Badea, M., Tiwari, S., Marty, J. L. (2021). Wearable biosensors: an alternative and practical approach in healthcare and disease monitoring. *Molecules, 26*(3), 748.
4. Khan, A., Gupta, S., & Gupta, S. K. (2022). Emerging UAV technology for disaster detection, mitigation, response, and preparedness. *Journal of Field Robotics*, *39*(6), 905–955.
5. Smith, M., Chambers, T., Abbott, M., & Signal, L. (2020). High stakes: Children's exposure to gambling and gambling marketing using wearable cameras. *International Journal of Mental Health and Addiction*, *18*, 1025–1047.
6. Kohli, P., Singh, K., & Sidhu, B. K. (2024). Design of Real Time Intelligent System for Women Safety. *Recent Patents on Engineering*, *18*(3), 77–83.
7. Lee, U., Han, K., Cho, H., Chung, K. M., Hong, H., Lee, S. J., Noh, Y., Park, S., & Carroll, J. M. (2019). Intelligent positive computing with mobile, wearable, and IoT devices: Literature review and research directions. *Ad Hoc Networks*, *83*, 8–24.
8. Ahmed, A., Aziz, S., Alzubaidi, M., Schneider, J., Irshaidat, S., Serhan, H. A., Abd-Alrazaq, A. A., Solaiman, B., & Househ, M. (2023). Wearable devices for anxiety & depression: A scoping review. *Computer Methods and Programs in Biomedicine Update*, *3*, 100095.
9. Patel, S., Park, H., Bonato, P., Chan, L., & Rodgers, M. (2012). A review of wearable sensors and systems with application in rehabilitation. *Journal of Neuroengineering and Rehabilitation*, *9*, 1–7.

10. Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the internet of things. Cluster of European research projects on the internet of things. *European Commision*, *3*(3), 34–36.
11. Xu, S., Zhang, Y., Jia, L., Mathewson, K. E., Jang, K. I., Kim, J., Fu, H., Huang, X., Chava, P., Wang, R., & Bhole, S. (2014). Soft microfluidic assemblies of sensors, circuits, and radios for the skin. *Science*, *344*(6179), 70–74.
12. Mohanty, B. K., & Patel, S. K. (2014). Area–delay–power efficient carry-select adder. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *61*(6), 418–422.
13. AnandJatti, M. K., Alisha, R. M., Vijayalakshmi, P., & ShresthaSinha Design and Development of an IOT based wearable device for the Safety and Security of women and girl children, *IEEE International Conference on Recent Trends in Electronics Information Communication Technology*, May 20–21, 2016.
14. Hyndavi, V., Sai Nikhita, N., & Rakesh, S. (2020). Smart Wearable Device for Women Safety Using IoT, *International Conference on Communication and Electronics Systems*.
15. Karmakar, S., & Rana, T. K. (2020). Smart Bag for Women Safety. In *International Conference on Electronics, Materials Engineering &NanoTechnology*.
16. Zully Amairany Montiel Fernandez et al. (2020). Challenges of Smart Cities: How Smartphone Apps Can Improve the Safety of Women. In *International Conference on Smart Grid and Smart Cities*.
17. Monisha, D. G., Monisha, M., Pavithra, G., & Subhashini, R. (2016). Women safety device and application-FEMME. *Indian Journal of Science and Technology*. https://doi.org/10.17485/ijst/2016/v9i10/88898
18. Lee, CC. (2020). Security and Privacy inWireless Sensor Networks: Advances and Challenges. *Sensors (Basel), 20*(3), 744. https://doi.org/10.3390/s20030744
19. Akram, W., Jain, M., & Sweetlin Hemalatha, C. (2019). ICRTAC, Design of a Smart Safety Device for Women using IoT. *Procedia Computer Science, 165*, 656–662. https://doi.org/10.1016/j.procs.2020.01.060
20. Hyndavi, V., Sai Nikhita, N., & Rakesh, S. (2020). Smart Wearable Device for Women Safety Using IoT. In *International Conference on Communication and Electronics Systems (ICCES)*.
21. B.Aarthy, M., Abirami, R., & Mangai, L. K. (2020). and M.Gengara, Enhancement of Women Safety using raspberry pi. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*.
22. Bhuvaneshwari, Mehtre (2019). A raspberry Pi-based Safety System for Women Security using IoT. *International Journal of Science and Research (IJSR)*.
23. Maheswaran Shanmugam, S., Nehru, & Shanmugam, S. (2018). A wearable embedded device for chronic low back patients to track lumbar spine position. *Biomedical Research 2018*, S118–S123.
24. Maheswaran, S., Kuppusamy, P. G., Ramesh, S. M., Sundararajand, T. V. P., & Yupapin, P. (2018). Refractive index sensor using dual core photonic crystal fiber– glucose detection applications. *Results in Physics, 11*, 577–578. https://doi.org/10.1016/j.rinp.2018.09.055
25. Banerjee, A., & Nayaka, R. R. (2022). A comprehensive overview on BIM-integrated cyber physical system architectures and practices in the architecture, engineering and construction industry. *Construction Innovation*, *22*(4), 727–748.
26. Lavanya, S., Susila, N., & Venkatachalam, K. (2019). *Impact of Cloud of clouds in enterprises applications. Novel practices and trends in Grid and Cloud Computing* (pp. 21–33). IGI Global.
27. Zivkovic, M., Bacanin, N., Venkatachalam, K., Nayyar, A., Djordjevic, A., Strumberger, I., & Al-Turjman, F. (2021). COVID19 cases prediction by using hybrid machine learning and beetle antennae search approach. *Sustainable Cities and Society, 66*.
28. Zivkovic, M., Zivkovic, T., Venkatachalam, K., & Bacanin, N. (2021). Enhanced Dragonfly Algorithm Adapted for Wireless Sensor Network Lifetime Optimization, In *Data Intelligence and Cognitive Informatics*, pp. 803–817.
29. Subramaniyan, S., Regan, R., Perumal, T., & Venkatachalam, K. (2020). Semi-supervised Machine Learning Algorithm for Predicting Diabetes using big DataAnalytics. In A. Haldorai, A. Ramu, & S. Khan (Eds.), *Business Intelligence for Enterprise Internet of things. EAI/Springer Innovations in Communication and Computing*. Springer.
30. Prabu, P., & Senthilnathan, T. (2020). Secured and flexible user authentication protocol for wireless sensor network. *International Journal of Intelligent Unmanned Systems, 8*(4), 2787–2793.

Nanda R. Wagh completed the master's in Computer Science and Engineering from MGM College of Engineering, Shree Ramanand Tirth Marathwada University Nanded, MS, India in 2009. Since then, she has worked as Assistant Professor in the Department of Computer Engineering/IT at MIT, Alandi at Savitribai Phule Pune University where her research interests include facial recognition, human-computer interaction, multisensory data fusion, multimodal emotion recognition, and women's and children safety. She has written a book on Artificial Intelligence for Anna University. She is inventor of patent. She is currently working as Lecturer in Computer Engineering Department, Government Polytechnic Pune under the Department of Technical Education, Mumbai. She is working as research scholar at Information Technology, DBATU, Lonere.

Dr. Sanjay R. Sutar received Ph.D from Shree Ramanand Tirth Marathwada University Nanded, MS, India. He completed the master's in Computer Science and Engineering from DBATU, Lonere and B.Tech from Walchand College of Engineering, Sangali. Since then, he has been working as Professor and Head in the Department of Information Technology at Dr. Babasaheb Ambedkar Technological University, Lonere, MS, India where his research interests include scheduling, genetic and Evolutionary Algorithm.

Anant S. Yadav pursuing his BE (Computer Engineering) from Sinhgad Academy of Engineering Savitribai Phule Pune University, MS, India. He completed school education from Priyadarshini Education Society and Junior college education from Wadia College Pune. His research interests include machine learning and cyber security. He has completed online machine learning certification.

Authors and Affiliations

Nanda R. Wagh[1] · Sanjay R. Sutar[2] · Anant S. Yadav[3]

✉ Nanda R. Wagh
nandawagh@dbatu.ac.in

Sanjay R. Sutar
srsutar@dbatu.ac.in

Anant S. Yadav
anantswara06@gmail.com

[1] Research Scholar, Department of Information Technology, Dr. Babasaheb Ambedakar Technological University, Lonere, Maharashtra, India

[2] Professor, Department of Information Technology, Dr. Babasaheb Ambedakar Technological University, Lonere, Maharashtra, India

[3] B. E. Student, Sinhgad Academy of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India