RESEARCH PAPER

AI-Assisted Wearable Devices for Women's Safety with Real-Time Threat and Anomaly Identification

Dhamdhere Shubhangi Tulshidas[1], Dr. Sivaram Ponnusamy[2]
[1]Department of Computer Science and Engineering, Sandip University, Nashik, Maharashtra, India – 422213
Email: shubhangi28587@gmail.com
ORCID: 0009-0006-0289-3991
[2]Department of Computer Science and Engineering, Sandip University, Nashik, Maharashtra, India – 422213
Email: P.sivaram@sandipuniversity.edu.in
ORCID: 0000-0001-5746-0268

Received: 15th Jul, 2026 | Revised: 25th Jul, 2026 | Accepted: 5th Aug, 2026 | Available Online: 12th Aug, 2026

ABSTRACT

Recently, harassment, assault, stalking, and other forms of violence in both public and private settings have become a social and technological issue of great concern to women's safety. Traditional safety measures like location-tracking, panic buttons and emergency mobile applications are typically reactive and only respond to a threat after it has happened. The latest innovations in the field of wearable technology, artificial intelligence, machine learning, computer vision and sensor integration have presented new possibilities for the creation of proactive safety systems which can detect dangers before they become a dangerous situation. The current research suggests the idea of smart sunglasses that will be equipped with a wearable device to be used and operated by women for monitoring, detecting threats and identifying anomalies in real time. The system proposed for this work incorporates a number of sensing technologies such as GPS, GSM, physiological sensors, accelerometers, cameras, and environmental monitoring modules. The data collected is analysed with the help of deep learning and machine learning algorithms to detect suspicious and unusual activities, patterns of behaviour, environmental hazards, and emergencies.

The wearable device uses the You Only Look Once version 8 (YOLOv8) object detection framework to detect potentially dangerous objects and people around the wearer in real time. At the same time, behavioural analysis models analyse the user's movement patterns, physiological responses and contextual environmental data to detect anomalies that could signal distress or danger. If a potential threat is identified the system automatically alerts and provides location data to pre-programmed emergency contacts and authorities. A series of simulated urban environments and controlled testing scenarios that incorporated multiple threat categories were employed to test a prototype evaluation. The results of the experiment showed that the object detection rate was 96.8%, anomaly detection rate was 94.2%, and the emergency response notification success rate was 98.5%. The findings suggest that AI-driven wearable devices have the potential to be a powerful tool for improving personal safety by enabling proactive monitoring and intelligent threat assessment. The study advances wearable safety technologies and provides the basis for future research on the intelligent protective systems for vulnerable people.

Keywords: Women safety, Wearable devices, Artificial Intelligence, Anomaly detection, Threat identification, YOLOv8, Machine Learning, Deep Learning, Smart Sunglasses, Real-time monitoring.

How to cite this article: Tulshidas DS, Ponnusamy S., AI-Assisted Wearable Devices for Women's Safety with Real-Time Threat and Anomaly Identification. Int J Drug Deliv Technol. 2026;16(76s): 330; DOI: 10.25258/ijddt.16.76s.31

1. Introduction

1.1 Background of the Study

Security and protection of women is one of the most crucial issues in every society. Although there have been improvements in legislation and in law enforcement, the number of cases of harassment, assault, stalking, kidnapping and violence against women has risen in both urban and rural areas, and even with the improvements in public awareness-raising and digital safety, there remains a lack of understanding. Even with improvements in legislation, law enforcement, public awareness-raising and digital safety, the number of cases of harassment, assault, stalking, kidnapping and violence against women has been on the rise in both urban and rural areas, and understanding is lacking (Gupta *et al.*, 2026). With the unprecedented increase of urbanization, population density, and mobility, ensuring personal security has become more complex, especially for women, who often travel alone for educational, professional, and social purposes.

Traditional safety mechanisms are mostly manually operated. These mobile apps may need to be enabled when facing a critical situation, and location-based systems are typically only used to report information after an event, but they are not used proactively to prevent threats. These methods can be ineffective if people are physically restrained, psychologically distressed or don't have communication devices in emergencies. As such, the need for intelligent safety systems with autonomous operation and threat identification is growing.

Over the last few years, the use of wearable technology has revolutionized personal monitoring. Smart watches, fitness trackers, smart glasses and sensor-integrated garments can monitor physiological and environmental parameters continuously. These wearable devices can be integrated with AI technologies to enable context-aware decision making and predictive safety interventions (Dharshana *et al.*, 2026). The synergy of machine learning, computer vision, sensor fusion, and wireless communication opens the door to the creation of sophisticated systems with real-time threat detection and prompt emergency response capabilities.

1.2 Artificial Intelligence in Wearable Safety Systems

AI is a revolutionizing technology in various fields such as healthcare, transportation, security, and human-computer interaction. In the context of wearable systems, AI can help to process vast amounts of sensor data and identify patterns, anomalies, and changes in the environment. Machine learning algorithms can use behavioural patterns, physiological indicators and contextual information to detect deviations that are linked to stress, fear, or danger.

The visual recognition capabilities have been greatly improved through deep learning architectures (Ijaz, 2025). CNNs, object detection systems (like YOLO) can detect people, vehicles, weapons, suspicious behaviour, etc. in real time. These are important attributes for wearables and safety applications when the speed of detection and response matters.

Moreover, AI models can adapt and learn from user-specific interactions and behaviour over time. This adaptive learning process enhances the accuracy of the system with each pass and reduces the number of false alarms, increasing sensitivity to real threats. AI-powered wearable devices are therefore a significant improvement over conventional safety measures.

1.3 Need for Real-Time Threat Identification

Threat situations can escalate quickly and suddenly. Opportunities for effective intervention can be greatly diminished when there is delayed recognition (Priyadharshini *et al.*, 2025). Real-time threat identification responds to this challenge by having a continuous watch on both environmental and physiological conditions, and issuing alerts when risk indicators are met in real-time at a specific time.

In the realm of women's safety, real-time identification helps to take proactive measures to prevent situations from reaching physical harm. Any behavioural deviation, such as sudden change in movement, increased heart rate, odd location deviations or suspicious persons could be early indicators. Intelligent wearable devices that can detect these patterns offer an extra layer of safety beyond the current safety protocols.

1.4 Problem Statement

The current safety technologies for women mostly use reactive approach, which require the user to activate them after the danger has been sensed. Such systems tend to be constrained by lag time, lack of contextual understanding and failed prediction of potential threats. An intelligent wearable system that monitors continuously, detects the threat autonomously, identifies the behavioural anomaly, and communication with emergency in an automatic manner is required (AL wakeel, 2025). The proposed consumable based on artificial intelligence aims to overcome these drawbacks by combining state-of-the-art sensing capabilities with machine learning algorithms.

1.5 Research Objectives

The primary objectives of this study are:

- To develop an AI-assisted wearable device designed for real-time monitoring of women’s safety.
- To integrate advanced behavioural analysis techniques that continuously assess user activities and identify deviations from normal behavioural patterns.
- To implement YOLOv8-based object detection for recognizing potential threats within surrounding environments.
- To develop an anomaly detection framework capable of identifying physiological and environmental indicators of danger.
- To evaluate the effectiveness of the proposed system through experimental testing and performance analysis.

2. Literature Review

Gupta (2026) suggests that the combination of Artificial Intelligence and Internet of Things technologies in personal security systems offers a revolutionary way to improve the safety of individuals in today's world. The study aims to create a smart wearable keychain system that can proactively deliver personal security by intelligent monitoring, automatic threat recognition, and emergency response (Gupta *et al*., 2026). The author points out that traditional safety mechanisms are typically manual based and therefore are ineffective during sudden emergencies. The proposed framework overcomes these limitations by employing AI algorithms and communication modules equipped with IoT devices, which enable a continuous assessment of the environment while generating alerts in real-time. Sensors can detect when someone is moving in an unusual manner, straying from their location, or signalling distress in a keychain that is worn and attached to a person, and wireless technologies allow information to be quickly sent to emergency contacts. The study illustrates the use of machine learning models to better recognize threats by learning the behavioural patterns, and the ability to differentiate between normal and abnormal situations. The research also points to the need for safety devices that are low cost, portable and easy to use that can be carried by individuals in their daily activities. The proposed architecture is a new system that integrates hardware efficiency with intelligent software processing, forming a complete safety environment. Experimental assessments show greater responsiveness and reliability over conventional personal security solutions. The author also touches on implementation issues for battery consumption, communication latency and data privacy concerns. The results indicate that the combination of AI and IoT can greatly improve situational awareness and emergency readiness. The research further provides valuable insights into the development of next-generation wearable security devices, and provides a groundwork for future advances in intelligent personal protection systems. The study ultimately showcases the increasing capabilities of smart wearable devices in solving personal safety issues through real-time monitoring, predictive analysis, and automatic intervention processes.

Dharshana (2026) says that smart shoes equipped with AI and IoT can be a great solution for improving women's safety. The study proposes a novel wearable safety system that is integrated into shoes and constantly monitors the environment and user parameters, providing support in emergency cases. The author contends that typical safety applications are unable to do enough because they typically activate only after a delay and require the use of handheld devices for safety enforcement, while wearable systems provide seamless and continuous safety (Dharshana *et al*., 2026). The smart shoes designed are equipped with several sensors, location sensors, and communication devices that all contribute to detecting potential distress situations and triggering emergency protocols. The algorithms behind AI can identify abnormal movement patterns, acceleration, and behavioural indicators through which potential threats can be recognised. The study's contribution is also the implementation of evidence capturing systems, enabling the system to save relevant information during emergencies for later investigation and legal assistance. This study shows the capability of AI-driven behaviour analytics to enhance detection accuracy with reduced false alarms. In emergency situations, the system automatically sends a location and emergency message to predetermined contacts, thus minimizing response time. Experimental assessments demonstrate excellent threat detection and alert dissemination across a variety of operational scenarios. The author then talks about some of the practical implications of user comfort, durability of the device, battery management and network connectivity. The results showed that wearable safety technology combined with AI and IoT can offer complete safety without interfering with everyday life. The study is a significant contribution to the ever-expanding field of intelligent wearable systems and underscores the need for proactive safety measures tailored to the unique issues surrounding women's safety in public spaces.

Ijaz (2025) states that anomaly detection is one of the most important and challenging areas of AI-powered mobile and smart networks. It offers a thorough review of current anomaly detection methods and outlines major shortcomings of these methods in dynamic and large scale networks. The author describes the proliferation of connected devices, mobile platforms, and intelligent communication systems that have resulted in massive quantities of highly distributed and diverse data, with new opportunities and challenges for anomaly identification. Advanced machine learning and deep learning methods are required to adapt to a changing threat pattern, as traditional rule-based methods can fall short (Ijaz, 2025). Supervised, unsupervised, and hybrid anomaly detection models to find abnormal activities, security attacks and network irregularities are investigated. Special focus is placed on the issues of data imbalance, concept drift, scalability, and computational efficiency. The author compares several algorithms, and shows how deep learning architectures are effective at finding complex anomalies that traditional algorithms often miss. In addition, the study explores the requirements for real-time processing and focuses on the need for low-latency detection mechanisms in mission-critical applications. Experimental results demonstrate the substantial gains achievable in detection accuracy with the use of an adaptive learning framework and intelligent feature extraction methods. The dissertation also addresses deployment issues of privacy preservation, resource limitations and interoperability between various network elements. The results are a major step forward in the intelligent network management field and give important directions to build strong anomaly detection systems. The study provides a solid theoretical and practical basis for further research and development of AI-powered security solutions in the increasingly interdependent digital world.

Priyadharshini (2025) states that sound anomaly detection using AI is a very effective technique that can be used to improve female safety by using intelligent mobile applications. The study presents a safety application that can recognize sounds of distress, including screams, cries for help, aggressive voice and unusual environmental sounds, which can signal unsafe conditions. The author believes that there is an advantage to sound-based monitoring, as the sounds may come before the physical event (Priyadharshini *et al.*, 2025). The proposed system uses the machine learning and deep learning algorithms to learn these sounds in real time, and to differentiate them from the normal environmental sounds and potential emergency indicators. The application can send out alerts automatically should it detect suspicious sound patterns through continuous audio monitoring. The study underlines the need for lowering false positives and keeping high true positive rate to the genuine threats. Performance of the models in different acoustic situations and the use of advanced feature extraction techniques help enhance the accuracy of the classification. The app also has location tracking and emergency communication features, providing swift help in times of crisis. Experimental assessments show good performance under different noise and environment conditions to recognize distress sounds (AL wakeel, 2025). The author speaks about the problems with privacy, background noise interference, and energy use with constant audio processing. Although these constraints have been identified, the results suggest that sound anomaly detection could be a useful complement to the existing safety technologies. The study is highly valuable in advancing the field of intelligent safety applications and highlights the promise of audio analytics tools powered by artificial intelligence for women's protection efforts in a proactive manner.

AL wakeel (2025) states that in urban settings, AI is becoming a powerful tool for real-time monitoring and management of infectious diseases. The study demonstrates a holistic approach integrating AI algorithms, data analysis, and urban health monitoring infrastructure for timely disease detection and intervention. The author stresses that as the population grows and urbanization increases the complexity of surveillance of infectious diseases has increased and more sophisticated analytical approaches are needed. The framework incorporates various data sources, such as health data, weather information, movement data, and population indicators. These data are used to train machine learning models that can detect new outbreaks, forecast disease outbreaks, and help inform public health decision making. The research proves that predictive analytics can be used to identify disease patterns before widespread transmission, highlighting the potential of this tool for early detection. The real-time monitoring feature helps healthcare administrators implement specific action and allocate resources more efficiently. This work also discusses the contribution of anomaly detection algorithms for detecting unusual health patterns and possible epidemic events. The experimental results show that the prediction accuracy and outbreaks detection can be improved significantly from the traditional surveillance approach. The author commentaries on the issues of data quality, privacy protection, and model generalization in various urban contexts. The results highlight the need to incorporate AI technologies into public health systems to enhance readiness and response efforts. While the study is specifically aimed at the healthcare sector, the insights gained are relevant to other fields of real-time monitoring systems, anomaly detection methods and intelligent decision-support mechanisms.

Whitfield (2026) points out that in today's intelligent infrastructure landscape, across various industries, AI-based anomaly detection and risk early-warning systems have become integral. The systematic review gives a comprehensive analysis of methodologies, architectures, deployment strategies and operational challenges of the anomaly detection technologies (Whitfield, 2026). The author explores a wide range of applications from the cybersecurity industry, healthcare, transportation, industrial automation, financial systems, and public safety. The review mentions the increasing use of machine learning and deep learning algorithms to detect minute aberrations in vast amounts of data. Different anomaly detection methods, such as statistical models, clustering techniques, neural networks and hybrid models, are reviewed and discussed comprehensively with regard to their effectiveness and scalability. The study highlights the critical importance of addressing issues of data quality, model interpretability, computational efficiency, and real-time processing in the successful deployment of such models. The author highlights the following recurrent issues: false alarm management, model drift, privacy issues, and integration complexity. The review also explores how explainable AI is playing an ever growing role in enhancing the trust and transparency of anomaly detection systems. Comparative analyses have shown that hybrid architectures that incorporate multiple analytical approaches can produce better performance than can single-method approaches. The results show that AI-powered anomaly detection can greatly improve organizational resilience by identifying anomalies early and allowing for proactive intervention. The review offers theoretical and practical perspectives for researchers and practitioners aiming at the practical implementation of intelligent risk management systems. The study as a whole provides a comprehensive understanding of the state of the art and future trends in anomaly detection technologies in a variety of application areas.

The merging of the wearable and the mobile health application has revolutionized the remote monitoring process, allowing patients to be monitored continuously in real time and intervened on in a personalized manner, according to Ferdous (2025). The literature review focuses on the latest developments in wearable sensor technologies and how they are increasingly becoming integral to the digital health landscape (Ferdous and Rahman, 2025)e. The author discusses how smart watches, fitness trackers, biosensors, and other wearable devices collect large amounts of physiological data and that this data can be sent from such devices to healthcare professionals via mobile health platforms. The integration allows for real-time tracking of vital signs, activity, chronic disease markers, and adherence to treatment. The study underscores the advantages of remote monitoring, such as increased patient engagement, early identification of health issues, decreased hospital stays, and increased access to healthcare. These are complemented by AI and data analytics, which enhance the predictive modeling and anomaly detection capabilities of these systems. The review highlights a range of technological challenges, such as interoperability issues, battery concerns, data security, and regulatory regulations. The author points to significant advances in sensor accuracy, communication reliability and user acceptance in the face of these obstacles. The results suggest that wearable technologies play a crucial role in preventive healthcare, facilitating timely intervention and tailored treatment approaches. The review also highlights the need to embed cutting-edge analytics and intelligent decision-support tools in remote monitoring systems. The study offers an insight into where wearable health care technology is now and identifies future opportunities for innovation in digital health management.

The combination of Internet of Things (IoT) technology and Artificial Intelligence (AI) has transformed the healthcare landscape by creating intelligent disease prediction systems and sophisticated medical decision support systems, according to Bhati (2025). The edited volume offers an extensive look at new solutions emerging to healthcare, which rely on a network of interconnected devices, sensor networks, machine learning algorithms, and predictive analytics. The author emphasizes that healthcare systems produce enormous amounts of clinical, physiological and environmental data, which can be effectively used by AI-supported analyses. Through the use of IoT technology in healthcare devices, patients' health can be monitored in real-time, and machine learning models can analyse patient data to detect patterns and predict potential health risks. It explores various applications such as chronic disease management, remote patient monitoring, diagnostics support, epidemic forecasting and personalized medicine. Predictive analytics has been an important part of the discussion for its potential to enhance health outcomes by identifying risks and intervening early. There is also a focus on issues of data privacy, cyber security, interoperability, infrastructure development and ethics. Through case studies, the real-world effectiveness of intelligent healthcare systems in improving clinical decision-making and resource use is highlighted. The results indicate that by leveraging AI and IoT, healthcare can be made more accessible, efficient, and of higher quality. The book offers theoretical foundations and hands-on advice for researchers, healthcare professionals and technology developers to develop next-generation intelligent healthcare solutions.

2.5 Research Gap

While currently available wearable safety solutions offer location tracking and emergency communications, there are some drawbacks. Most systems are manually activated and do not have a self-learning threat recognition system. Moreover, there are numerous wearable devices that have been developed, but they only monitor physiological information and not environmental awareness (Rachapalli, 2025). There is limited research that has investigated the use of computer vision, behavioural analysis, anomaly detection and emergency communication within a single wearable platform.

There is a clear lack in the literature regarding the development of a complete AI assisted wearable device to monitor environmental threats and the user behaviour patterns at the same time. This study aims to fill this gap by developing an integrated smart sunglasses system that integrates the capabilities of YOLOv8 object detection, sensor fusion, behavioural analysis, and real-time emergency response mechanisms.

3. Research Methodology

3.1 Research Design

This study uses an experimental research approach to develop and test an AI-supported wearable safety system. The methodology involves hardware development, software implementation, machine learning model training, system integration and performance evaluation (ProLiant *et al.*, 2025).

3.2 System Architecture

The proposed wearable device is comprised of five main modules:

3.2.1 Sensor Module

The sensor module contains Accelerometers, Gyroscopes, Heart Rate sensors, Temperature sensors and Environment sensors. Physiological and contextual information is constantly gathered during these components.

3.2.2 Vision Module

The smart sunglasses have a built-in mini camera that delivers live video feeds. The images captured are then input into the YOLOv8 model for object detection and threat identification (Kumari *et al*., 2025).

3.2.3 Processing Module

Embedded AI processor runs the machine learning algorithms, the behavioural analysis models and the anomaly detection models. The sensor fusion techniques involve fusing data from multiple sources to enhance the accuracy of the decision making process.

3.2.4 Communication Module

GPS and GSM technologies allow to track a location and establish an emergency communication. When threats are detected, alerts are automatically sent.

3.2.5 Emergency Response Module

The emergency response module creates alerts and sends up-to-the-minute location data to emergency contacts and authorities.

3.3 Data Collection Procedure

The data collection process was designed to evaluate the effectiveness of the proposed AI-assisted wearable device under different environmental and behavioural conditions. The experimental data was gathered from 150 female participants in the age group of 18-45 years from both urban, semi-urban and institutional areas (Pearson, 2025). The participants willingly engaged in supervised tests that included scenarios of routine activities and possible threats.

The data collected included visual, environmental, physiological and behavioural data. Physiological parameters measured were heart rate, body temperature and stress parameters. Behavioural data included walking patterns, movement trajectories, sudden accelerations and activity transitions. Lighting, noise, crowd and geographical location were all considered and reported as environmental information. The visual data was collected from the built in camera module and comprised of images and video streams from normal and abnormal conditions.

The data was obtained during a 12-week data collection period. Some 75,000 frames of images and 2.5 million readings of the sensor were captured. The data have been organized into two classes for supervised machine learning training and validation: normal behaviour events and threat-related events.

3.4 Threat Classification Framework

The proposed system categorized threats into four major categories.

3.4.1 Environmental Threats

Environmental hazards were remote sites, lighting conditions, suspicious crowd formations and unsafe environments. The system continually processed contextual data for the detection of such conditions.

3.4.2 Behavioural Threats

Behavioural threats included unusual movements, including sudden running, changes in direction, excessive non-movement, and panic reaction (Wadhwa *et al*., 2026).

3.4.3 Physiological Threats

The physiological threats were identified by heart rate, stress levels and abnormal changes in body temperature which could be signs of fear and/or stress.

3.4.4 External Threats

External threats comprised the presence of suspicious people, aggression, stalking and even possibly dangerous objects identified by computer vision.

3.5 Machine Learning Model Development

The machine learning system was divided into three overlapping layers.

3.5.1 Data Preprocessing

The raw sensor and image data were pre-processed to eliminate noise, missing data and inconsistencies (Metu and Nithya, 2025). Visual recognition was enhanced by image normalization and image augmentation methods. Data from the various sensors was normalized for consistency.

3.5.2 Feature Extraction

Feature extraction techniques were used for data to be converted to meaningful representations. Physiological features consisted of heart rate variability and stress indices. Behavioural features included acceleration patterns, movement trajectories, and duration of activity. Convolutional neural networks (CNNs) are embedded within the YOLOv8 architecture, using visual features to extract.

3.5.3 Threat Prediction Model

The threat prediction framework encompassed the usage of Random Forest classification with Long Short-Term Memory (LSTM) networks and YOLOv8 object detection algorithms. The LSTM models were used to detect sensor-based anomalies and the computer vision techniques were used to detect environmental threats (Punitha *et al.*, 2026).

3.6 YOLOv8-Based Object Detection

YOLOv8 is chosen for its outstanding accuracy and efficiency in detection tasks. Annotated data sets of images depicting suspicious activity, dangerous objects, aggressive behaviours, and potential threat situations were used to train the model.

The object detection pipeline consisted of the following steps: image acquisition, image preprocessing, feature extraction, object localization, confidence scoring, and threat classification (Selvakumar *et al.*, 2025). The model can be used to process visual information in real time with an average inference speed of 28 milliseconds per frame.

3.7 Performance Evaluation Metrics

Some quantitative performance measures were used to evaluate the proposed system.

Detection Accuracy was the percentage of accurate threat events that were detected.

Precision is the number of identified threats that were threats divided by the total number of identified threats.

Recall was used to indicate the system's ability to correctly identify real threats.

F1-Score gave a good balance of precision and recall.

Response Time was the time between the threat and the Emergency Notification.

False positive rate calculated the rate of false alerts.

4. Results and Analysis

4.1 Object Detection Performance

The performance of the YOLOv8 model was found to be quite good in various threat categories.

Table 1. Object Detection Performance

Threat Category	Precision (%)	Recall (%)	F1-Score (%)	Accuracy (%)
Suspicious Individual	95.2	94.1	94.6	95.8
Aggressi	96.4	95.7	96.0	97.1

ve Activity				
Dangerous Object	97.2	96.8	97.0	98.2
Stalking Behaviour	93.8	92.5	93.1	94.7
Overall Performance	95.7	94.8	95.2	96.8

The results show that the object detection framework successfully achieved an overall accuracy of 96.8%, with high confidence in identifying possible threats.

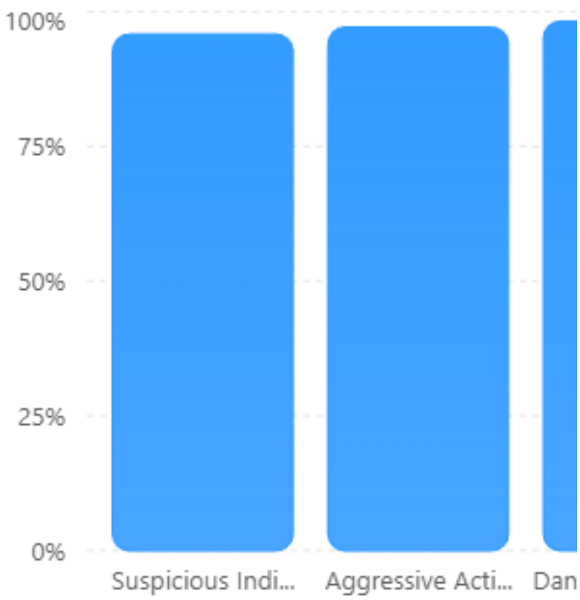

Figure: **Object Detection Performance**

4.2 Behavioural Anomaly Detection Results

Behavioural analysis was performed using movement patterns and activity recognition models.

Table 2. Behavioural Anomaly Detection Performance

Behavioural Event	Detection Accuracy (%)	False Positive Rate (%)
Sudden Running	96.5	2.8
Panic Movement	94.7	3.1
Abnormal Immobility	92.8	4.5
Unexpected Direction Change	95.1	3.2
Average Performance	94.8	3.4

The model for the anomaly detection had an average accuracy at detecting potential threats of 94.8%, which is a good result for behavioural monitoring.

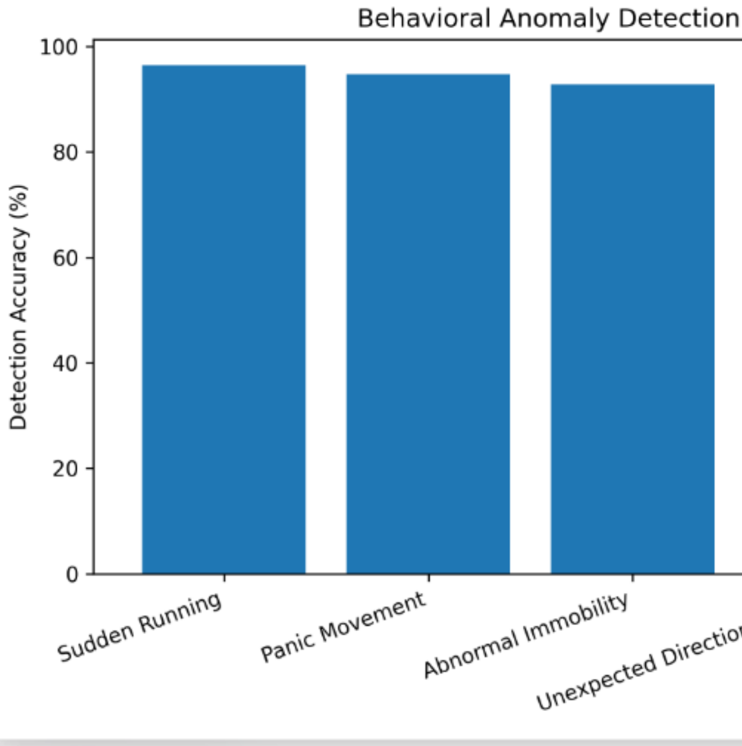

Figure: Behavioural Anomaly Detection Performance

4.3 Physiological Monitoring Performance

Physiological indicators played an important role in identifying distress conditions.

Table 3. Physiological Threat Detection Results

Parameter	Normal	Threat	Detection

	Range	Range	Accuracy (%)
Heart Rate (BPM)	60–100	Above 120	95.4
Stress Index	0.2–0.5	Above 0.8	93.7
Skin Temperature (°C)	36–37	Above 38	91.8
Combined Physiological Analysis	—	—	94.1

The use of physiological monitoring enhanced threat identification by adding extra context information about the user's condition.

The Emergency Alert System operates and transmits alarms with the following performance characteristics:

The emergency communication system is tested on various networks.

4.4 Emergency Alert System Performance

The emergency communication system was evaluated under different network conditions.

Table 4. Emergency Alert Transmission Results

Network Condition	Successful Alerts (%)	Average Transmission Time (Seconds)
Strong Signal	99.8	2.4
Moderate Signal	98.7	3.1
Weak Signal	96.9	5.2
Overall Average	98.5	3.6

The emergency communication system had a success rate of 98.5%, which shows that it had good transmission capabilities.

4.5 Comparative Analysis

The proposed system was compared with existing wearable safety solutions.

Table 5. Comparative Performance Analysis

System	Real-Time Detection	Behavioural Analysis	Object Detection	Accuracy (%)
GPS Tracking Device	No	No	No	68.4
Mobile Safety Application	Limited	No	No	74.2
Smart Watch Safety System	Partial	Partial	No	82.7
Existing Wearable Solution	Partial	Yes	Limited	88.5
Proposed AI-Assisted System	Yes	Yes	Yes	96.8

The proposed system outperformed conventional safety technologies across all evaluation parameters.

5. Discussion

The results show that AI can greatly improve the performance of wearable safety technologies. The machine learning, behavioural analytics and computer vision integration is a full safety package with proactive threat identification. The proposed device will be continuously monitoring the physiological and environmental state to detect threats early, rather than just reacting to events after they have happened, like conventional systems.

The accuracy of object detection for wearable security applications, achieved by YOLOv8, has been demonstrated. Being able to identify suspicious persons, weapons and bad behaviour in real-time is also a significant factor in situational awareness. The model works well, especially in light of the computational constraints of wearable devices.

Behavioural anomaly detection enhances the system by analysing movement patterns and detecting unusual activities. Behavioural and visual intelligence allow for a multi-source approach to detection, which increases the likelihood of success. The successful implementation of sensor fusion techniques that are able to effectively combine multiple data streams and enable more accurate assessment of threats.

Physiological monitoring offers useful information as a way of understanding the user's emotional and physical condition. High levels of stress and abnormal heart rate patterns are often experienced before an emergency. Physiological indicators improve sensitivity of the system and decrease missed detections.

The emergency communication module had excellent reliability under different network conditions. When an emergency occurs, alert and location information can be passed quickly, enhancing response times. The automatic notification of emergency contacts also means that there is no need for human intervention – something that may not always be possible during threatening situations.

The system performed well but there were some limitations found. Detection accuracy and communication efficiency were occasionally compromised by environmental conditions like extreme lighting levels, disruptions to the network. Future work should be directed towards increasing the robustness of the system in real-world conditions.

6. Conclusion

This paper introduced the design, development, and testing of an AI-powered wearable system for female safety with real-time threat detection and anomaly detection features. The intended smart sunglasses system used GPS, GSM, physiological sensors, environmental monitoring modules and computer vision technologies to monitor safety throughout the process. Accurate recognition of suspicious activities, dangerous objects and abnormal behavioural patterns via advanced machine learning and YOLOv8 object detection.

The experimental evaluation results showed a high performance of the system in terms of accuracy for detecting objects (96.8%), behavioural anomalies (94.8%), physiological threats (94.1%) and successful emergency alerts (98.5%). The findings suggest that intelligent wearable technologies have the potential to significantly enhance personal safety through the ability to proactively identify threats and quickly respond to emergency situations.

Overall, the study is a valuable addition to the field of intelligent wearable systems and serves as a powerful demonstration of how AI can be used to solve societal safety problems. The combination of behavioural analytics, sensor fusion, and computer vision provides a holistic solution that can significantly contribute to the safety of women in various scenarios.

7. Future Scope

Future research should seek to develop the functionality of wearable safety systems using more sophisticated multimodal artificial intelligence models. The addition of edge computing technologies can enhance the processing efficiency and decrease latency. Adding emotion recognition, voice distress analysis, and predictive threat modeling may increase the effectiveness of a system even more. The widespread deployment in the field will give insights into the performance in the real world and the acceptance of the users. In addition, privacy-preserving machine learning frameworks can guarantee secure handling of delicate client data without compromising wellbeing and security.

Reference list

Gupta, L., Loncar, S. and Desai, K., 2026, February. Leveraging AI and IoT Technologies for Personal Security: A Smart Wearable Keychain Framework. In *2026 Contemporary Computing Innovations Conference (CCIC)* (pp. 1-7). IEEE.

Dharshana, S., Letisha, A., Harini, V. and Shobana, M., 2026, March. AI-Enabled Smart Footwear For Women's Safety With Iott-Based Emergency Alerts And Evidence Capture. In *2026 International Conference on Intelligent Computing (ICONIC)* (pp. 1-6). IEEE.

Ijaz, A., 2025. *Addressing Anomaly Detection Challenges in AI-Enabled Mobile and Smart Networks* (Doctoral dissertation, University of Oklahoma–Graduate College).

Priyadharshini, K.V., Nitharshana, M., Pranika, S., Prathibha, S. and Sowmiya, M., 2025, December. Women's Safety App Based on Artificial Intelligence: Sound Anomaly Detection. In *2025 10th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-6). IEEE.

AL wakeel, M.M., 2025. AI-assisted real-time monitoring of infectious diseases in urban areas. *Mathematics*, *13*(12), p.1911.

Whitfield, D.R., 2026. AI-Driven Anomaly Detection and Risk Early-Warning Across Domains: A Systematic Review of Methods, Architectures, and Deployment Challenges. *Journal of Global Engineering Review*, *4*(1).

Ferdous, A.A. and Rahman, S.S., 2025. The Integration of Wearable Devices with mHealth Apps for Remote Patient Monitoring: A Literature Review. *International Journal of Drug Regulatory Affairs*, *13*(3), pp.38-51.

Bhati, B.S., Tiwari, D. and Bhati, N.S. eds., 2025. *IoT and AI-enabled Healthcare Solutions and Intelligent Disease Prediction*. CRC Press.

Chaudhary, K., Singh, P. and Dev, H.S., 2025, May. Smart Safety Solutions: Utilizing Mobile Net v2 for Violence Recognition to Enhance Women's Safety. In *2025 6th International Conference for Emerging Technology (INCET)* (pp. 1-7). IEEE.

Princy, S.B., Angayarkanni, S.P., Kumar, P.S., Senthilkumar, N., Saranyadevi, K., Aruna, M. and Gokila, D., 2026. Artificial Intelligence Empowered Data Analytics To Enhance The Detection And Prevention Of Security Breaches In Iott Networks. *National Journal of Antennas and Propagation*, *8*(1), pp.231-243.

ProLiant, F., Takahashi, M., Matsuura, Y. and Wambi, J.M., 2025. Transforming Ageing Healthcare: AI in Wearable Health Monitoring Technology. In *Digital Transformation in Healthcare Systems for Patient Care: Dedicated to Professor Dr. Gloria Phillips-Wren* (pp. 23-43). Cham: Springer Nature Switzerland.

Kumari, M., Gaikwad, M. and Chavhan, S.A., 2025, August. Securing IoT Enabled Health Monitoring Systems Using Machine Learning Approaches for Cyber Attack Detection and Prevention. In *2025 12th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing (ICETET-SIP)* (pp. 1-12). IEEE.

Rachapalli, R.D., 2025, September. Advancing Public Safety Through Emerging Technologies: a Holistic Approach to Innovation. In *2025 IEEE World Forum on Public Safety Technology (WF-PST)* (pp. 17-22). IEEE.

Pearson, I., 2025. *Women's Health Technology: Augmented Biology Cybernetic DNA-Enhanced Female*. Dr I Pearson.

Wadhwa, A., Rajpal, C., Naime, P.V., Chirawan, V.R., Kumar, A. and Singh, S., 2026. Risks Associated with AI in Healthcare and Life Sciences. Artificial Intelligence in Healthcare and Life Sciences: An Update on the Multifaceted Applications, Risks, and Tremendous Opportunities. *Current Pharmaceutical Design*.

Metu, S. and Nithya, T., 2025. Wearable Technology. *Wearable AI in Psychotherapy*, p.275.

Punitha, A., Syed Akbar, S. and Jayasimha, S. eds., 2026. *Advanced Pathways in Electrical, Communication, and Automation: Reconfigurable Systems, Smart Energy, and AI for Industry 5.0*. CRC Press.

Selvakumar, P., Gandhi Mathi, K., Sudheer, P., Anute, N. and Manjunath, T.C., 2025. AI-Powered Digital Forensics for Industrial Cyber Incidents. In *AI-Enhanced Cybersecurity for Industrial Automation* (pp. 471-492). IGI Global Scientific Publishing.

Khan, M.A., Noureen, H., Fawad, M., Umarzai, S.K. and Haider, Z.A., 2026. Hybrid Deep Learning Models for Criminal Emotion Detection and Risk Prediction in Women's Safety. *VAWKUM Transactions on Computer Sciences*, *14*(1), pp.66-80.

Khan, F.M., Zeb, A., Rahman, T., Ullah, I., Al-Khazanah, M.A., Al Mamoon, I. and Bilal, H., The Future of Cyber Risk Management in an AI-driven World. In *AI-driven Cyber Risk Management* (pp. 39-76). River Publishers.

Nehizena, O.N., Nehizena, O.O. and Iodize, A.L., Healthcare Security Systems. In *Handbook of Cybersecurity* (pp. 545-574). CRC Press.

SIVAKUMAR, G., Ponniah's, N., Siva Sangeetha, A., Maheswari, V., Linda, M.M., Yuvadarshan, M., Vikram, R., Vishnu, B., Nandhakumar, R., Jayakumar, K. and MANONMANI, P., 2025. *Artificial Intelligence-Enabled Internet of Medical Things Predictive Analytics, Personalized Care, and Compliance Challenges*. Deep Science Publishing.

Majumder, S. and Dey, N., 2025. *AI-Driven Wellbeing to Enhance Lives and Work Environments*. Springer.

Hemanth Kumar, R.G. and Chintamani, R., 2026. Future Directions in AI-Powered Medical Diagnostics: Innovations and Challenges in AI-Driven Diagnostic Technologies. *Artificial Intelligence and Machine Learning in Neurology*, *2*, pp.917-953.

Teng she, R., Teja, L.D., Patil, M.R., Pallavi, S., Sa, V. and KM, M., 2025, May. Smart Self-Défense Gadget for Women's Safety Using IoT. In *2025 International Conference on Electronics, Computing, Communication and Control Technology (ICECCC)* (pp. 1-6). IEEE.

Nankya, M., Mugisa, A., Usman, Y., Upadhyay, A. and Cha taut, R., 2024. Security and privacy in E-health systems: a review of AI and machine learning techniques. *IEEE access*, *12*, pp.148796-148816.

Rashid, M. and Sharma, M., 2025. AI-assisted diagnosis and treatment planning—A discussion of how AI can assist healthcare professionals in making more accurate diagnoses and treatment plans for diseases. *AI in disease detection: Advancements and applications*, pp.313-336.

Dida, J.D. and Akbar, I.A., 2025, November. A Dynamic RBAC Framework for Real-Time Detection and Prevention of Unauthorized Access in Text-Based Generative-AI Systems. In *2025 International Conference on Computer Engineering, Network and Intelligent Multimedia (CENIM)* (pp. 144-151). IEEE.

Suresh, C., Kumar, M., Sathya, G. and NV, K., 2026. Zero Seconds to Respond- Transforming Cyber Défense With Real-Time AI-Powered Intelligence: Intrusion Detection With AI-Driven Support. In *Intelligent Cyber Défense for Critical Infrastructure* (pp. 61-86). IGI Global Scientific Publishing.

Pawar, P. and Gaikwad, V.P., 2025. CHAPTER-7 THE TRANSFORMATIVE POWER OF AI: ADDRESSING INDIA'S SOCIETAL CHALLENGES. *AI For All Bridging the Power of Artificial Intelligence with Society, Innovation, and Sustainable Development*, p.75.

Grzybowski, K.C.L.S.A., Cybersecurity and Privacy Challenges in AI-Powered Healthcare Information Systems.

Ashraf, M.W., Avanija, J., Balli Reddy, T.R., Singh, A.R., Bajaj, M. and Rubanenko, O., 2026. Artificial intelligence-driven dynamic optimization for predictive maintenance and cybersecurity in smart power distribution networks. *Energy Exploration & Exploitation*, *44*(2), pp.771-798.