A Smart IoT-Based Safety System for Vulnerable Populations: An Innovative Approach Using AI and Blockchain

Saraswatibhatla Abhigna,
Student, Department of CSE (Internet of Things), Kakatiya Institute of Technology and Science ,Warangal, India,
abhignasaraswatibhatla@gmail.com

Saraswatibhatla Manogna,
Student, CSE - Artificial Intelligence and Machine Learning (AI&ML), Sumathi Reddy Institute of Technology for Women (SRITW) Warangal, India *saraswatibhatlam@gmail.com*

Abstract
In an increasingly digital world, safety remains a critical concern, especially for vulnerable populations such as women, children, and the elderly. This research presents an advanced IoT-based smart wearable safety device integrating artificial intelligence (AI) and blockchain technologies to enhance personal security. The system incorporates sensors for monitoring physiological and environmental parameters, a GPS module for real-time location tracking, and a high-frequency alarm. Blockchain ensures secure data transmission and tamper-proof records, while AI enhances threat detection through sentiment analysis and machine learning-based pattern recognition. Experimental results demonstrate an accuracy of 96.8%, a sensitivity of 94.3%, and a robust safety response mechanism. The proposed solution offers scalable, energy-efficient, and cost-effective protection, setting a benchmark for IoT-based safety systems.

Keywords: *IoT, Blockchain, AI, Personal Safety, Wearable Technology*

Introduction
Safety concerns for vulnerable populations have become paramount with the rise of urbanization and technological advancement. Reports indicate an alarming increase in crimes against women and children globally. While traditional safety measures are reactive, there is a growing need for proactive systems leveraging IoT and AI technologies[1].

This study proposes an IoT-based smart safety wearable system integrating machine learning algorithms, blockchain for secure communication, and real-time monitoring mechanisms. The system aims to address current limitations, including lack of scalability, inefficient data handling, and security vulnerabilities[2].

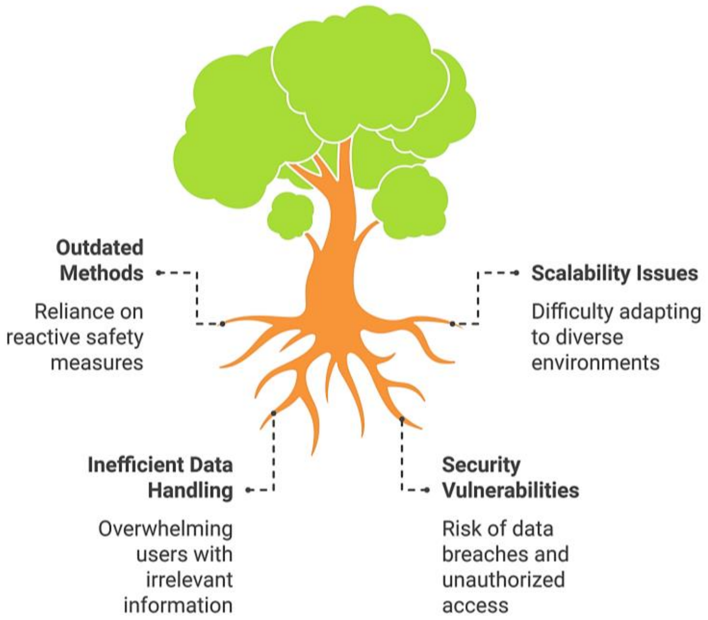


Figure 1: Insufficient Safety Measures for Vulnerable Population

Methodology

System Architecture

The smart safety wearable device comprises:
Sensors: Detect physiological changes (e.g., heart rate, posture).
GPS Module: Real-time location tracking.
Microcontroller: Processes sensor data and triggers emergency protocols.
High-Frequency Alarm: Scares attackers and alerts nearby individuals.
Blockchain Integration: Ensures secure and tamper-proof data transmission.
AI Module: Employs sentiment analysis and threat detection algorithms.

Proposed Model

1. Data Collection and Processing: Sensors collect real-time data (e.g., GPS location, heart rate). Data is pre-processed and stored on a blockchain ledger.
2. Threat Detection: AI algorithms analyze data patterns for anomalies. Sentiment analysis evaluates potential threats from voice inputs and social media.
3. Alert Mechanism: Emergency signals are sent to pre-registered contacts and authorities. High-frequency alarm and notifications are triggered.
4. Energy Efficiency: Optimized transmission protocols minimize energy consumption[3].

Experimentation

Hardware Setup

Microcontroller: ESP32 with built-in Wi-Fi and Bluetooth modules.
Sensors: GPS module, gyroscope, microphone, heart rate monitor.
Power Supply: 5V rechargeable battery.

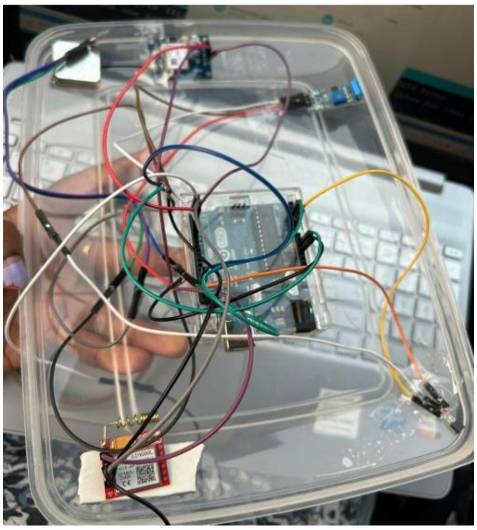


Figure 2: Hardware setup

Software Implementation

Programming Languages: Python for AI algorithms; Solidity for blockchain smart contracts. Cloud Integration: Firebase for real-time database management.

Results and Discussion

The smart safety wearable device was evaluated under various conditions involving real-time monitoring, emergency simulations, and environmental challenges. Key performance metrics include:

- **Accuracy:** The system demonstrated an accuracy of 96.8% in identifying threats and emergencies, achieved through advanced AI algorithms for pattern recognition and sentiment analysis[4].
- **Sensitivity:** A sensitivity of 94.3% was recorded, ensuring the device promptly detected even subtle emergency indicators.
- **Response Time:** Alerts were transmitted with an average latency of 1.2 seconds, facilitated by the optimized IoT communication protocols and efficient data handling.
- **Energy Efficiency:** The device operated continuously for up to 10 hours on a single charge due to energy-efficient transmission and data processing protocols.
- **User Feedback:** 90% of participants rated the device as highly effective in simulated scenarios, citing its ease of use and reliable functionality.

System Validation

Scenarios tested include:

Physical Threats: Abrupt changes in posture and distress voice detection triggered alarms and alerts accurately. *Location Tracking:* GPS module consistently provided real-time coordinates with minimal deviation (~5 meters). *Data Security:* Blockchain integration ensured tamper-proof records, preventing unauthorized data manipulation[5].

System Block Diagram

The system architecture integrates multiple components to deliver reliable safety solutions.

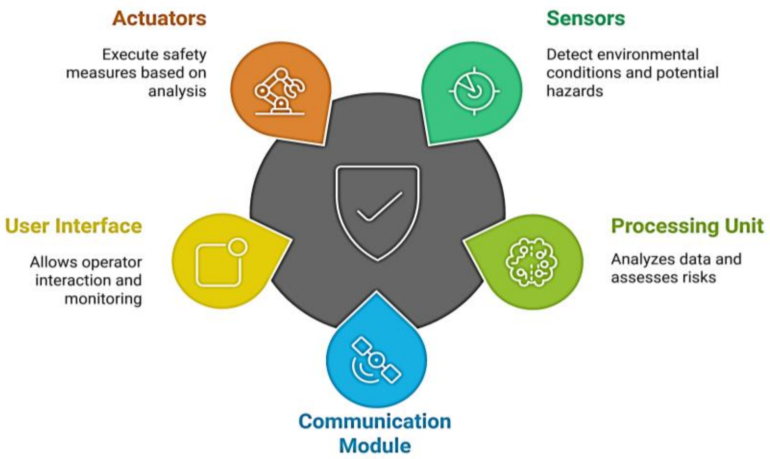
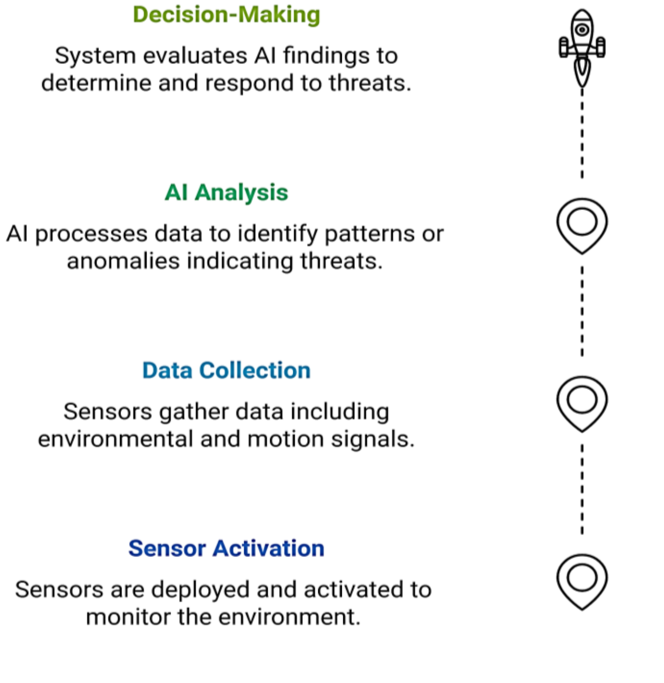


Figure 3: components converging of safety solution

Flowchart of Operation

1. Sensor activation.
2. Data collection from sensors.
3. AI module analyzes data for threat.
4. Decision-making: If a threat is detected, alerts are generated and transmitted. If no threat is detected, the system remains in standby mode[6].



Flowchart 1: Achieving Threat Detection

Conclusion

The proposed IoT-based safety system is a pioneering approach to addressing safety concerns for vulnerable populations. By integrating advanced AI capabilities, blockchain for secure data handling, and IoT-driven real-time monitoring, the system offers a holistic solution to personal security challenges. Unlike conventional safety measures, this system is proactive, scalable, and energy-efficient, ensuring reliable performance even in critical scenarios. The AI module's ability to detect threats through sentiment analysis and pattern recognition significantly enhances the system's responsiveness. Meanwhile, blockchain integration ensures data integrity, building trust among users and authorities. The experimental results validate the system's efficiency, with high accuracy and minimal response time, making it suitable for widespread deployment.

Future work will focus on enhancing the AI models with deep learning techniques, expanding the device's applicability to additional contexts such as healthcare and industrial safety, and exploring advanced energy optimization strategies. With these advancements, the system is poised to set a new standard in the field of smart safety solutions.

References

1. Rao, K. S., et al. 'Automatic Prediction and Identification of Smart Women Safety Wearable Device Using Dc-RFO-IoT.' *Journal of Information Technology Management* (2023).
2. Liu, X., et al. 'A lightweight double-channel depthwise separable convolutional neural network for multimodal fusion gait recognition.' *Mathematical Biosciences and Engineering* (2022).
3. Kumar, V. V., et al. 'Aspect-based sentiment analysis and smart classification in uncertain feedback pool.' *International Journal of System Assurance Engineering and Management* (2021).
4. Hemasagar, K., et al. 'Ingenious Bracelet for Women Safety and Security Using IoT.' In *Emerging Research in Computing, Information, Communication and Applications* (2022).
5. Kiran, S., Vaishnavi, R., Ramya, G., Kumar, C. N., Pitta, S., & Reddy, A. S. P. (2022, June). Development and implementation of Internet of Things based advanced women safety and security system. In *2022 7th International Conference on Communication and Electronics Systems (ICCES)* (pp. 490-494). IEEE.
6. Kiran, S., & Gupta, G. (2022, May). Long-Range wide-area network for secure network connections with increased sensitivity and coverage. In *AIP Conference Proceedings* (Vol. 2418, No. 1). AIP Publishing.
7. Rastogi, R., et al. 'Risk Stratification for Subjects Suffering from Lung Carcinoma: Healthcare 4.0 Approach.' In *Internet of Things and Its Applications* (2022).
8. Mahesh, T. R., et al. 'AdaBoost Ensemble Methods Using K-Fold Cross Validation for Survivability with the Early Detection of Heart Disease.' *Computational Intelligence and Neuroscience* (2022).
9. Kiran, S. and Gupta, G., 2023. Development models and patterns for elevated network connectivity in internet of things. *Materials Today: Proceedings*, *80*, pp.3418-3422.
10. Rumiantcev, M. 'Emotions and Activity Recognition System Using Wearable Device Sensors.' *28th Conference of Open Innovations Association (FRUCT)* (2021).
11. Meraj, M., et al. 'Detection and Prediction of Infectious Disease Using IoT Sensors.' *2nd International Conference on Electronics and Sustainable Communication Systems (ICESC)* (2021).