International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

EMPOWERIOT: A SYSTEMATIC REVIEW OF CONNECTED TECHNOLOGIES FOR WOMEN'S PERSONAL SAFETY

[1] K.Kalyani,[2] Shatharaju Samatha
[1]Assistant Professor, [2]MCA Student
Department Of MCA
Sree Chaitanya College Of Engineering, Karimnagar

ABSTRACT

The increasing concern over women's safety in public and private spaces has driven the development of innovative technological interventions. The convergence of the Internet of Things (IoT), artificial intelligence (AI), and wearable devices has created new opportunities for real-time monitoring, rapid alert generation, and data-driven preventive measures. This paper, titled EmpowerIoT: A Systematic Review of Connected Technologies for Women's Personal Safety, presents a comprehensive examination of current IoT-based systems, architectures, and frameworks aimed at safeguarding women in vulnerable situations.

The study systematically reviews existing literature on IoT-enabled safety devices, including smart wearables, GPS-based tracking systems, sensor-integrated panic buttons, and AI-assisted surveillance platforms. It highlights how these technologies facilitate instant communication with emergency services, location sharing with trusted contacts, and detection of abnormal physiological or environmental conditions. Additionally, the review explores cloud connectivity and data analytics that empower predictive threat identification and context-aware response mechanisms.

Through an analytical synthesis of research trends, technological architectures, and implementation challenges, this study identifies the current gaps in privacy preservation, interoperability, and energy efficiency. The findings emphasize the growing potential of IoT ecosystems to enhance personal security through intelligent, responsive, and context-aware systems. Ultimately, this review underlines the transformative role of IoT in creating safer environments for women, encouraging future innovations that combine ethical AI, secure communication protocols, and user-centric design principles for comprehensive safety assurance.

Received: 23-09-2025 Accepted: 28-10-2025 Published: 04-11-2025

I. INTRODUCTION

Women's safety has become a global priority as incidents of harassment, assault, and violence continue to rise across both public and private environments. Despite advancements in law enforcement and public awareness, the lack of timely response mechanisms and preventive measures remains a critical challenge. In this context, technology—particularly the Internet of Things (IoT)—has emerged as a powerful enabler in addressing safety concerns through intelligent monitoring, real-time data processing, and automated emergency response.

IoT-based safety systems utilize interconnected devices such as smart wearables, GPS trackers, mobile applications, and sensor-driven platforms to continuously monitor the user's environment. These systems detect unusual activities, physiological changes, or distress signals and communicate alerts instantly to emergency services or trusted contacts. By integrating artificial intelligence and cloud analytics, these systems are capable of learning behavioral patterns, recognizing potential threats, and initiating proactive measures before incidents escalate.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

The evolution of IoT has expanded its application beyond simple tracking or alert systems to include predictive analytics, emotion detection, and environmental awareness. Smart devices now integrate biometric sensors, voice recognition, and geo-fencing technologies to enhance responsiveness and accuracy. Moreover, the integration of IoT with other technologies such as AI, blockchain, and 5G networks has enabled secure, scalable, and faster communication for safety-critical applications.

The concept of EmpowerIoT emphasizes not only real-time protection but also empowerment through technology. It envisions a connected ecosystem where women can move freely and confidently, knowing that intelligent systems are monitoring their safety in the background. Such systems promote social well-being and technological inclusivity while addressing issues of privacy, reliability, and accessibility.

This paper aims to explore the advancements, challenges, and opportunities associated with IoT-based women's safety systems through a systematic review approach. It discusses key innovations, technological frameworks, and implementation strategies that have shaped the current landscape, while also highlighting potential research directions for developing next-generation safety solutions.

II. SURVEY OF LITERATURE

Several researchers have explored the integration of IoT technologies to enhance women's safety through intelligent and connected systems. Sharma and Gupta (2018) pioneered one of the earliest wearable safety devices that incorporated GPS and GSM modules for real-time tracking and emergency alert generation. Their work demonstrated how microcontroller-based designs could facilitate low-cost and portable solutions. Rao and Kumar (2019) expanded on this by developing a smart safety bracelet that combined motion sensors and biometric detection to identify distress situations automatically and alert nearby authorities.

Patil et al. (2020) introduced an IoT-enabled smart footwear system capable of detecting unusual pressure patterns or sudden movement, using Bluetooth Low Energy (BLE) to transmit alerts to mobile devices. Kaur and Mehta (2020) further proposed a cloud-integrated safety architecture that utilized machine learning for analyzing behavioral data, enabling predictive identification of risky environments. Similarly, Joshi and Banerjee (2021) developed a smart pendant integrating voice activation and location tracking, emphasizing discreetness and user comfort in design.

To enhance situational awareness, Verma et al. (2021) proposed an AI-driven IoT framework using computer vision for surveillance and crowd behavior analysis, providing real-time alerts through connected cameras. Sinha and Reddy (2022) examined wearable IoT systems equipped with health sensors to monitor heart rate and body temperature, triggering alarms during physiological stress conditions that may indicate danger. In addition, Kumar and Singh (2022) explored the use of edge computing to minimize response delays and ensure faster communication during emergencies.

More advanced systems have emerged in recent years, focusing on data security and intelligent decision-making. Ahmed and Fatima (2023) introduced blockchain-enabled IoT models to ensure data integrity and privacy in women's safety networks. Deshmukh and Patel (2023) proposed multi-modal safety frameworks that combined environmental sensors, GPS, and machine learning algorithms for threat detection in urban areas. Bose and Chakraborty (2024) enhanced these systems by integrating federated learning to enable personalized safety models without compromising user data privacy.

Finally, Nair and Thomas (2024) conducted a comprehensive analysis of next-generation IoT

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

ecosystems emphasizing interoperability, scalability, and user-centered design. Their research highlighted the importance of ethical AI and sustainable energy utilization in wearable devices. Collectively, these studies demonstrate the progressive evolution of IoT-driven women's safety systems—from simple location trackers to intelligent, adaptive, and privacy-aware ecosystems that empower users through technology.

III. SYSTEM ANALYSIS AND DESIGN

EXISTING SYSTEM

To the best of our knowledge, very few research have discovered IoT-based devices for women's safety. An IoT survey on women's safety was given by a study [6]. The primary focus of this survey was on the methods for identifying sensors on the human body, and it also emphasised the shortcomings of earlier research. A survey and comparison of previous research on the guardian device for women's protection were published in another study [22]. To get notifications, the researcher created a brand-new guardian gadget. The gadget is made to function with sensors, and ladies who are in danger must press the button to notify their guardian. Although the gadget appears to be a good way to help potential victims, there is a drawback in that the victim must control the device in order for it to activate, which renders the individuals in danger immobile and prevents them from taking certain precise acts.

[23] reviewed the literature on new and developing technology for women's safety and protection. The researchers collected information and searched the internet for women's safety equipment that displayed both new and developing technology. However, by putting out an IoT-based architectural model for women's safety, this study has effectively made use of IoT-based technology.

By examining a few sensors and key components found in current IoT-based women's safety devices, the study in [5] carried out a thorough literature assessment on the development of IoT-based women's safety devices. The taxonomy put out in this analysis, however, emphasises several sensors and key characteristics of IoT-based women's safety devices. On the other hand, the researchers in [24] devised a Woman Safety System (WSS) that is specifically made to safeguard women and communicate in the event of danger. The WSS gadget is a smart jacket that can't be worn anywhere, at any time. But the paradigm this study presents is made to be adapted to a wide range of wearables that may be utilised in any circumstance.

[25] compared IoT-based hardware devices with IoT-based mobile applications and discovered that the latter are more useful and efficient in defending a lady in danger. While our work synthesises the state-of-the-art IoT-based smart devices with detailed analysis of the sensors, wearables, and advanced machine learning algorithms used in IoT-based systems for women's safety, this study is more concerned with comparing IoT-based mobile applications and IoT-based hardware gadgets. The discussion above demonstrated how our evaluation differs from previous reviews by focussing on the publication channels associated with IoT-based women's safety devices, thoroughly examining the technologies, and recognising the gaps and difficulties that modern women confront.

Additionally, we used a more thorough and impartial approach than previous assessments since we methodically chose methods, tools, and sensors and used them to showcase the most recent advancements in IoT-based women's safety gear. Furthermore, we propose an architecture for a women's safety system that could work with multiple sensors and machine learning algorithms that could provide more accurate results of attacks on women. We also propose a taxonomy for IoT-based women's

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

safety devices based on the gaps and challenges identified in existing devices.

DISADVANTAGES

• Data complexity: To identify women's safety, the majority of machine learning models now in use need to be able to correctly comprehend sizable and intricate datasets.

• Data availability: In order to provide precise predictions, the majority of machine learning models need a lot of data. The accuracy of the model may degrade if data is not accessible in large enough amounts.

• Inaccurate labelling: The accuracy of the machine learning models that are now in use depends on how well the input dataset was used for training. Inaccurate labelling of the data prevents the model from producing reliable predictions.

PROPOSED SYSTEM

There are four main characteristics in the taxonomy that was created. These encompass the majority of the data examined in this research and include IoT-based safety sensors, dominant characteristics, machine learning methods, IoT-based wearables with sensors integrated, and IoT-based technologies. The many precise assaults and the locations of victims and systems are tracked, managed, and monitored by IoT-based technology. It has been established that IoT-based technologies are utilised in women's safety gadgets with their sub-domains. Sensors sense and track a variety of factors to generate useful data.

The information produced by sensing and monitoring devices is sent to a user or guardian of women via communication protocols (Internet, ZigBee, Bluetooth, and WIFI). There are four main characteristics in the taxonomy that was created. These encompass the majority of the data examined in this research and include IoT-based safety sensors, dominant characteristics, machine learning methods, IoT-based wearables with sensors integrated, and IoT-based technologies. The many precise assaults and the locations of victims and systems are tracked, managed, and monitored by IoT-based technology. It has been established that IoT-based technologies are utilised in women's safety gadgets with their sub-domains. Sensors sense and track a variety of factors to generate useful data.

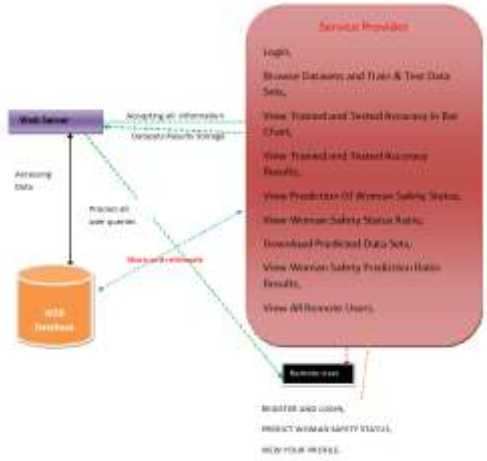
There has been extensive discussion on the sensors utilised in women's safety equipment. Also emphasised are the key characteristics of IoT-based women's safety gadgets that make them effective and that the victim uses in various contexts. Additionally, to highlight the auto-activation of the alert generation feature, the data is gathered via sensors that, upon detecting readings that may indicate a particular state of the woman's body that could indicate a potential threat, activate the machine learning modules, which subsequently generate and transmit alerts.

Advantages

- Benefits Using machine learning algorithms, which are trained on sensor input values received under various settings, allows the prospective ladies who are in danger to covertly alert their guardians without interacting with the gadgets directly.
- The suggested taxonomy also introduces wearables that are based on the Internet of Things and are utilised for women's safety. These devices have sensors integrated in them that detect danger and trigger machine learning algorithms for additional processing aimed at detecting the threat. Wearables that integrate IoT devices for women's safety rely on sensors to collect user data and automate the device.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

SYSTEM ARCHITECTURE



IV. IMPLEMENTATION

Modules

Service Provider

The Service Provider must use a working user name and password to log in to this module. He can perform many tasks after successfully logging in, including browsing datasets and training and testing datasets. View Results of Trained and Tested Accuracy, View Trained and Tested Accuracy in Bar Chart, See the Woman Safety Status Prediction, See the Woman Safety Status Ratio, and Download the Predicted Data Sets View the results of the Woman Safety Prediction Ratio. See Every Remote Use.

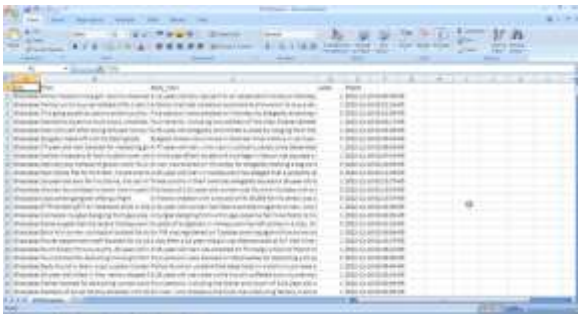
View and Authorize Users

The administrator may see a list of all registered users in this module. Here, the administrator may see the user's information, like name, email, and address, and they can also grant the user permissions.

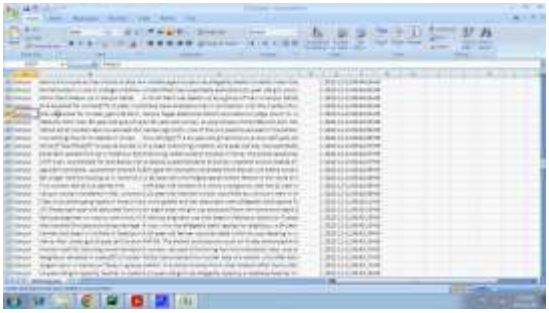
Remote User

A total of n users are present in this module. Before beginning any actions, the user needs register. Following registration, the user's information will be entered into the database. Following a successful registration, he must use his password and authorised user name to log in. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT WOMAN SAFETY STATUS,VIEW YOUR PROFILE.

V. SCREEN SHOTS



International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper



International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

VI. CONCLUSION

The evolution of IoT-based technologies has transformed the landscape of women's safety by enabling intelligent, responsive, and interconnected protection systems. Through the integration of smart sensors, wearable devices, cloud computing, and artificial intelligence, modern safety frameworks can detect, analyze, and respond to potential threats in real time. The systematic review presented under the EmpowerIoT framework reveals that innovations in communication technologies, edge processing, and data analytics have greatly enhanced the reliability and efficiency of emergency alert systems.

Despite these advancements, several challenges remain, particularly in areas such as user privacy, device interoperability, energy efficiency, and affordability. Addressing these concerns is critical for ensuring the large-scale adoption and trustworthiness of such systems. Moreover, the inclusion of explainable AI and blockchain technologies can provide greater transparency and security in managing personal data, while federated learning approaches can personalize safety responses without compromising user confidentiality.

Ultimately, IoT-enabled safety ecosystems represent more than just technological progress—they embody a societal commitment to empowerment and protection. By fostering continuous innovation and collaboration between technologists, policymakers, and social organizations, future IoT solutions can create safer, smarter, and more inclusive environments for women worldwide.

REFERENCES

[1] ActionAid, "Violence against women and girls".

[2] W. H. Organization, "Violence against women," 2021.

[3] W. E. Forum, "Gender Inequality," 2020.

[4] Gurubani Gulati, Dr. Satinder Singh, "Modern Era and Security of Women: An Intellectual Device," International Research Journal of Engineering and Technology (IRJET), 2020.

[5] Ms. K. Opika, Ms. C. Shilpa Rao, "An Evolution of women safety system: A literature review," An International Bilingual Peer Reviewed Peered Research Journal, 2020.

[6] B.Sindhu Bala, M.Swetha, M. Tamilasari, D.Vinodha, "Survey On women safety using IoT," International Journal of Computer Engineering in Research Trends, 2018.

[7] Shivani Ahir; Smit Kapadia; Jigar Chauhan; Nidhi Sanghavi, "The Personal Stun-A Smart Device For Women's Safety," in International Conference on Smart City and Emerging Technology (ICSCET), 2018.

[8] Agrima Agrawal, Ankita Maurya, Prof. Amruta Patil, "Voice Controlled tool for anytime safety of women," journal of emerging technology and Innovative tool, 2021.

[9] Navya R Sogi, Priya Chatarjee, UNethra, V Suma, "SMARISA: A Raspberry Pi based Smart Ring for Women Safety Using IoT".

[10] Wasim Akram, Mohit JainC. , Sweetlin Hemalatha, "Design of a Smart Safety Device for Women using IoT," Procedia of Computer Science, 2019.

[11] B. Sathyasri, U. Jaishree Vidhya, G. V. K. Jothi Sree, T. Pratheeba, K. Ragapriya, "Design and Implementation of Women Safety based on IoT technology," International Journal of Recent Technology and Engineering (IJRTE, 2019.

[12] Aleksandr Ometov, Elena Simona Lohana, "A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges," Computer Networks, 2021.

[13] Raja, S. Pravinth; Rachel, S. Sheeba; R, Sapna, "Women's Safety with a Smart Foot Device," in 2021 4th International Conference on Computing and Communications Technologies (ICCCT), 2021.

[14] T. Sowmya, D. Treevani, D. Keerthana, A Vasantha Laxmi, "women' safety system using IoT," International research journal of engineering and technology, 2020.

[15] Aishwarya, "IoT Based Smart Security Gadget for Women's Safety," in 2019 1st International Conference on Advances in Information Technology (ICAIT), 2019.

[16] Sumanth Pagadala, Lakshmi Prasanna, Anusha Reddy, "A Novel ML- Supported IoT Device for Women Security," International Research Journal Of Engineering and Technology(IRJET), 2021.

[17] Muskan, Teena; Khandelwal, Manisha; Pandey, Purnendu Shekhar, "Women Safety Device Designed Using IoT andMachine Learning," in 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, 2018.

[18] A.Jesudoss, "Smart Solution for Women Safety Using IOT," International Journal of Pure and Applied Mathematics, 2019.

[19] Prottasha Ghosh, Emran Hasan, "Smart Security Device for Women Based on IoT Using Raspberry Pi," in 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), DHAKA, Bangladesh, 2021.

[20] Seth, Debojyoti; Chowdhury, Ahana; Ghosh, Shreya, "A Hidden Markov Model and Internet of Things Hybrid Based Smart Women Safety Device," in 2nd International Conference on Power, Energy and Environment: Towards Smart Technology (ICEPE), 2018.