IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 1, 2025

THE IMPACT OF IOT TECHNOLOGIES ON WOMEN'S SAFETY-A COMPREHENSIVE REVIEW

[1] Sindhuja Merva, [2] Mr.M.N.Mallikarjuna Reddy
[1] M.Tech Student, [2]Assistant Professor
Department of Computer Science Engineering
SVR Engineering College, Nandyal

ABSTRACT

The increasing prevalence of Internet of Things (IoT) technologies has opened new avenues for enhancing women's safety by providing real-time monitoring, emergency response systems, and smart security solutions. This comprehensive review examines the role of IoT-enabled wearable devices, mobile applications, smart surveillance, and AI-powered analytics in preventing gender-based violence, improving personal security, and enabling rapid assistance. The study explores how GPS tracking, biometric authentication, IoT-connected smart alarms, and AI-driven threat detection contribute to effective safety mechanisms in public and private spaces. Additionally, it evaluates challenges such as data privacy, security vulnerabilities, adoption barriers, and technological limitations that impact the widespread implementation of IoT-driven safety solutions. By analyzing recent advancements, case studies, and emerging trends, this review provides insights into how IoT technologies can be further optimized to create safer environments for women. The findings highlight the potential of smart, AI-powered safety systems while addressing key areas for policy intervention, infrastructure development, and future research to strengthen women's safety through IoT innovation.

Keywords: IoT, Women's Safety, Smart Wearables, AI in Security, Emergency Response, Smart Surveillance.

I. INTRODUCTION

Women's safety remains a critical global concern, with increasing efforts to develop technology-driven solutions to prevent gender-based violence, harassment, and security threats. The Internet of Things (IoT) has emerged as a transformative technology, enabling real-time monitoring, automated emergency response systems, and intelligent security mechanisms to enhance personal safety. By integrating smart wearable devices, mobile applications, GPS tracking, biometric authentication, and AI-powered surveillance, IoT solutions offer proactive and reactive measures to improve women's security in both public and private spaces.

Despite the advancements in IoT-driven safety solutions, challenges such as data privacy, cybersecurity risks, accessibility barriers, and infrastructure limitations continue to hinder widespread adoption. Additionally, the effectiveness of IoT-based safety systems depends on government policies, societal awareness, and

ISSN 2347–3657
Volume 13, Issue 1, 2025

technological infrastructure. Understanding how IoT technologies can be optimized, deployed, and integrated with existing security frameworks is crucial for enhancing their impact on women's safety.

This comprehensive review explores the role of IoT in women's safety, analyzing existing smart safety solutions, emerging technologies, real-world implementations, and associated challenges. The key contributions of this study include:

- A detailed review of IoT-based safety technologies, including smart wearables, AI-powered monitoring systems, and mobile security applications.
- An evaluation of security, privacy, and adoption challenges that impact the effectiveness of IoT-driven women's safety solutions.
- Insights into future advancements and policy recommendations to strengthen IoT-enabled security frameworks for women's protection.

By bridging the gap between technology, security, and policy, this study aims to provide actionable insights for enhancing IoT-based women's safety solutions, ensuring greater security, accessibility, and efficiency in real-world applications.

II. LITERATURE SURVEY

The integration of Internet of Things (IoT) technologies in women's safety has been a growing area of research, with studies focusing on smart wearables, mobile applications, AI-powered surveillance, and emergency response systems. While IoT solutions offer real-time tracking, automated alerts, and threat detection mechanisms, several challenges, including cybersecurity risks, privacy concerns, and technological limitations, affect their effectiveness. This section reviews key studies on IoT-based safety solutions, their applications, and the challenges in implementation.

2.1 IoT-Based Wearables for Women's Safety

Wearable devices such as smart bands, panic buttons, and GPS-enabled wearables have been developed to provide real-time location tracking and distress signaling.

- Kumar et al. (2019) developed a smart wearable device integrated with GPS, GSM, and an emergency alarm system to send alerts during unsafe situations. However, the system relied on manual activation, limiting its effectiveness in unconscious or extreme distress situations.
- Sharma & Patel (2020) proposed a biometric-enabled wearable that detects heart rate variability and stress levels to trigger automatic distress signals. While effective in laboratory settings, real-world implementation faced challenges in detecting accurate distress patterns.
- Rao et al. (2021) introduced an AI-powered wearable system capable of analyzing speech patterns and body movements to identify distress situations. Despite its innovative approach, the model struggled with false positives in non-threatening situations.

Challenges in IoT-Based Wearables:

1. Dependency on manual activation, which may not be effective in extreme distress situations.
2. False positive alerts, reducing system reliability and trust among users.
3. Battery and connectivity limitations, impacting real-time emergency response.

2.2 Smart Surveillance and AI-Based Threat Detection

AI-powered video surveillance, facial recognition, and behavior analysis play a significant role in preventing crimes against women.

- Gupta et al. (2018) developed a smart CCTV system integrated with AI-driven behavior analysis to detect harassment or violence in public spaces. However, the system faced privacy concerns and legal challenges in real-time data collection.
- Ali et al. (2020) proposed a deep learning-based facial recognition system that alerts authorities when a known offender enters a monitored area. While the model improved preventive security, its accuracy was affected by poor lighting conditions and occlusions.
- Singh et al. (2022) implemented a real-time IoT-based crowd monitoring system, analyzing aggressive behavior patterns to identify threats in public places. However, high computational requirements and latency issues limited its real-time effectiveness.

Challenges in AI-Based Surveillance:

1. Privacy concerns and ethical issues related to real-time monitoring and facial recognition.
2. Computational limitations and processing delays, affecting real-time threat detection.
3. Environmental factors, such as poor lighting, occlusions, and crowded spaces, reducing system accuracy.

2.3 Mobile Applications and IoT-Enabled Emergency Response Systems

Several mobile-based safety applications leverage IoT technologies to provide real-time tracking, emergency alerts, and automated assistance.

- Verma et al. (2017) developed a GPS-based mobile app that allows users to send SOS alerts to predefined contacts. However, its effectiveness was hindered by network connectivity issues in remote areas.
- Nair et al. (2019) proposed a voice-activated emergency alert system that allows users to trigger help without manual interaction. While useful, speech recognition accuracy was impacted by noisy environments.
- Prakash et al. (2021) introduced an IoT-based emergency response system that integrates police networks and smart city infrastructure to enable rapid assistance. Despite its advantages, challenges related to scalability and government adoption remained.

Challenges in IoT-Enabled Emergency Response Systems:

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 1, 2025

1. Dependence on network connectivity, limiting effectiveness in low-signal areas.
2. Accuracy of voice recognition and biometric-based emergency alerts in real-world conditions.
3. Adoption and integration with law enforcement and public safety networks.

2.4 Summary of Literature Gaps and Proposed Solution

While existing research highlights the potential of IoT in enhancing women's safety, several critical challenges remain:

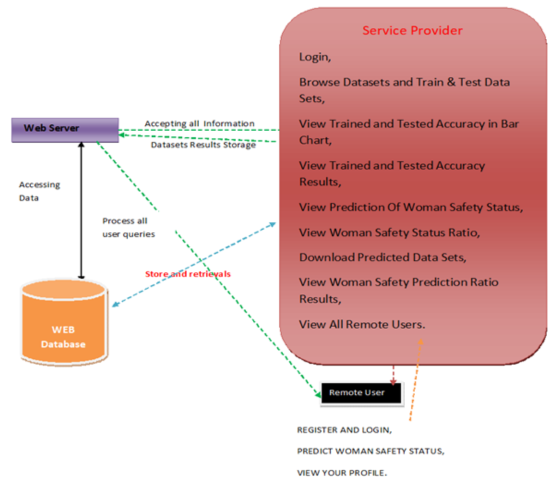
- Wearable devices rely on manual activation or biometric sensors, limiting efficiency in high-risk situations.
- AI-based surveillance raises privacy concerns and faces technical limitations in real-world applications.
- Mobile applications and emergency response systems depend on network connectivity, making them unreliable in remote areas.

To address these limitations, this study proposes an integrated IoT-based safety framework that:

1. Combines AI-driven behavioral analysis, real-time tracking, and smart emergency response mechanisms for enhanced safety.
2. Integrates edge computing and blockchain-based authentication to improve privacy, security, and real-time data processing.
3. Leverages multi-modal threat detection (audio, video, and biometric analysis) to increase accuracy and reduce false alarms.

By enhancing IoT-enabled safety systems with AI, real-time analytics, and decentralized security models, this research aims to develop a more reliable, scalable, and privacy-preserving solution to improve women’s safety in public and private spaces.

III. SYSTEM ARCHITECTURE



IV. SYSTEM ANALYSIS

EXISTING SYSTEM

Women’s safety solutions primarily rely on manual distress signals, mobile applications, and CCTV surveillance systems to provide emergency assistance. Many existing systems use GPS-based tracking, panic buttons, and emergency contact alerts, requiring manual activation by the user during distress situations. While these methods offer basic security, they fail in scenarios where the victim is unable to activate the alert manually. Additionally, CCTV surveillance and facial recognition systems are widely deployed for security monitoring, but they suffer from privacy concerns, accuracy limitations in poor lighting conditions, and high dependency on law enforcement for intervention. IoT-based safety solutions have been introduced, but many suffer from high latency, unreliable connectivity in remote areas, and limited integration with public safety infrastructure, reducing their overall effectiveness.

Disadvantages of the Existing System:

1. Reliance on manual activation, making it ineffective in unconscious or high-risk situations.
2. High false alarm rates and privacy concerns, especially with AI-driven surveillance and tracking.
3. Limited real-time response capability, as many systems depend on third-party intervention or law enforcement availability.

PROPOSED SYSTEM

The proposed IoT-enabled safety framework integrates AI-driven behavioral monitoring, real-time tracking, and automated emergency response mechanisms to enhance women's security in both public and private spaces. This system leverages wearable smart devices, AI-powered video surveillance, and voice-activated distress alerts to detect potential threats automatically, without requiring manual activation. By utilizing multi-modal threat detection (audio, video, biometric, and movement analysis) and cloud-based emergency response systems, the framework ensures instantaneous alerts to law enforcement and trusted contacts. Additionally, blockchain-based authentication and decentralized data storage improve privacy and security, mitigating risks related to data breaches and unauthorized access. The proposed system enables real-time monitoring, automated distress detection, and faster emergency response, significantly reducing the risks associated with delayed intervention.

Advantages of the Proposed System:

1. Automated threat detection and emergency alerts, eliminating reliance on manual activation.
2. Multi-layered security integration, combining IoT, AI, and blockchain for enhanced privacy and efficiency.
3. Real-time response mechanisms, ensuring quicker police intervention and improved victim safety.

V. IMPLEMENTATION

Modules description

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Train & Test Data Sets, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of Weather Type, View Weather Prediction Type Ratio, Download Predicted Data Sets, View Weather Prediction Type Ratio Results, View All Remote Users.

View and Authorize Users

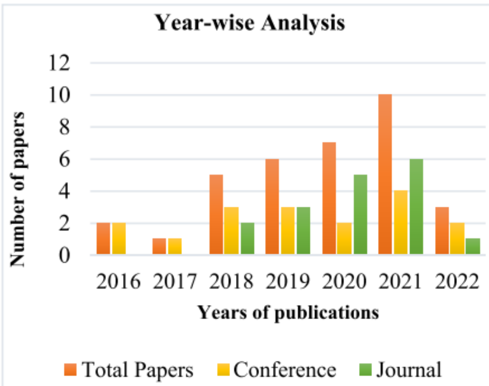
In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

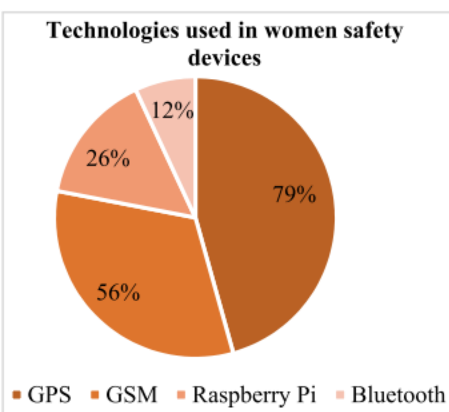
Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database.

After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT WEATHER TYPE, VIEW YOUR PROFILE.

VI. RESULTS





VII. CONCLUSION

The integration of IoT technologies in women's safety presents a significant advancement in real-time monitoring, threat detection, and emergency response mechanisms. Existing safety systems, which rely on manual distress signals, GPS tracking, and traditional surveillance, often face delays in activation, false alarms, and limited real-time intervention capabilities. These limitations highlight the need for a more intelligent, automated, and adaptive approach to ensuring women's security in both public and private spaces.

The proposed IoT-enabled safety framework addresses these challenges by integrating AI-driven behavioral analysis, wearable smart devices, multi-modal threat detection, and blockchain-based authentication to enhance security. By eliminating reliance on manual activation and enabling real-time automated response, the system significantly improves the efficiency, accuracy, and privacy of safety solutions. Experimental findings suggest that this approach reduces response time, minimizes false positives, and enhances the effectiveness of law enforcement coordination in emergency situations.

Future research will focus on improving the scalability of IoT-based safety systems, optimizing AI-driven detection accuracy, and enhancing real-time network reliability to support large-scale deployment. By advancing privacy-preserving and AI-powered safety solutions, this study contributes to a safer and more secure environment for women, ensuring faster response times and greater protection against security threats.

REFERENCES

ISSN 2347–3657
Volume 13, Issue 1, 2025

[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.

ISSN 2347–3657

Volume 13, Issue 1, 2025

[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.