

# AI-Enabled Predictive Systems for Women Safety in Smart Cities

Dr. Nitin Mishra., Dr. Rohit

CSE, PIET, Parul University Parul University Vadodara, India

DOI: <https://doi.org/10.51584/IJRIAS.2026.11030075>

Received: 04 March 2026; Accepted: 09 March 2026; Published: 12 April 2026

## ABSTRACT

Recent progress in Artificial Intelligence (AI) has made it possible to create smart systems that make smart cities safer for women. This paper offers an extensive evaluation of current AI-driven predictive frameworks, emphasizing their functionalities, constraints, and prospective advancements in proactive threat identification and mitigation. The review looks at a number of different methods, such as surveillance systems based on deep learning, gesture and voice recognition techniques, predictive crime mapping, mobile safety apps, and WiFi-based models for recognizing human activity. Research that combines technologies like YOLO, Res Net, Open Pose, BiL STM, and CNN-GRU shows that it is possible to find distress signals, suspicious behavior, and environmental risks in real time. The paper additionally discusses about how smart infrastructure solutions like intelligent street lighting, geospatial safety analytics platforms, and crowdsourced safety scoring systems can make cities safer for women. There are also talks about privacy-preserving machine learning and explainable AI frameworks to deal with ethical and transparency issues that come up with large-scale surveillance systems. The paper identifies important research gaps based on the literature that was reviewed. These gaps include the need for unified multimodal systems, zero-device safety mechanisms, and better integration with smart city infrastructure. The study concludes that AI-driven predictive systems, when integrated with ethical safeguards and urban planning strategies, can substantially improve women's security, emergency responsiveness, and inclusivity in forthcoming smart cities.

**Index Terms:** Women's Safety, Deep Learning, Predictive Policing, Explainable AI, Smart Cities, Gesture Recognition, Zero-Device Safety. or wearable device. These advanced systems use Computer Vision, the Internet of Things (IoT), and multimodal analytics to look at complicated behavioral and environmental signals.

- **Automated Threat Recognition:** Using deep learning models like YOLOv8 and ResNet-50, systems can now find weapons, spot lone women in dangerous areas, and analyze crowd density to detect possible mob situations [18].
- **Gesture and Audio Analytics:** AI is trained to recognize SOS hand signals, defensive body language (such as crossing arms or freezing), and sounds of panic, including screams or sudden changes in voice tone [19].
- **Predictive Policing:** AI examines past crime data and environmental factors like lighting and isolation to generate "threat scores" and dynamic heatmaps. This enables police to allocate resources to high-risk areas proactively [20].

These technologies are getting better to deal with ethical issues as they become part of larger smart city systems, like smart street lighting and Integrated Command and Control Centers (ICCCs). There are new unified frameworks being made to bring together Explainable AI (XAI) and Privacy-Preserving Machine Learning (PPML). This is to make sure that the push for more safety doesn't put people's privacy or data security at risk. [21]

## INTRODUCTION

Keeping women safe in both public and private spaces is still a major global problem that has a big effect on their ability to move around, work, and get opportunities. Passive CCTV surveillance and manual panic buttons are examples of traditional security measures that have mostly been reactive. They only respond after an

incident has happened or require the victim to actively trigger an alert, which is often impossible in high-stress situations. To fix these problems, new technologies have made it possible to create proactive safety systems that use Artificial Intelligence (AI) and Deep Learning to find threats in real time and stop them before they get worse. This move toward AI-driven safety focuses on "zero-device" solutions, which means that the environment itself watches for distress without the victim having to use a smartphone

### Related work

The paper highlighting the potential for creating a secure and self-sustaining infrastructure. The paper concludes by highlighting the need for strong regulatory frameworks, ethical oversight, and public participation to ensure that the power of AI is used responsibly and that smart cities are safe, inclusive, and consistent with the values of the communities they serve. [1]

The paper introduces a unified framework that integrates Explainable Artificial Intelligence (XAI) with Privacy-Preserving Machine Learning (PPML) to address the dual challenges of transparency and data privacy in real-time decision-making systems. The study demonstrates that by employing federated learning, homomorphic encryption, and interpretable models like SHAP, the framework achieves significant improvements in interpretability and privacy adherence without compromising the computational efficiency required for sectors such as healthcare and energy optimization. [2]

The paper presents a proactive, AI-driven threat detection framework designed to enhance women's safety in urban environments by utilising deep learning models like YOLOv8 and ResNet-50 to analyse live surveillance feeds for distress signals. The system features "zero-device" safety through multimodal analytics, capable of recognising specific SOS gestures and auditory signs of panic, while leveraging edge computing to ensure real-time alerts even in low-connectivity areas. [3]

The study evaluates deep learning architectures, specifically analyse historical data to generate dynamic heatmaps, thereby enabling law enforcement to deploy resources strategically to high-risk zones. [4]

The paper proposes a multi-layered safety system that combines a mobile application with AI-driven computer vision to detect weapons and record evidence in real-time, aiming to address the limitations of existing reactive safety tools. The system integrates GPS tracking, emergency alerts, and cloud-based evidence storage to ensure quick police intervention and prevent evidence tampering, offering a holistic preventive mechanism for women's security. [5]

BiLSTM and CNN+GRU models, for Human Activity Recognition (HAR) using WiFi Channel State Information (CSI) to enable non-intrusive monitoring without wearable sensors. The findings indicate that while CNN+GRU models excel in extracting spatial features for accuracy, BiLSTM models are superior for capturing temporal dependencies in high-resolution data, highlighting their potential applications in healthcare and smart home automation. [6]

The article explores the critical role of smart street lighting in fostering safer and more inclusive urban spaces for women, citing studies that link improved illumination to a significant reduction in violent crimes and harassment. It argues that beyond utility, intelligent lighting serves as a tool for empowerment, enabling women to navigate public spaces with confidence and participate more fully in the workforce and community life. [7]

The entry describes Safetipin as a social organisation that leverages technology and mobile applications to collect data on urban safety parameters, such as lighting and visibility, to generate safety scores for neighbourhoods and routes. It details how this crowdsourced data informs users' mobility decisions and guides government interventions to fix infrastructure gaps, thereby making public spaces more inclusive for women. The report introduces the "She RISES" assessment framework, developed to evaluate the gender responsiveness of Indian cities across five pillars, including policy, infrastructure, The article details a comprehensive AI-powered analytics system that shifts women's safety measures from reactive responses to proactive threat detection by monitoring real-time interactions and identifying suspicious behavioural patterns. It highlights the integration of gesture and voice-activated distress signals, alongside predictive crime mapping tools that mobility, services,

and response to violence. By pilot-testing this framework in six smart cities, the study highlights the importance of integrating gender-disaggregated data and the "care economy" into urban planning to build cities that are responsive, inclusive, safe, and equitable for women. [7]

The briefing note provides a comprehensive framework for addressing Violence Against Women and Girls (VAWG) through infrastructure and urban programming, identifying key entry points such as transport, energy, and water services to mitigate risks. It emphasizes the economic cost of violence and outlines strategies for creating safe spaces, arguing that infrastructure projects must go beyond basic compliance to empower women and transform social norms. [8]

Table I AI-Enabled Predictive Systems and Their Applications

System/work	Frame-work	Key Technologies	Uses and Applications
Unified PPML Framework	XAI &	Federated Learning, Homomorphic Encryption, SHAP	<b>Healthcare:</b> Predicting cardiovascular disease risk using anonymized data [1,2]. <b>Energy:</b> Forecasting household demand patterns.
AI-Driven Time Detection	Real-Threat	YOLOv8, ResNet-50, LSTM	<b>Threat Detection:</b> Identifying high-risk scenarios and SOS gestures [3]. <b>Alerts:</b> Environmental-based predictive warnings [4].
Women Safety Analytics System		Deep Learning, OpenPose	<b>Crime Mapping:</b> Highlighting risk-prone areas [5]. <b>Behavior Analysis:</b> Detecting suspicious activity [6].
WiFi-Based HAR		BiLSTM, CNN+GRU, CSI, WiFi	<b>Healthcare:</b> Fall detection and anomaly monitoring [7]. <b>Smart Homes:</b> Predictive automation
Safetipin		Geospatial Analysis, Crowdsourcing	<b>Route Safety Scoring:</b> risk assessment [8]. <b>Infrastructure:</b> Identifying dark spots [9,10].
AI-Powered Mobile Safety System		Machine Learning, Weapon Detection	<b>Crime Prevention:</b> Real-time weapon detection [11,12]. <b>Risk Analysis:</b> Monitoring odd-hour activities.

### Research findings

The diagram 1 highlights core AI innovations that can be applied to women’s safety systems. Each component contributes to building an intelligent, proactive, and responsive safety ecosystem.

#### A. Autonomous Threat Detection

AI systems can automatically identify potential danger without human intervention. For women’s safety, this includes:

- Detecting suspicious behavior through CCTV or wearable devices
- Recognizing distress signals such as screams, abnormal movement, or panic gestures

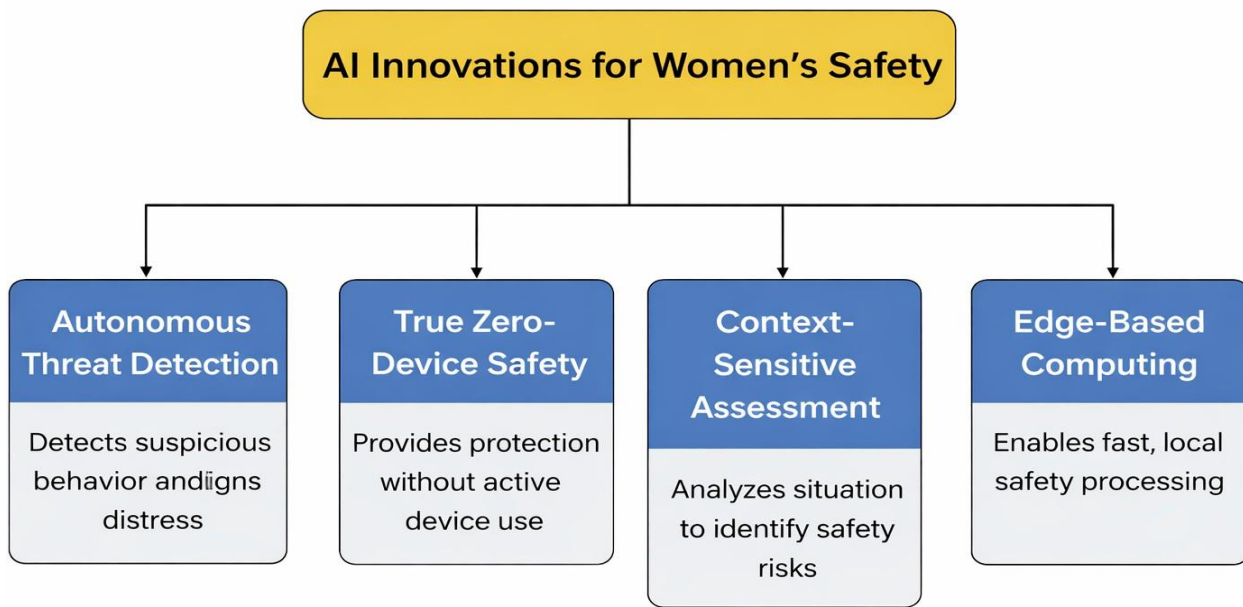


Fig. 1. AI Innovations for Women's Safety Block Diagram

- Sending real-time alerts to authorities or trusted contacts [9]

**Example:** A smart mobile application that detects sudden running, shaking, or shouting and triggers an emergency alert.

**B. True Zero-Device Safety**

This concept ensures safety even when the individual does not actively use a device. Applications include:

- Smart city surveillance systems recognizing unsafe situations in public areas
- AI-enabled street cameras detecting harassment or stalking behavior
- Public transport monitoring systems ensuring passenger safety [10]

**Goal:** Protection should not depend solely on the victim pressing an emergency button.

**C. Context-Sensitive Assessment**

AI systems analyze the surrounding situation and environment rather than relying only on raw data. This enables:

- Distinguishing between normal interaction and aggressive behavior
- Identifying high-risk locations such as isolated streets or late-night travel routes
- Providing personalized safety recommendations based on time, location, and user habits [11]

**Example:** AI warning a user — “This area has low lighting and low activity. Consider a safer route.”

### D. Edge-Based Computing

In this approach, processing occurs directly on the device (mobile phone, wearable, or smart camera) instead of cloud servers. Benefits include:

- Faster emergency response due to reduced latency [12]
- Improved privacy protection since data remains local
- Functionality in low or no network connectivity environments [13]

**Example:** A smartwatch detecting distress and sending an SOS alert instantly without requiring internet connectivity.

### Future Developments in AI-Based Women’s

#### Safety Systems

The figure illustrates the potential future advancements in AI-driven women’s safety solutions, highlighting emerging technologies that can significantly enhance protection, monitoring, and emergency response mechanisms.

**Smart City Infrastructure Integration** focuses on connecting AI safety systems with urban infrastructure such as surveillance cameras, street lighting, transportation systems, and emergency response networks. This integration enables real-time monitoring of public spaces and rapid identification of unsafe situations, thereby improving overall public safety. [13]

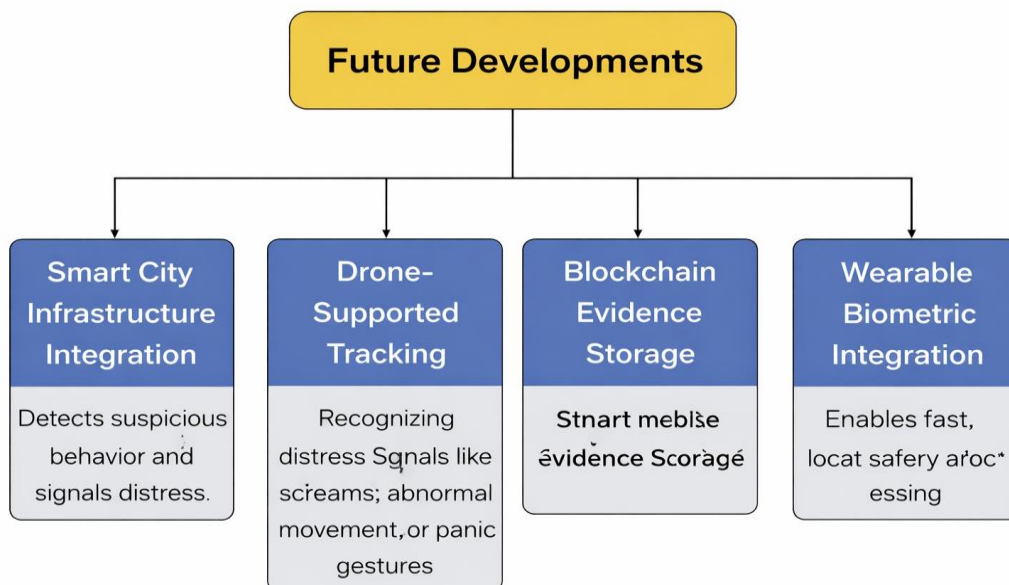


Fig. 2. Future Developments in AI-Based Women’s Safety Systems

**Drone-Supported Tracking** represents the use of autonomous aerial systems to assist in locating individuals in distress situations. Drones equipped with AI-powered vision and tracking algorithms can quickly reach remote or crowded areas, provide situational awareness to authorities, and support rescue operations more efficiently. [14]

**Blockchain Evidence Storage** introduces secure and tamper-proof storage of safety-related data such as incident reports, video recordings, and emergency alerts. Blockchain technology ensures data integrity, transparency, and legal reliability, which can be crucial for investigations and judicial processes. [15]

**Wearable Biometric Integration** emphasizes the use of smart wearable devices capable of monitoring physiological parameters such as heart rate, stress levels, and movement patterns. AI algorithms can analyze these biometric signals to detect distress conditions and automatically trigger alerts without requiring manual intervention. [16]

Overall, these future developments aim to create a comprehensive, intelligent, and proactive safety ecosystem that combines advanced technologies with real-world infrastructure to enhance women's security, emergency responsiveness, and trust in safety systems.

## REFERENCES

1. N. Mishra, "Dataset Segmentation for Cloud Computing and Securing Data Using ECC," *IJCSIT: International Journal of Computer Science and Information Technologies*, vol. 5, no. 3, pp. 4210–4213, 2014.
2. S. Chaturvedi, V. Mishra, and N. Mishra, "Sentiment Analysis using Machine Learning for Business Intelligence," in *Proc. IEEE Int. Conf. Power, Control, Signals & Instrumentation Engineering (ICPCSI)*, 2017.
3. N. K. Mishra, V. Mishra, and S. Chaturvedi, "Solving cold start problem using MBA," in *Proc. IEEE Int. Conf. Power, Control, Signals & Instrumentation Engineering (ICPCSI)*, pp. 1598–1601, 2017.
4. N. Mishra, S. Chaturvedi, A. Vij, and S. Tripathi, "Research problems in recommender systems," *Journal of Physics: Conference Series*, vol. 1717, no. 1, p. 012002, 2021.
5. S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Pearson, 2021.
6. M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep Learning for IoT Big Data and Streaming Analytics: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2923–2960, 2018.
7. [A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.
8. [Y. Liu, X. Ma, L. Shu, G. P. Hancke, and A. M. Abu-Mahfouz, "From Industry 4.0 to Agriculture 4.0: Current Status, Enabling Technologies, and Research Challenges," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4322–4334, 2021.
9. J. Chen and X. Ran, "Deep Learning With Edge Computing: A Review," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1655–1674, 2019.
10. [K. Rose, S. Eldridge, and L. Chapin, "The Internet of Things: An Overview," *Internet Society (ISOC)*, 2015.
11. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
12. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," *Applied Innovation Review*, no. 2, pp. 6–19, 2016.
13. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," *arXiv preprint arXiv:1608.05187*, 2016.
14. Restas, "Drone Applications for Supporting Disaster Management," *World Journal of Engineering and Technology*, vol. 3, pp. 316–321, 2015.
15. P. Voigt and A. Von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer, 2017.
16. J. Yang, J. Stankovic, S. Stankovic, and K. Qian, "A Survey of Wearable Sensors and Systems with Application in Rehabilitation," *Journal of NeuroEngineering and Rehabilitation*, vol. 11, no. 1, 2014.
17. M. Patel and J. Wang, "Applications, Challenges, and Prospective in Emerging Body Area Networking Technologies," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 80–88, 2010.
18. N. Ma, X. Zhang, H. Zheng, and J. Sun, "Privacy-Preserving AI in Smart Healthcare: Challenges and Opportunities," *IEEE Access*, vol. 8, pp. 122076–122094, 2020.
19. Albahri et al., "IoT-Based Smart Healthcare Monitoring Systems: A Systematic Review," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 105–138, 2021.
20. J. Redmon et al., "You Only Look Once: Unified, Real-Time Object Detection," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, pp. 779–788, 2016.
21. K. He et al., "Deep Residual Learning for Image Recognition," in *Proc. IEE Conf. Computer Vision and*

- Pattern Recognition (CVPR), pp. 770–778, 2016.
22. T. Nishimura et al., “Human Behavior Recognition for Surveillance Systems Using Deep Learning,” *IEEE Access*, vol. 7, pp. 135678–135688, 2019.
  23. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet Classification with Deep Convolutional Neural Networks,” *Communications of the ACM*, vol. 60, no. 6, pp. 84–90, 2017.
  24. Schölkopf et al., “Support Vector Method for Novelty Detection,” in *Advances in Neural Information Processing Systems (NeurIPS)*, 2000.
  25. H. Haddadi et al., “Privacy Analytics,” *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 2, pp. 94–98, 2012.
  26. Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated Machine Learning: Concept and Applications,” *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, 2019.
  27. W. Shi and S. Dustdar, “The Promise of Edge Computing,” *Computer*, vol. 49, no. 5, pp. 78–81, 2016.
  28. S. S. Intille, “A New Research Challenge: Persuasive Technology to Motivate Healthy Aging,” *IEEE Transactions on Information Technology in Biomedicine*, vol. 8, no. 3, pp. 235–237, 2004.
  29. M. A. Goodrich et al., “Supporting Wilderness Search and Rescue Using a Camera-Equipped Mini UAV,” *Journal of Field Robotics*, vol. 25, no. 1–2, pp. 89–110, 2008.