**Case Study ID: SIH1605**

**1. Title: Women Safety Analytics Using Network Solutions**

**2. Introduction :**

Women’s safety is a significant concern in India, particularly in urban areas where the threat of harassment and violence is prevalent. To address these challenges, Bharat Electronics Limited (BEL), a state-owned aerospace and defense company, developed a Women Safety Analytics System leveraging advanced networking and analytical technologies. This system aims to provide real-time monitoring, alerting, and response mechanisms to protect women from safety threats in public spaces.

* Overview: The Women Safety Analytics System developed by BEL integrates various technologies, including IoT (Internet of Things) devices, networked surveillance systems, AI-driven analytics, and communication networks. The system is designed to monitor public spaces, identify potential safety threats, and facilitate rapid response by law enforcement agencies.
* Objective: The primary objective of the Women Safety Analytics System developed by Bharat Electronics Limited (BEL) is to enhance the safety and security of women in urban areas by leveraging advanced networking, IoT, and analytical technologies to enable real-time monitoring, early threat detection, and prompt response to potential safety threats in public spaces.

**3. Background**

* Organization/System /Description: Bharat Electronics Limited (BEL) has developed a Women Safety Analytics System to enhance safety for women in urban areas. The system integrates high-definition surveillance cameras, IoT devices like GPS-enabled wearable pendants, and AI-driven analytics to monitor public spaces. AI algorithms analyze video feeds in real-time to detect suspicious behaviors, triggering alerts to a central monitoring hub. The system also includes a mobile app for users to check route safety and report incidents. Robust communication networks ensure real-time data transmission, while privacy and network reliability are safeguarded through encryption and redundant networks.
* Current Network Setup: The current network setup for the BEL Women Safety Analytics System

includes the following key components:

* High-Speed Internet Connectivity: Enables real-time transmission of large volumes of video data from surveillance cameras to the central monitoring hub.
* Secure VPNs: Virtual Private Networks (VPNs) secure communications between IoT devices, cameras, and the monitoring hub, protecting data from unauthorized access.
* Redundant Networks: Multiple network paths ensure continuous operation, with backups in place to prevent downtime in case of network failures.

**4. Problem Statement**

* Challenges Faced: Despite various efforts by law enforcement agencies, women continue to face safety risks, especially in urban environments. Incidents of harassment, stalking, and assault are often underreported due to a lack of immediate response mechanisms. There is a need for a robust, technology-driven solution that can monitor public spaces, detect potential threats, and alert authorities in real time to prevent or respond to incidents effectively.

**5. Proposed Solutions**

* Approach
* Technologies/Protocols Used

**6. Implementation**

* Process: Networked Surveillance Cameras:
* - High-definition CCTV cameras with network connectivity are installed in strategic locations across urban areas. These cameras are connected to a central monitoring system via a secure, high-speed network.

* IoT Devices:
* - Wearable devices, such as smart pendants or bracelets equipped with GPS and panic buttons, are provided to women. These devices can send distress signals when activated, providing real-time location data to the monitoring system.
* Implementation: BEL initiated a pilot program in a major Indian city, focusing on areas with high foot traffic, such as markets, public transport hubs, and educational institutions. The pilot involved installing surveillance cameras and deploying IoT devices to volunteers. The data from these devices were fed into the central monitoring hub for analysis.
* Data Analytics and Threat Detection
* The AI-powered analytics system processed the video feeds and data from IoT devices in real time. It identified patterns indicative of potential threats, such as a person being followed for an extended period or sudden crowding around an individual. Upon detecting such patterns, the system automatically triggered alerts to the monitoring hub.
* Response Mechanism
* When a threat was detected, the system provided real-time alerts to the central monitoring hub. The operators could then assess the situation through live video feeds and take appropriate action, such as dispatching police officers to the location or contacting the woman through her

IoT device. The system also allowed for automated notifications to be sent to local law enforcement agencies, reducing response times.

* Timeline: BEL is exploring ways to enhance the system by incorporating additional features such as predictive analytics, broader IoT device integration, and expanding the network to cover more areas. The goal is to create a scalable, nationwide system that can be adapted to different environments and needs, ultimately contributing to a safer society for women.

**7. Results and Analysis**

* Outcomes: The Women Safety Analytics System was highly effective during the pilot phase. Key outcomes included:
* - Reduction in Incidents: There was a noticeable decrease in reported incidents of harassment and assault in areas covered by the system, attributed to the increased surveillance and rapid response capabilities.
* - Increased Public Confidence: Women in the pilot areas reported feeling safer, knowing that help was available at the press of a button and that potential threats were being actively monitored.
* - Positive Law Enforcement Feedback: Local police found the system to be a valuable tool in preventing and responding to crimes against women, leading to discussions about expanding the program to other areas.
* Analysis: The system was designed to be modular, allowing for incremental scaling by adding more cameras, IoT devices, and processing power as needed.

**8. Security Integration**

* Security Measures: High-Speed Internet Connectivity: Ensures that large volumes of video data can be transmitted in real time.
* - Secure VPNs: Virtual Private Networks (VPNs) are used to secure communications between the various components of the system, protecting data from interception.
* - \*Redundant Networks: To prevent downtime, the system uses redundant network paths, ensuring that if one network fails, another can take over without disrupting operations.
* - \*Edge Computing: Some data processing is done at the edge (closer to the data source) to reduce latency and ensure faster response times.

**9. Conclusion**

* Summary: Bharat Electronics Limited’s Women Safety Analytics System is an innovative use of network technologies, IoT devices, and AI-powered analytics to address the critical issue of women’s safety in urban areas. By leveraging advanced networking solutions, BEL has created a system that not only detects and prevents potential threats in real time but also empowers
* women to take control of their safety. The success of the pilot program highlights the potential for broader implementation, making public spaces safer for women across the country.
* Recommendations: BEL is exploring ways to enhance the system by incorporating additional features such as predictive analytics, broader IoT device integration, and expanding the network to cover more areas. The goal is to create a scalable, nationwide system that can be adapted to different environments and needs, ultimately contributing to a safer society for women

**10. References**

**Citations: Reference Research papers**

**Industry Articles on Women’s Safety Technology**

**Research Papers on IoT and AI in Public Safety**

**NAME: AMBATI NISSI THOMAS**

**ID-NUMBER: 2320030280**

**SECTION-NO: 4**