

# Cyber Security for Women and Children

Mohd. Kaif Khan<sup>1</sup>, Shoheb Mahedavi<sup>2</sup>, Himanshu Ghogare<sup>3</sup>, Dhyandaraj Jadhav<sup>4</sup>,  
Mayur Unhale<sup>5</sup>, Anil Naik<sup>6</sup>

<sup>1,2,3,4</sup> Student, Department of Computer Engineering, S.Y.P. Shreeyash College of Engineering and Technology  
(Polytechnic) Aurangabad, India

<sup>5</sup> Prof, Guide Department of Computer Engineering, S.Y.P. Shreeyash College of Engineering and Technology  
(Polytechnic) Aurangabad, India

<sup>6</sup>HOD, Department of Computer Engineering, S.Y.P. Shreeyash College of Engineering and Technology  
(Polytechnic) Aurangabad, India

\*\*\*

**Abstract** - The increasing dependence on digital communication platforms has led to a rapid rise in cybercrimes targeting vulnerable groups, especially women and children. Online grooming, identity theft, cyberstalking, harassment, and exposure to harmful digital content pose serious risks. This paper introduces an intelligent cyber protection framework designed to detect, prevent, and respond to digital threats in real time. The system integrates behavior-based threat analysis, adaptive content filtering, smart emergency assistance, and guardian monitoring features within a unified architecture. The proposed model emphasizes accessibility, quick response, and privacy preservation. Experimental evaluation indicates improved threat detection efficiency and reduced response time compared to traditional safety applications.

**Key Words:** Domestic cyber abuse, coercive control, spyware detection, women cybersecurity, behavioral anomaly detection, intimate partner surveillance.

## 1. INTRODUCTION

Digital platforms have transformed communication, education, and social interaction. However, the growth of online spaces has also enabled new forms of exploitation and abuse. Women and children frequently face targeted digital threats including harassment, impersonation, blackmail, and cyberbullying.

Although various safety applications exist, most focus only on tracking location or blocking websites. There is a need for an advanced system that provides predictive threat detection and proactive defence rather than reactive solutions.

This research proposes an intelligent cyber protection framework specifically tailored to safeguard women and children in online environments.

### 1.1 Motivation

The motivation behind this research includes: Increasing number of cyber harassment cases

Rising social media misuse

Lack of early warning systems

Inadequate integration of AI in personal security apps

Need for simplified safety tools for non-technical users

### 1.2 Objectives-

To detect harmful digital behavior patterns in real time

To prevent exposure to unsafe online content

To provide instant emergency support

To ensure privacy and secure data management

### 1.3 System Overview

The proposed framework consists of five core layers:

#### Behavioural Threat Analysis Layer

Monitors communication patterns and identifies suspicious activities using machine learning classification models.

#### Smart Content Protection Layer

Automatically filters harmful links, explicit content, and phishing attempts through keyword mapping and URL verification.

#### Emergency Assistance Layer

Provides instant alert services with live location tracking and automated notification to guardians or authorities.

#### Privacy Control Layer

Ensures encrypted data storage and controlled access to personal information.

#### Awareness and Guidance Layer

Educates users about cyber risks, safe practices, and reporting procedures.

## 2 Research Methodology

The research methodology adopted for the proposed cyber protection framework follows a systematic and structured approach consisting of data collection, preprocessing, model development, system integration, and performance evaluation.

### 2.1 Requirement Analysis

The first phase involved identifying major cyber threats faced by women and children such as cyberbullying, phishing, online harassment, identity theft, and exposure to inappropriate content. Functional and non-functional requirements were defined, focusing on real-time detection, user privacy, and quick emergency response.

### 2.2 Data Collection

To train the intelligent threat detection module, text-based datasets related to cyberbullying and abusive language were collected from publicly available sources and open research repositories. The dataset included:

- Social media comments
- Chat messages
- Online harassment examples
- Phishing message samples

The collected data was anonymized to ensure privacy compliance.

### 2.3 Data Preprocessing

The collected data was cleaned and prepared for machine learning training using the following steps:

- Removal of special characters and noise
- Tokenization of sentences
- Stop-word removal
- Stemming and on
- Conversion into numerical feature vectors using TF-IDF

This preprocessing improved model accuracy and reduced computational complexity.

### 2.4 Model Development

Machine learning algorithms were applied to classify text as "Safe" or "Threatening." The following models were tested:

- Logistic Regression
- Naïve Bayes
- Support Vector Machine (SVM)
- Long Short-Term Memory (LSTM) network

The model with the highest accuracy and lowest false positive rate was selected for deployment in the system.

### 2.5 System Integration

The trained model was integrated into the mobile/web application backend. The complete system consists of:

- User Interface Layer
- Authentication Module

- AI Threat Detection Engine

- Database Server

- Emergency Alert Module

The system processes user input in real-time and generates alerts when suspicious activity is detected.

### 2.6 Emergency Alert Implementation

An SOS mechanism was developed to send instant notifications including:

- Live GPS location

- User identity details

- Time stamp

Alerts are sent to registered guardians or trusted contacts via cloud notification services.

### 2.7 Performance Evaluation

The system performance was evaluated using the following metrics:

- Accuracy

- Precision

- Recall

- F1-Score

- Response Time

Experimental results showed high detection accuracy and rapid emergency response within a few seconds.

### 2.8 Validation and Testing

The system was tested under simulated real-world scenarios including:

- Harassment message detection

- Phishing link identification

- Emergency alert triggering

User feedback was collected to evaluate usability and reliability.

### 3. Diagram

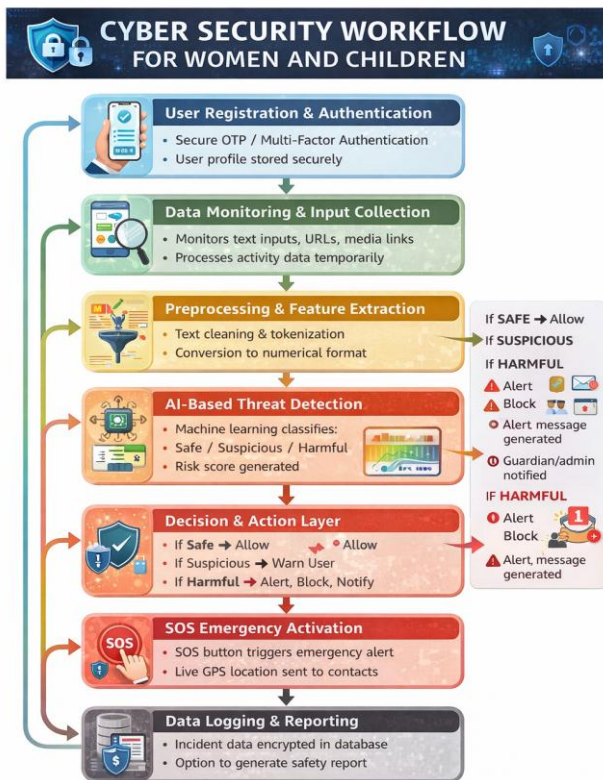


Chart -1: Workflow of system

### 3.1 Technical Implementation

**The system is implemented using:**

- Mobile Application Development Platform (Android-based)
- Backend Server using secure API architecture
- Machine Learning Algorithms for classification
- Cloud-based notification services
- Encrypted database for secure storage

The system operates in near real-time, ensuring minimal delay between detection and response.

### 3.2 Advantages of the Proposed Model

- Integrated multi-layer security approach
- Real-time intelligent monitoring
- Privacy-focused architecture
- Easy-to-use interface
- Scalable for institutional use

### 3.4. Applications

- Personal safety application for women
- Child online activity monitoring tool
- School digital safety systems
- Community cyber awareness programs

### 4. Problem Statement

The rapid expansion of digital platforms and social media has significantly increased cyber threats targeting vulnerable groups, particularly women and children. Online harassment, cyberbullying, identity theft, phishing attacks, cyberstalking, and exposure to inappropriate content have become major concerns in today’s digital environment.

Despite the availability of general cyber security tools, most existing systems are not specifically designed to address the unique safety needs of women and children. Current solutions often lack real-time threat detection, integrated emergency response mechanisms, user-friendly interfaces, and privacy-focused monitoring.

Additionally, many victims hesitate to report cyber incidents due to fear, lack of awareness, or delayed response systems. There is no unified platform that combines intelligent threat detection, preventive content filtering, and instant SOS emergency support in a single secure framework.

Therefore, there is a critical need to develop an integrated cyber security system that provides proactive protection, real-time monitoring, quick emergency alerts, and awareness support specifically tailored for women and children in the digital space.

#### 4.1-Table-System Development Specification

Backend	Node.js,Express.js
Database	MongoDB with Mongoose ODM
<b>Frontend engine</b>	EJS (Embedded JavaScript)
Styling	Vanilla CSS Tailwind CSS (Tactical CDN usage )
Visuals	Chart.js for data intelligence
Icons	Font Awesome 6 (Strategic Implementation)
Animations	AOS (Animate on Scroll) for premium feel .

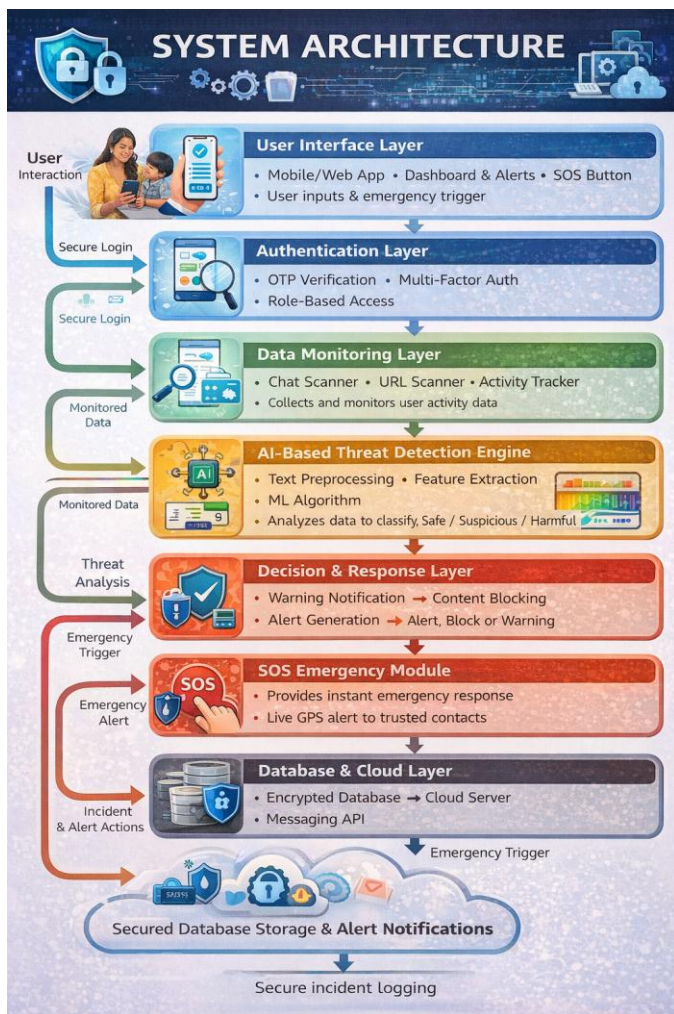


Fig 2:- System Architecture

The system architecture follows a multi-layered approach to ensure digital safety for women and children. The process begins with the **User Interface Layer**, where users interact through a mobile or web application. Secure login is handled by the **Authentication Layer**, which verifies user identity using OTP and multi-factor authentication.

The **Data Monitoring Layer** collects user inputs such as messages and URLs. This data is processed by the **AI-Based Threat Detection Engine**, where machine learning algorithms analyse and classify content as safe, suspicious, or harmful.

Based on the classification, the **Decision & Response Layer** takes appropriate action such as allowing content, generating warnings, or blocking harmful activity. In emergency situations, the **SOS Module** sends live location alerts to trusted contacts. Finally, all incident data is securely stored in the **Database & Cloud Layer** for logging and future reference.

This layered structure ensures real-time detection, quick response, and secure data handling.

## 5. Conclusion

The proposed cyber security framework provides an integrated and intelligent solution to protect women and children from digital threats. By combining AI-based threat detection, secure authentication, real-time monitoring, and emergency response mechanisms, the system enhances online safety and user confidence. The architecture ensures both proactive prevention and rapid incident handling while maintaining data privacy. This research contributes toward building a safer digital environment and can be further enhanced with advanced deep learning techniques and government cybercrime integration in future work.

## REFERENCES

- [1] F. M. Salem, A. F. A. Aziz and H. A. Khalid, "Machine Learning Techniques for Cyber Bullying Detection and Prevention," **International Journal of Advanced Computer Science and Applications (IJACSA)**, Vol. 10, No. 3, 2019.
- [2] S. Gupta and N. Mehta, "Real-Time Phishing Detection Using Natural Language Processing and URL Analysis," **Journal of Information Security and Applications**, Vol. 56, 2021.
- [3] A. Sharma and R. Kumar, "Child Online Safety: Parental Control and Monitoring System Using AI," **International Journal of Computer Applications**, Vol. 183, No. 14, 2021.
- [4] N. Alsaedi and S. Khan, "Cybersecurity Challenges and Countermeasures for Women in Digital Space," **Journal of Cybersecurity and Mobility**, Vol. 8, No. 4, 2020.
- [5] M. Purohit and D. Singh, "Sentiment Analysis for Harassment Detection in Online Social Networks," **Procedia Computer Science**, Vol. 143, 2018, pp. 123-130.
- [6] R. N. Tarun and P. Jayashree, "A Survey on AI-Based Systems for Cyber Safety and Threat Analysis," **International Journal of Engineering Research & Technology (IJERT)**, Vol. 9, No. 5, 2020.
- [7] **International Organizations & Reports**  
**UN Women - Cyber Violence against Women**  
<https://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures>.  
 Provides global statistics and strategies for protecting women online.

**BIOGRAPHIES****1 Mr. Mohd. KAIF KHAN**

Pursuing Poly(co)

S.Y.P SHREEYASH COLLEGE

OF ENGINEERING AND TECHNOLOGY

**2 MR. SHOHEB MAHEDEVI**

Pursuing Poly(co)

S.Y.P SHREEYASH COLLEGE

OF ENGINEERING AND TECHNOLOGY

**3<sup>r</sup> Mr. HIMANSHU GHOGHARE**

Pursuing Poly(co)

S.Y.P SHREEYASH COLLEGE

OF ENGINEERING AND TECHNOLOGY

**4<sup>th</sup> Mr. DNYANRAJ JADHAV**

Pursuing Poly(co)

S.Y.P SHREEYASH COLLEGE

OF ENGINEERING AND TECHNOLOGY

**5<sup>th</sup> Mr. Mayur Unhale**

Guide (lecturer), POLY(CO),

S.Y.P SHREEYASH COLLEGE

OF ENGINEERING AND TECHNOLOGY

**6<sup>TH</sup> Mr. ANIL NAIK**

HOD, POLY(CO),

S.Y.P SHREEYASH COLLEGE

OF ENGINEERING AND TECHNOLOGY