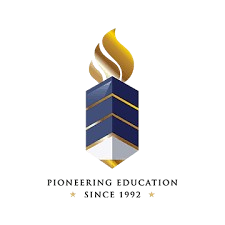
**ShieldNet – AI-Based Phishing and Spam Protection System**

Project Synopsis

By

Zoya Khan

Bachelor of Science (Computer Science)



**DEPARTMENT OF COMPUTER SCIENCE**

SHREE L. R. TIWARI DEGREE COLLEGE OF ARTS, COMMERCE & SCIENCE

(Affiliated with University of Mumbai)

THANE, 401107

MAHARASHTRA

2025-26

**1. Introduction**

Phishing attacks, scam links, and spam-based harassment are becoming increasingly sophisticated in today’s digital age, putting both individuals and organizations at risk. Traditional security tools often fail to detect new or cleverly disguised threats, especially those shared through emails, messages, and social media. ShieldNet aims to solve this problem by providing an intelligent, real-time protection system that uses machine learning to analyze and block suspicious links before the user can engage with them.

The system works across multiple channels—web, email, and messaging—and offers a user-friendly dashboard for link scanning, real-time alerts, and activity tracking. It also introduces a unique mobile-focused feature, "Shield Mode," which helps protect users from spam calls and SMS harassment.

**2. Project Category**

* Cybersecurity & Privacy Protection
* Artificial Intelligence & Machine Learning
* Web and Mobile-Based Security Solutions

**3. Objective**

* To build a smart and scalable AI-based system that:
* Detects and blocks phishing links in real time
* Provides alerts and safe browsing feedback through a browser extension
* Prevents spam calls and SMS via mobile Shield Mode
* Offers a user-centric dashboard for transparency, analytics, and interaction
* Uses explainable AI to describe why a link or message is considered dangerous

**4. System Requirements**

1. Hardware Requirements:

* Processor: Dual-core CPU
* RAM: 4 GB
* Storage: 100 GB HDD or SSD
* Internet connection
* Recommended:
* Processor: Intel i5/i7 or equivalent
* RAM: 8-16 GB
* SSD storage
* GPU for model training/inference (optional)

**2**. **Software Requirements:**

* OS: Windows / Linux / macOS
* Frontend: React.js, Tailwind CSS, Chart.js
* Backend: Node.js, Express.js, FastAPI (Python)
* ML Model: Scikit-learn, TensorFlow
* Browser Extension: JavaScript, WebExtension API
* Mobile Shield: Android SDK / Kotlin / Flutter
* AI Explanation: OpenAI GPT API
* Database: MongoDB

**5. Scope of the Project**

* ShieldNet offers a comprehensive defense platform that operates across the following domains:
* Web Security: Browser-based phishing link detection and prevention
* Email Filtering: Smart analysis of email content and embedded URLs
* Messaging Apps: Auto-analysis and flagging of suspicious links
* Mobile Shield Mode: Protection against spam calls and messages
* AI Explainability: Human-friendly summaries explaining detected threats
* User Dashboard: Activity log, threat summaries, safe browsing statistics
* It is designed for individual users, organizations, educational institutions, and cyber-awareness campaigns.

**6. Expected Results**

* Accurate real-time classification of phishing URLs and scam content
* Successful blocking of suspicious links before user interaction
* Mobile call/SMS protection using behavioral spam detection
* User dashboard with analytics, threat history, and scan tools
* AI-powered explanation engine to clarify security actions
* Scalable backend supporting reports, analytics, and alerts
* Seamless user experience across platforms (web, email, mobile)