

An Intelligent Model for Teen E-Safety Prediction

Mrs. Jyothika K R, Vanishri V Arkachari

Assistant Professor, Department of MCA, BIET, Davanagere-577004 jyothikakarkushi@gmail.com

,Davanagere, Karanataka, India

P.G. Student, 4th Semester, Department of MCA, BIET, Davanagere-577004

vanishriv2002@gmail.com, Davanagere, Karanataka, India

ABSTRACT

A machine learning-based system called the Intelligent Model for Teen E-Safety Prediction was created to assess teens online activity and forecast their cybersecurity risk levels. Teens are more susceptible to cybersecurity risks like phishing cyberbullying data breaches and exposure to harmful content as they rely more and more education and entertainment. Conventional tools such as parental controls and antivirus software are unable to evaluate behavioral patterns or offer tailored safety insights. In order to close this gap the suggested system uses sophisticated algorithms like Random Forest XGBoost and LightGBM in conjunction with reliable preprocessing methods to categorize teens cybersecurity behavior according to characteristics like browsing patterns social media usage device patterns password strength and exposure to online threats.

High prediction accuracy is guaranteed by this data-driven strategy which also encourages young users to adopt safer online practices.

The system incorporates a full web-based platform with administrative and user features predictive analytics. Trustworthy advice administrators can maintain legal aid information pertaining to cyber issues update FAQs and manage user accounts. After registering and logging in users can view educational materials to increase their digital awareness and receive real-time predictions about their cybersecurity behavior.

KEYWORDS: Teen e-safety, Online safety prediction, Adolescent digital behavior, Cyber risk detection, Internet safety monitoring, Youth online protection.

I. INTRODUCTION

An Intelligent Model for Teen E-Safety Prediction is a machine learning-based system that looks at teens online activities and digital habits in order to analyze and forecast their cybersecurity behavior. The model divides users into various safety groups based on data-driven insights from characteristics like social

media usage browsing habits password strength VPN usage and exposure to online threats. The system guarantees high accuracy and dependability in detecting possible cybersecurity threats by incorporating cutting-edge algorithms like Random Forest XGBoost and LightGBM within a strong preprocessing and training pipeline. This clever strategy aids in comprehending teen online behavior encouraging safe internet usage and offering helpful assistance to parents teachers and cybersecurity experts to raise young users awareness of digital safety. Teenagers most active the current digital age participating online gaming educational platforms and other digital environments. Teens are exposed to a number of cybersecurity risks including phishing attacks cyberbullying data breaches and exposure to dangerous websites even though this digital connectivity offers learning and social interaction. Intelligent systems that can examine young users digital footprints and anticipate possible and more necessary as their online behavior continues to influence their safety. The Intelligent Model for Teen E-Safety Prediction is a data-driven solution created classifying teens online behavior patterns according to their digital activities and level of security awareness.

The suggested model uses data analytics and machine learning to evaluate and forecast teens cybersecurity behavior. The system divides users into various cybersecurity risk categories based on factors like device usage browsing

habits social media engagement password strength VPN usage and exposure to cyber threats. To ensure precise and trustworthy predictions the model integrates a thorough data preprocessing and training pipeline that combines cutting-edge algorithms like Random Forest XGBoost LightGBM and Gradient Boosting. Additionally, the dataset is balanced by the use of methods like SMOTE (Synthetic Minority Oversampling Technique) which resolves any class imbalance problems that might skew the results. This clever system seeks to reveal teens degree of cyber awareness and susceptibility. It assists parents educators and cybersecurity specialists in identifying the elements that lead to risky online conduct by evaluating behavioral data. Predictive analytics of this kind tailored interventions to improve teen cyber hygiene encourage safe digital practices and create awareness campaigns. The model is useful for educational institutions and cybersecurity monitoring applications because it incorporates user-friendly input interfaces and enables real-time prediction based on new user data.

An intelligent web-based tool called the Teen E-Safety Prediction System was created to increase teens awareness of and protection for cybersecurity. To guarantee efficient operation and significant engagement it incorporates both administrative and user functionalities. The system enables the administrator to safely log in manage registered users by viewing or removing accounts and keep up a dynamic FAQ section cyberspace.

current legal resources and advice for online safety concerns the administrator can also add or remove legal aid details pertaining to cyber issues. The system provides an interactive and educational interface for the users. Users can access the machine learning-driven cybersecurity behavior classification system which evaluates their digital habits and forecasts their level of cybersecurity risk after registering and logging in with valid credentials. Teens are better equipped to recognize their online behavior patterns and implement safer behaviors as a result.

Problem Statement

Teenagers are more susceptible to cybersecurity risks like phishing data breaches cyberbullying and exposure to harmful content increased education and entertainment. There is still a big awareness and proactive behavior gap among young users even with the abundance of online safety tools. Additionally, there is a dearth of integrated systems that offer advice and legal support for cyber issues evaluating online behavior. Therefore, an intelligent and user-friendly platform that can evaluate teens digital activity categorize their cybersecurity behavior using machine learning and provide pertinent legal and educational resources to raise awareness of online safety is the issue. By creating an Intelligent Teen E-Safety Prediction System that integrates administrative and legal aid features with machine learning-driven behavior analysis this project seeks to close this

gap and encourage safer online behavior among teenagers.

II. RELEATED WORK

Existing System

There aren't many platforms or tools in the current system that are especially designed to evaluate and counsel teenagers on their cybersecurity behavior. The majority of available solutions are either parental control software or general antivirus software which mainly concentrate on monitoring or blocking dangerous content rather than examining user behavior patterns. These systems don't offer individualized awareness or legal support regarding cyber issues and they lack the intelligence to determine each person's risk level based on online activity. Additionally, there is little integration between behavioral prediction educational awareness and legal advice which makes it challenging for teenagers to comprehend their exposure to cyber risk and take the necessary precautions.

Proposed System

By using machine learning to analyze teens digital activities and categorize their cybersecurity behavior into various risk categories the proposed Intelligent Teen E- Safety Prediction System seeks to get around these constraints. This system offers a dual- interface log in and see personalized predictions and safety insights while administrators can manage users FAQs and

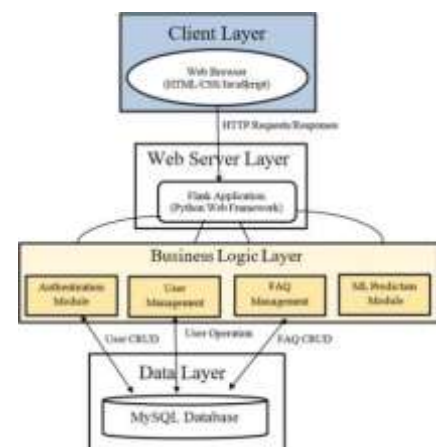
legal aid information. Legal aid and FAQ modules improve awareness and guidance while the incorporation of a machine learning- driven prediction model aids in precisely determining user risk levels. This suggested system encourages a comprehensive approach to online safety and cyber awareness by educating and empowering teenagers to adopt safe digital habits in addition to forecasting risky online behavior.

III. METHODOLOGY

The system is intended to be an intelligent machine-learning-driven platform that assesses teenager's online safety behavior using a variety of digital activity indicators. It serves as a decision-support tool that aids in categorizing a user's cybersecurity behavior according to the risk category. From a wider angle the system functions as a data-processing and prediction layer incorporated into an intuitive user interface that allows teenagers to log in enter data and view their e-safety classification right away. In order to keep the system current applicable and usable administrators indirectly manage the dataset through user and FAQ management. To make sure that predictions accurately reflect actual digital habits the system communicates with preprocessing units machine-learning models and data-validation modules. While administrators keep control and governance over content and user management it functions as a safe interactive

environment that supports teens by encouraging awareness and safe online practices. Data acquisition is the first step in the methodology's structured pipeline which concludes with a deployable prediction system. Initially a comprehensive dataset is gathered that represents a variety of teen online behaviors including device usage risky website visits login attempts phishing incidents and awareness scores. Preprocessing procedures for this data include handling missing values standardizing numerical features encoding categorical features and using SMOTE to balance the dataset to address class imbalance. The most accurate model is then found by using cross-validation to train a number of machine- learning algorithms such as Random Forest XGBoost Gradient Boosting and LightGBM. For deployment the top-performing model is stored as a reusable prediction pipeline.

ARCHITECTURE DIADRAM



IV.RESULTS

SNAPSHOTS:

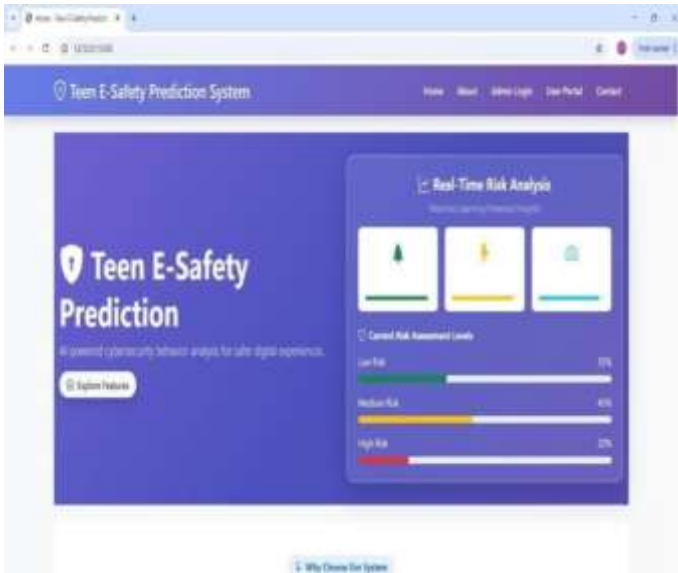


Fig: Teen E-Safety Home Page

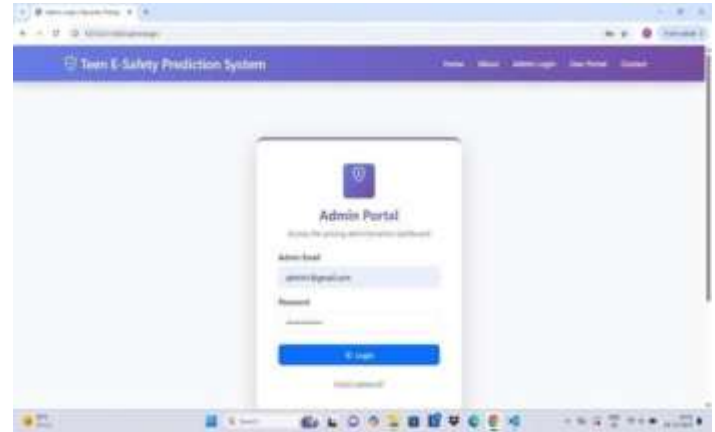


Fig: Admin Login Page

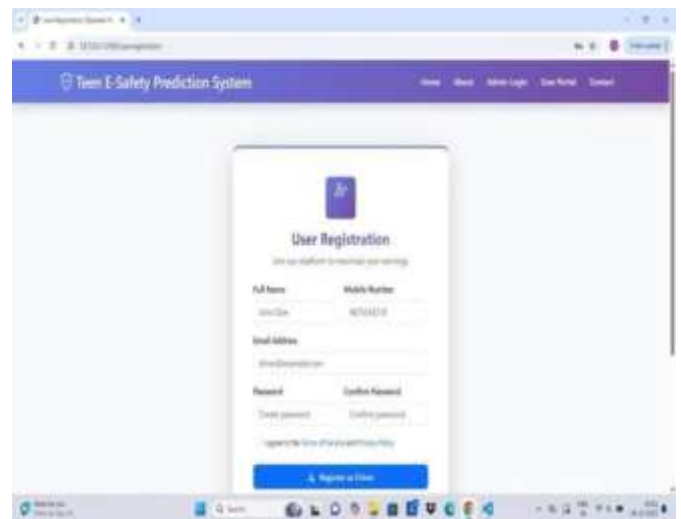


Fig: User Registration Page

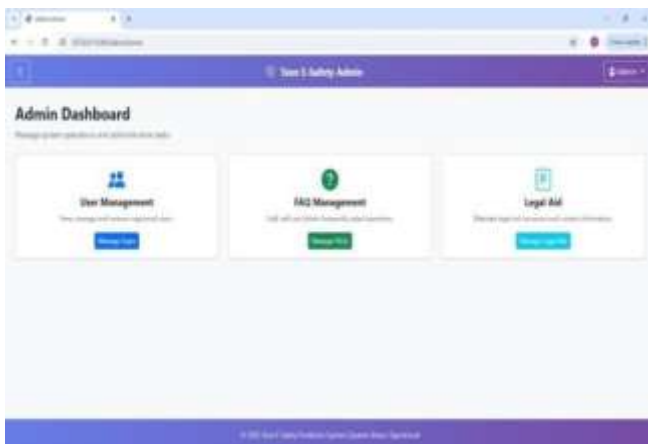


Fig: Admin Dashboard Page



Fig: Prediction Page

V. CONCLUSION

To evaluate cybersecurity risks among teenagers the Intelligent Teen E-Safety Prediction System effectively combines machine-learning techniques with behavioral data. By using sophisticated models and preprocessing pipelines the system guarantees precise and significant forecasts. Because of its user-friendly design the platform can be effectively used by administrators and teenagers. The system promotes responsible online behavior and raises awareness of cyber risks by offering practical insights into online safety practices. All things considered the project shows how artificial intelligence can be effectively used to improve cyber safety in a contemporary digital environment.

VI. REFERENCES

- A Deep Learning Framework for Teenage Cybersecurity Awareness Using Real- World E-Safety Data; Authors: Shu Xu, Song Peng, Jie An; Publication: Informatica Vol. 49, No. 18 (2025); DOI: 10.31449/inf.v49i18.7861
- Cybersecurity awareness for children: A systematic literature review; Authors: F Quayyum, D.S. Cruzes, L. Jaccheri; Publication: International Journal of Child-Computer Interaction, Vol 30 (2021); DOI: 10.1016/j.ijcci.2021.100343; E-ISSN: 2212-8689.
- Online Safety for Children and Youth

under the 4Cs Framework — A Focus on Digital Policies in Australia, Canada, and the UK; Authors: Yujin Jang, Bomin Ko; Publication: Children (Basel), Vol 10 Issue 8 (2023); DOI: 10.3390/children10081415; E-ISSN: 2227-9067.

- Improving Children's E-Safety Skills through an Interactive Learning Environment: A Quasi-Experimental Study; Authors: Iolie Nicolaidou & Agnes Venizelou; Publication: Multimodal Technologies and Interaction, Vol 4, Issue 2 (2020); DOI: 10.3390/mti4020010.
- YouthSafe: A Youth-Centric Safety Benchmark and Safeguard Model for Large Language Models; Authors: Yaman Yu, Yiren Liu, Jacky Zhang, Yun Huang, Yang Wang; Publication: arXiv preprint arXiv:2509.08997v1 (2025); DOI/identifier: arXiv:2509.08997v1