# CITIZEN SAFETY APP FOR PROTECTION AGAINST CYBER CRIMES

**Janhavi Chaudhari[1], Roshani Nalawade[2], Aditya Singote[3], Ayush Shukla[4], Dr. C. M. Raut[5]**

[1]*Computer Department, Mumbai University, India*

[2]*Computer Department, Mumbai University, India*

[3]*Computer Department, Mumbai University, India*

[4]*Computer Department, Mumbai University, India*

[5]*Computer Department, Mumbai University, India*

***Abstract***

***The Citizen Safety App is an innovative mobile solution designed to proactively combat cybercrimes by employing real-time monitoring and analysis of various elements. Beyond scrutinizing mobile numbers, SMS headers, URL links, UPI addresses and SMS templates, the app introduces an array of features to enhance user safety. A Nearby User Connection system facilitates emergency communication among users in critical situations, while simplified laws associated with cybercrimes empower users with legal knowledge. The app also incorporates an AI-generated video story feature, offering an immersive learning experience about potential threats and providing tips on maintaining digital safety. This multifaceted approach aims to empower users with the tools, knowledge, and support needed to navigate the digital landscape securely, safeguarding personal information and financial assets from cybercriminals.***

***Keywords***

***Citizensafety, Cybercrime, Cybersecurity, mobileapp ,laws***

## 1.INTRODUCTION:

In our digitally interconnected world, technological advancements have ushered in numerous benefits alongside new and complex challenges, especially in the face of evolving cybercrime tactics. Malicious actors continually threaten the privacy and security of citizens. To address these concerns, we introduce the Citizen Safety App—a real-time solution aimed at protecting individuals from cybercrimes by promptly flagging malicious and fraudulent indicators. This comprehensive application focuses on elements such as mobile numbers, SMS headers, URL links, UPI addresses and SMS templates.

The motivation behind the Citizen Safety App is rooted in the imperative to empower individuals and enhance their safety in the digital landscape. As cybercrimes proliferate, providing citizens with a user-friendly tool becomes essential to protect against scams, phishing attempts, and fraudulent activities. The app aims to equip users with the ability to swiftly identify potential threats, reducing the likelihood of falling victim to cybercriminals and contributing to a safer online environment for all.

Building upon existing cybersecurity technologies, the Citizen Safety App leverages artificial intelligence, machine learning, and data analysis to recognize patterns and indicators of malicious activities. Its unique contribution lies in a user-centric approach, real-time detection capabilities, and comprehensive coverage of potential threat indicators, making

it a versatile tool with applications as a defense against phishing attacks, fraud, and cyber scams. Moreover, its utility extends to businesses, financial institutions, and law enforcement agencies, providing an additional layer of protection and serving as an educational tool to enhance users' awareness of cybercriminal tactics. The report delves into the app's features, technology, and potential challenges, highlighting its role in safeguarding individuals and organizations in an increasingly digitized world.

## 2. LITERATURE SURVEY:

### 2.1 GOVERNMENT INITIATIVE(GI):

By NISAP (Part of the National Cyber Security Policy), by making the citizens of SCI realize regarding need for the prevention of cybercrimes, the GoI should try to improve awareness among the citizens of SCI for the prevention of cybercrimes.

### 2.2 SOCIAL MEDIA (SM):

Awareness among citizens of SCI may be developed by social media as it would help exchange information regarding the menace of cybercrimes in the proposed SCI. This ingredient would enhance awareness which in turn motivates the citizens of SCI to use technology to prevent cybercrimes in SCI.

### 2.3 WORD OF MOUTH (WOM):

The exchange of views from person to person through talks constitutes the affairs termed as WOM. It helps to form an effective influence to improve the awareness of citizens of SCI regarding cybercrimes. It helps develop preventive measures against cybercrimes in SCI.

### 2.4 ORGANISATION(ORG):

The role of organizations functioning in SCI is vital for forming awareness instrumental to prevent cybercrimes in SCI. The functions of the organizations should be flawless to develop trust among the citizens of SCI on these organizations. It would bring the confidence of the citizens of SCI in these organizations and in that case, the actions of the organizations would impact the citizens of SCI to develop an awareness of cybercrimes .

### 2.5 AWARENESS OF CYBERCRIMES(AOC):

It is associated with the knowledge and attention of the users. This helps the users to know details about the internet and its functionalities. This helps the citizens of SCI to improve their awareness of cybercrimes and its dangers. This would help to prevent cybercrimes in SCI.

### 2.6 PERCEIVED USEFULNESS(PU):

It is the perception of citizens of SCI for the prevention of cybercrimes. It includes many ingredients like effectiveness, performance, trust, risk perception, and productivity. It motivates the citizens to use technologies essential to prevent cybercrimes in SCI. It is associated with the sense of perceiving the usefulness of the technology.

### 2.7 PERCEIVED EASE OF USE(PEU):

It is construed to be degree to which citizens of SCI would believe that some efforts are needed to learn for use of a technology essential to prevent cybercrimes in SCI. This ingredient includes factors like simplicity, compatibility, and self efficacy. This impacts on actual use of technology to prevent cybercrimes in SCI.

### 2.8 PREVENTIONS OF CYBERCRIMES IN SCI(PCS):

The prevention of cybercrimes in SCI includes mechanisms required to increase awareness among the citizens of SCI and includes actual technology use. This would help to prevent cybercrimes in SCI.

## 3.PROPOSED SYSTEM

We chose to use the Random Forest classification algorithm for our malicious URL detection model due to its robust and reliable performance in the field of cybersecurity. The Random Forest algorithm is an ensemble learning method that combines the predictive power of multiple decision trees. This approach significantly enhances the accuracy of classification by mitigating the overfitting problem often encountered with individual decision trees. In our application, this algorithm is particularly valuable because it can effectively analyse and categorize URLs into four distinct classes: spam, malicious, defacement, and safe. By aggregating the results of numerous decision trees, the Random Forest algorithm provides a comprehensive and accurate assessment of whether a given URL poses a threat, enabling us to protect users from potential cybercrimes. For our spam SMS detection model, we opted for the Naive Bayes classification model and Bayes' theorem. The Naive Bayes algorithm is well-suited for text classification tasks, such as distinguishing between spam and legitimate SMS messages. It works by calculating the probability of a message belonging to each category and then selecting the category with the highest probability. Bayes' theorem is a fundamental probability theory that underpins Naive Bayes. This approach is ideal for our application because it can efficiently analyse the content of SMS messages and classify them as either spam or ham. The simplicity and efficiency of the Naive Bayes classifier make it a strong choice for

real-time SMS classification, helping to protect users from unwanted and potentially harmful messages. To detect UPI and cryptocurrency wallet scams, we plan to leverage the NPCI API provided by the government. This API is a reliable and authoritative source of information that can verify the authenticity of users and their transactions, helping us identify potential threats. Machine learning (ML) will also play a crucial role in the process, as it can analyze transaction data and patterns to identify anomalies or suspicious activities associated with Bitcoin transactions. By combining the NPCI API and ML, we can provide users with a powerful defense against fraudulent UPI and cryptocurrency wallet transactions, thereby enhancing their safety and security in the digital financial realm.

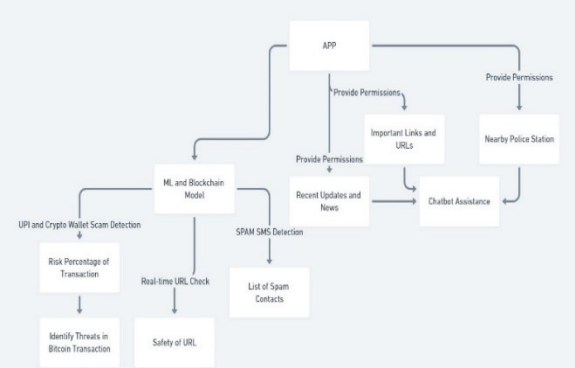



Fig.1 FLOW CHART OF MOBILE APP

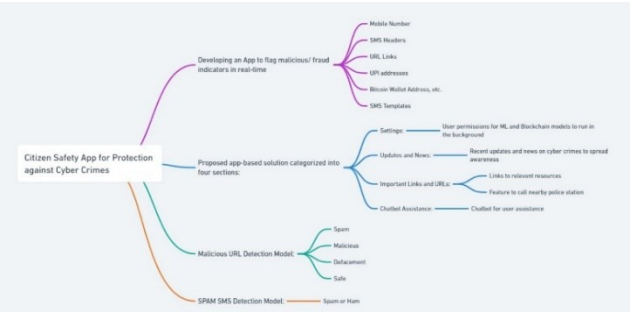



Fig.2 DETAILED FLOW IDEA PROPOSED

## 4.DESIGN AND IMPLEMENTATION

The cybersecurity app, developed using React Native for the frontend and FastAPI for real-time processing, is designed to provide users with a holistic solution for combating cybercrimes. Leveraging Hugging Face models for SMS, URL, and call fraud, fine-tuned on a dedicated dataset, along with a machine learning model for UPI address fraud, the app ensures real-time monitoring and prevention of various threats. The integration of Google Maps API facilitates a Nearby User Connection system during emergencies. Additionally, the app features a Stories and Blog section for users to share and learn from cybercrime incidents, a Know Your Laws section for simplified legal information, and a chatbot to assist users in understanding and addressing fraud-related issues. In the Know Your Laws section, there is an added integration of AI-generated stories for all types of crime in Hindi, ensuring citizens of India are aware in detail. Furthermore, storybooks for children are included to educate the younger audience about cybersecurity.

### 4.1.FRAUD PREVENTION:

#### *4.1.1. SMS FRAUD:*

- Implementation: The app utilizes the Hugging Face model for SMS fraud detection, fine-tuned with a specific dataset. The SMS fraud detection model[1] operates in two steps: first, it checks whether there is any URL present or not, and then the URL is tested. Subsequently, the SMS message is classified based on context, and the SMS is handled accordingly in real-time[5] .The model is seamlessly integrated into the React Native frontend, with FastAPI managing the backend for real-time processing and monitoring..

#### *4.1.2. URL FRAUD:*

- Implementation: Leveraging the Hugging Face model for URL fraud detection[4][6], the app fine-tunes the model on a dedicated dataset. Integration into the React Native frontend and FastAPI backend ensures continuous real-time monitoring of URL links.

#### *4.1.3. CALL FRAUD:*

- Implementation: The Hugging Face model for call fraud detection is integrated into the React Native app using react-native-call-log library for real time call handling, with fine-tuning on a call fraud-specific dataset. FastAPI manages the backend, enabling efficient real-time monitoring and response to potential call fraud.

#### *4.1.4. UPI ADDRESS FRAUD:*

- Implementation: A dedicated machine learning model for UPI address fraud is created and integrated into the React Native frontend. FastAPI handles the backend, allowing real-time detection and classification of fraudulent UPI addresses.

### 4.2.EMERGENCY RESPONSE:

#### *4.2.1. Nearby User Connection:*

- Implementation: The app implements a Nearby User Connection system using the Google Maps API for real-time location detection. Integration with React Native and a dedicated server[4] ensures accurate user location tracking, facilitating quick communication among nearby users during emergencies.

### 4.3.USER ENGAGEMENT:

#### *4.3.1. STORIES AND BLOG SECTION:*

- Implementation: Within the React Native app, a user-friendly interface is created for the Stories and Blog section. FastAPI is employed to manage the backend, storing and retrieving user-generated content to foster a community-driven approach to understanding and preventing cybercrimes.

#### *4.3.2. KNOW YOUR LAWS:*

- Implementation: The app features a section that simplifies Indian cyber laws. The design includes an intuitive user interface within React Native, while FastAPI manages the backend, integrating relevant APIs for the latest legal information, ensuring easy navigation, and accessibility. AI-generated stories for all types of crime in Hindi and storybooks for children are integrated to enhance user awareness and education.

#### *4.3.3. CHATBOT:*

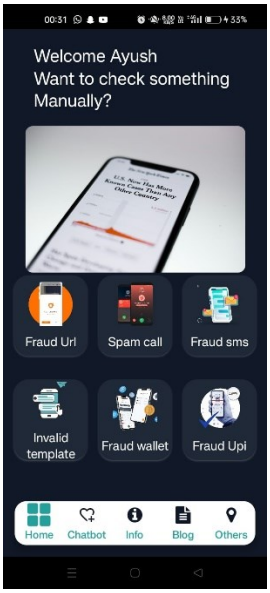
- Implementation: A chatbot is seamlessly integrated into the React Native app to assist users. The chatbot platform connects to the frontend, providing real-time information on fraud prevention, incident reporting, and resolution steps. Regular updates to the chatbot's knowledge base enhance its effectiveness in guiding users through potential cyber threats and solutions.

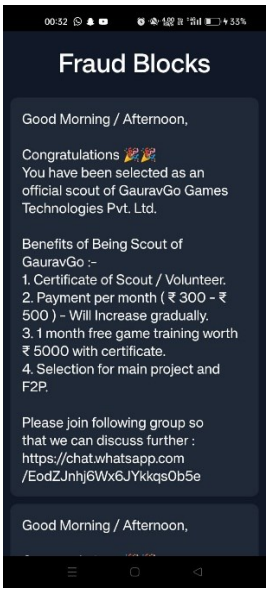
## 5. RESULT AND DISCUSSIONS:

The implementation of the proposed cybersecurity app has yielded promising results, providing users with a comprehensive and user-friendly solution to combat cybercrimes. Leveraging React Native for the frontend and Fast API for real-time processing has enabled seamless integration of cutting-edge technologies and features.

### 5.1. FRAUD PREVENTION:

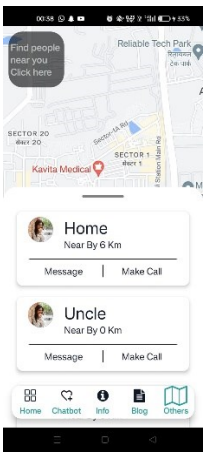
The integration of Hugging Face models for SMS, URL, and call fraud, along with a dedicated machine learning model for UPI address fraud, has demonstrated effective real-time monitoring and prevention of various cyber threats. The continuous fine-tuning of these models ensures adaptability to evolving fraud patterns, enhancing the app's ability to safeguard users.

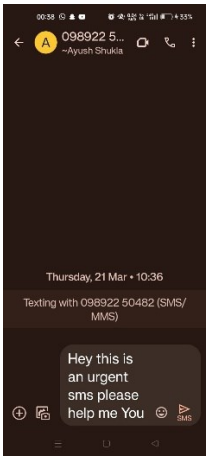



### 5.2. NEARBY USER CONNECTION:

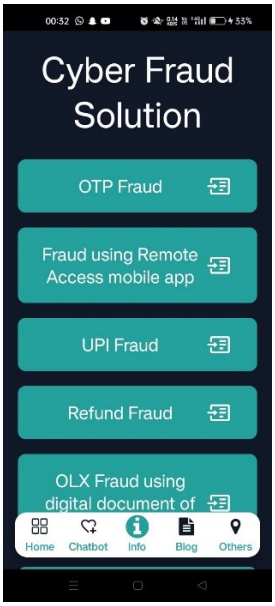
The integration of the Google Maps API has successfully facilitated a Nearby Freaquently contacted User Connection system during emergencies with emergency message and call option. Geofencing technology and automatic emergency alerts have improved the accuracy and responsiveness of this feature, ensuring swift communication among users in critical situations.

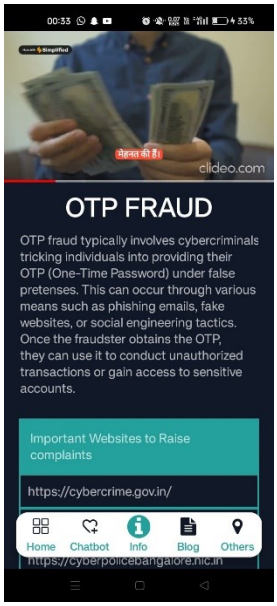


### 5.3. USER ENGAGEMENT AND EDUCATION:

The Stories and Blog section has become a thriving community-driven platform, allowing users to share and learn from real cybercrime incidents. The gamification elements have incentivized active user participation, fostering a sense of community awareness. The Know Your Laws section, with its added integration of AI-generated stories in Hindi, has successfully enhanced user awareness and understanding of cyber laws. Moreover, the inclusion of storybooks for children has proven effective in educating the younger audience about the importance of cybersecurity.



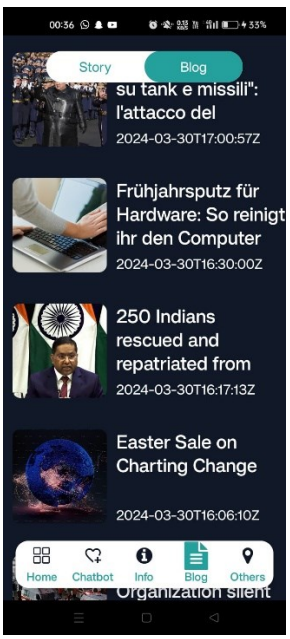



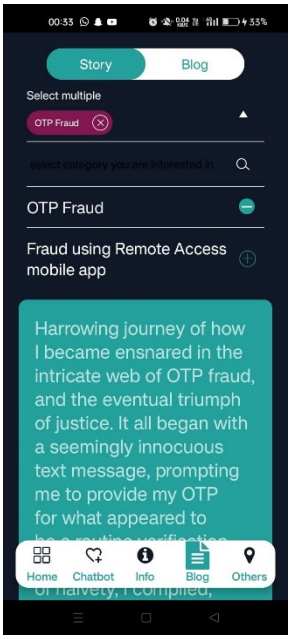

### 5.4. CHATBOT FUNCTIONALITY:

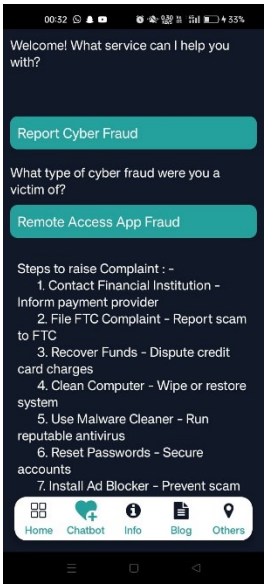
The chatbot has become an invaluable tool for users, providing real-time information on fraud prevention, incident reporting, and resolution steps. Improved natural language processing and interactive decision trees have enhanced the chatbot's ability to guide users through complex scenarios, making it a reliable source of assistance.

### 5.5. Cross-Platform Integration:

The extension of platform support to additional devices and the implementation of cloud-based synchronization have successfully provided users with a seamless experience across various platforms. This has contributed to increased accessibility and user convenience.




## 6. ACKNOWLEDGMENT:

On the successful completion of this project, we would like to express our gratitude to our Prof. Dr CM. RAUT who helped us throughout the development of this project. We would also like to extend our appreciation to the creators of every website, application, and feature that we have been inspired or referred to create this application. We hope that this project can serve its purpose and can someday be implemented as a viable business idea.

## 7. CONCLUSION:

The cybersecurity app stands as a comprehensive and innovative solution in the realm of digital safety. Leveraging cutting-edge technologies such as React Native, FastAPI, Hugging Face models, and machine learning, the app effectively addresses various cyber threats in real-time. The integration of Google Maps API enhances emergency response with the Nearby User Connection system, showcasing a commitment to user safety during critical situations.

The community-driven Stories and Blog section, along with AI-generated crime stories in Hindi, fosters user engagement and cultural relevance. The Know Your Laws section simplifies legal information, providing a valuable resource for users. Additionally, the inclusion of storybooks for children contributes to building a foundation of cybersecurity awareness from a young age. Overall, the app successfully combines technology, education, and user engagement to create a robust and user-friendly tool in the ongoing battle against cybercrimes.

## 8. REFERENCES:


[1] H. Faris, A. M. Al-Zoubi, A. A. Heidari et al., "An intelligent system for spam detection and identification of the most relevant features based on evolutionary random weight networks," Information Fusion , vol. 48, pp. 67–83, 2019.

[2] E. Blanzieri and A. Bryl, "A survey of learning-based techniques of email spam filtering," Artificial Intelligence Review , vol. 29, no. 1, pp. 63–92, 2008.

[3] A. Alghoul, S. Al Ajrami, G. Al Jarousha, G. Harb, and S. S. Abu-Naser, "Email classification using artificial neural network," International Journal for Academic Development , vol. 2, 2018.

[4] React Native & Geolocation: Finding Nearest Location :

https://medium.com/human-case-study/react-native-geolocation-finding-nearest-location-636b07236950

[5] Listen to incoming SMS from React Native App using React Native Bridge: https://ajayts7.medium.com/z-1bc0cbd5d00c.

[6] M. E. H. V. S. Aalla and N. R. Dumpala, "Malicious URL prediction using machine learning techniques", Ann. Romanian Soc. Cell Biol. , vol. 25, no. 5, pp. 2170-2176, Jan. 2021, [online] Available: https://www.annalsofrscb.ro/index.php/journal/article/view/4752.