ADVANCEMENTS IN MACHINE LEARNING FOR ENHANCED CYBERSECURITY AND FINANCIAL ANALYSIS

Abinaya
PSG College Of Technology
Coimbatore
21i301@psgtech.ac.in

Divyalakshmi
PSG College Of Technology
Coimbatore
21i314@psgtech.ac.in

Kavyaa
PSG College Of Technology
Coimbatore
21i322@psgtech.ac.in

Sruthimalya
PSG College Of Technology
Coimbatore
21i361@psgtech.ac.in

***Abstract*-The Citizen Safety App is a proactive solution designed to protect individuals from cybercrimes by leveraging machine learning and real-time monitoring. It analyzes various elements such as mobile numbers, SMS headers, URL links, UPI addresses, Bitcoin wallet addresses, and SMS templates to identify potential threats and alert users promptly. The app's machine learning model is trained on diverse datasets of cyber threats, utilizing supervised and unsupervised learning techniques. Integration with external APIs enhances its analysis capabilities, while a user-friendly interface provides clear alerts and actionable insights. The app's machine learning pipeline encompasses data collection, preprocessing, feature engineering, model training, evaluation, integration, deployment, and maintenance. Overall, the Citizen Safety App represents a valuable tool in combating cybercrimes and safeguarding individuals' digital security.**

Keywords - Citizen Safety app, Cybercrimes, Malicious indicators, SMS headers, URL links, UPI addresses.

I.INTRODUCTION

In today's interconnected digital landscape, cybercrimes pose a pervasive threat to individuals' safety and security. Malicious actors exploit various tactics, including phishing, identity theft, and fraud, to exploit vulnerabilities and perpetrate crimes, often evading detection by traditional means. Recognizing the critical need for proactive protection, the Citizen Safety App emerges as a groundbreaking solution aimed at empowering individuals to defend themselves against cyber threats in real-time.

Leveraging advanced technologies such as machine learning and data analysis, the Citizen Safety App offers a comprehensive approach to identifying and mitigating potential risks. By analyzing diverse data elements such as mobile numbers, SMS headers, URL links, UPI addresses, Bitcoin wallet addresses, and SMS templates, the app detects suspicious activity and alerts users promptly. This proactive stance not only enhances individuals' awareness of cyber threats but also equips them with actionable insights to protect their digital assets and personal information effectively.

II.NEED FOR WORK

The escalating frequency and sophistication of cybercrimes underscore the urgent need for robust solutions to protect individuals' digital safety. Traditional methods of cybersecurity, while valuable, often struggle to keep pace with evolving threats, leaving individuals vulnerable to exploitation. Furthermore, as technology continues to advance and connectivity becomes increasingly ubiquitous, the potential attack surface for cybercriminals expands exponentially. Thus,

there is a pressing need for innovative approaches that can proactively identify and thwart cyber threats in real-time, empowering individuals to navigate the digital landscape securely.

The Citizen Safety App addresses this critical need by harnessing cutting-edge technologies such as machine learning and data analysis to provide individuals with proactive protection against cybercrimes. By analyzing multiple data points and patterns, including mobile numbers, SMS headers, URL links, UPI addresses, Bitcoin wallet addresses, and SMS templates, the app offers a comprehensive defense mechanism. Moreover, the app's ability to monitor incoming data in real-time enhances individuals' situational awareness, enabling them to respond swiftly to potential threats. Overall, the Citizen Safety App represents a crucial step forward in safeguarding individuals' digital security and preserving trust in the digital ecosystem.

III.LITERATURE REVIEW

A. SMS Spam and Phishing Detection

Al-Musawa and Newman (2010) conducted a study reviewing SMS spam filtering techniques. They explored methods such as keyword analysis, message structure examination, and sender identification to differentiate spam messages from legitimate ones, shedding light on the evolving landscape of text-based cyber threats[1].

Liu et al. (2021) focused on detecting SMS spear phishing attacks targeting mobile devices through SMS messages. They discussed various detection techniques, potentially including machine learning algorithms, text analysis, and behavioral analysis, providing insights through potential case studies or real-world examples[2].

B. Phishing URL Detection

Huang et al. (2019) explored phishing URL detection methodologies, particularly leveraging Convolutional Neural Networks (CNNs). Their research highlighted the effectiveness of CNNs in discerning suspicious URL characteristics, contributing to advancements in cyber defense mechanisms against phishing attacks[3].

Ahmad Sahban et al. introduced QsecR, a secure QR code scanner designed to detect malicious URLs. Their work likely employed machine learning algorithms or pattern recognition techniques, aiming to enhance security by providing real-time detection and warning mechanisms when scanning potentially harmful QR codes[4].

C. Security Analysis of Unified Payments Interface and Payment Apps

Kumar et al. (2020) likely assessed the security aspects of the Unified Payments Interface (UPI) and various payment apps used in India. Their analysis may have delved into architecture, protocols, and implementation details to identify security vulnerabilities and risks, providing recommendations for improving security[5].

D. Investigating Bitcoin Balances and Wallet Addresses

Keshav Kaushi et al. (2019) introduced an automated method for investigating Bitcoin balances and wallet addresses, aiming to streamline and enhance the process of analyzing transactions and blockchain data. Their research likely presented a novel approach involving data mining techniques, machine learning algorithms, or blockchain analysis tools to automate extraction and analysis of Bitcoin-related information[6].

IV.PROPOSED METHOD

A.BLOCK DIAGRAM

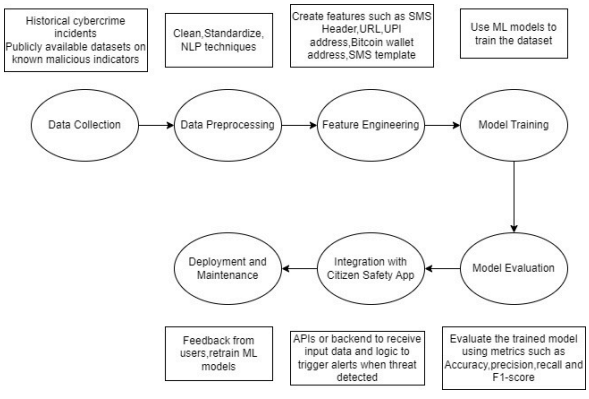

Fig 1. Block diagram

B. DATASETS

In our study, we employed diverse datasets to explore and address various challenges in machine learning applications. For citizen safety enhancement, we utilized the "spam.csv" dataset [7] as in Fig 3 for spam message detection, facilitating the development and evaluation of models ranging from Multinomial Naive Bayes to sophisticated transformer architectures like RoBERTa. Additionally, our investigation into phishing URL detection was supported by the "phising.csv" dataset [8] as in FIG 4, which enabled the training and assessment of a multitude of classifiers including Logistic Regression, K-Nearest Neighbors, Support Vector Machines, Decision Trees, Random Forest, Gradient Boosting, CatBoost, and Multi-Layer Perceptron. Furthermore, our analysis extended to financial domains with the utilization of the Elliptic dataset [9] as in Fig 5, comprising features, classes, and edgelists across multiple CSV files, to predict Bitcoin prices utilizing Convolutional Neural Networks. These datasets provided rich and diverse sources of information, facilitating comprehensive analyses and offering insights into real-world applications of machine learning across cybersecurity and financial domains.

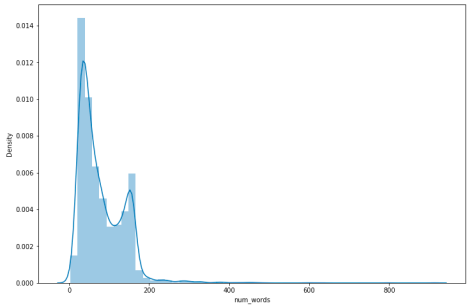

Fig 2. train.csv density with number of words

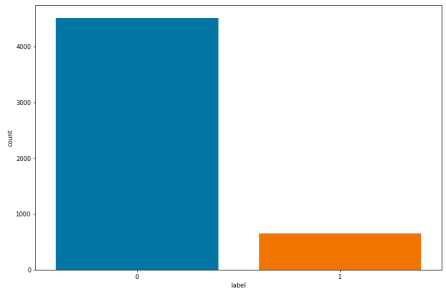

Fig 3. spam.csv label categories

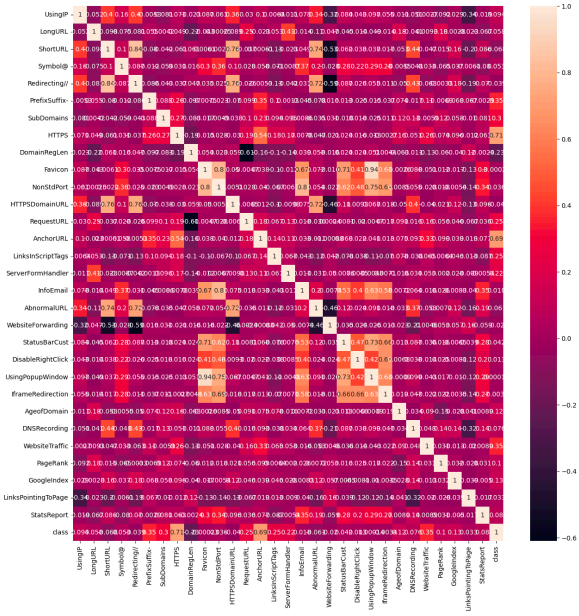

Fig 4. Heatmap of phishing.csv

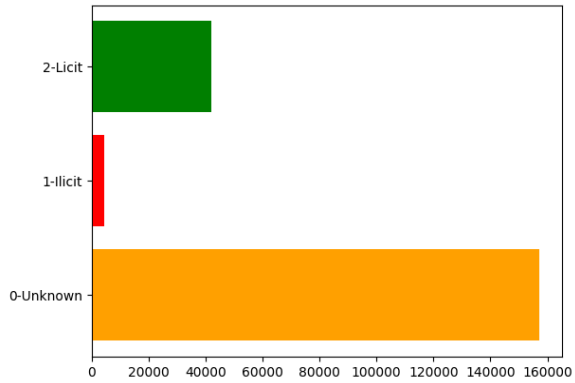

Fig 5. Bitcoin label categories

C. ALGORITHM

1. Data Collection:

Gather data from various sources such as Historical cybercrime incidents,Publicly available datasets on known malicious indicators,User interactions within the app (e.g., reported incidents) and External APIs for real-time data on cyber threats.

2. Data Preprocessing:

Clean the collected data to handle missing values, duplicates, and inconsistencies.Extract relevant features from different types of data (e.g., mobile numbers, URLs).Use natural language processing (NLP) techniques to preprocess text data (e.g., SMS templates)

3. Feature Engineering:

Create features from different data elements such as Mobile number features (e.g., country code, carrier information),SMS header features (e.g., sender information, message timestamp),URL features (e.g., domain reputation, URL length),UPI address features (e.g., validity, transaction history),Bitcoin wallet address features (e.g., transaction frequency, blacklisted addresses),SMS template features (e.g., keyword frequency, sentiment analysis)

4. Model Training:

Train machine learning models to detect malicious or fraudulent indicators, considering different types of data:

- Supervised learning models (e.g., logistic regression, random forest) for classification tasks.
- Unsupervised learning models (e.g., clustering algorithms) for anomaly detection.
- Neural network models (e.g., deep learning architectures) for complex pattern recognition.

Use labeled data to train the models, with a focus on balancing precision and recall for accurate threat detection.

5. Model Evaluation:

Evaluate the trained models using appropriate metrics such as accuracy, precision, recall, and F1-score.Perform cross-validation and hyperparameter tuning to optimize model performance.Validate the models using real-world data and simulated cyber threat scenarios to ensure robustness.

6. Integration with Citizen Safety App:

Integrate the trained models into the Citizen Safety App infrastructure for real-time threat detection.Develop APIs or backend services to receive input data (e.g., SMS messages, URLs) and provide predictions.Implement logic to trigger alerts and notifications for users when potential threats are detected.

7. Deployment:

Deploy the Citizen Safety App with integrated machine learning models on appropriate platforms (e.g., web, mobile).Monitor the performance of the app and models in production to

ensure reliability and scalability.Implement logging and error handling mechanisms for debugging and troubleshooting.

V. EXPERIMENTAL RESULTS

In our pursuit of developing a citizen safety app, we embarked on a series of experiments aimed at refining our approach to effectively identify spam messages. Initially, we employed a Multinomial Naive Bayes (MultinomialNB) model trained on the "spam.csv" dataset. This initial model exhibited a commendable accuracy of approximately 96.89%.

Subsequently, we sought to enhance the performance of our spam detection system by leveraging state-of-the-art techniques in natural language processing. To this end, we adopted a RoBERTa - Base transformer model, which was fine-tuned using the "train.csv" dataset. Through meticulous training spanning 50 epochs, our refined model achieved a notable accuracy of about 99.22% as shon in Fig 6 and Fig 8 for the loss and accuracy graph.

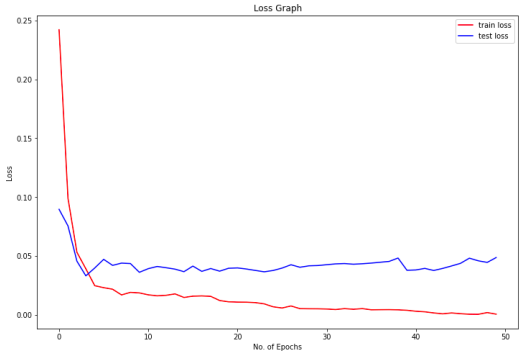

Fig 6. Model loss for RoBerta based transformer model

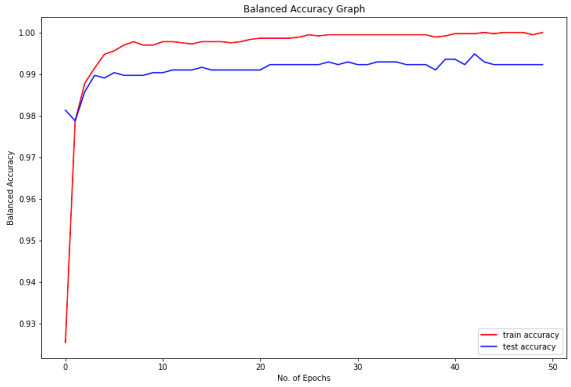

Fig 7. Model accuracy for RoBerta based transformer model

Additionally, to make our spam detection system accessible and user-friendly, we developed a mobile application. This application allows users to input text messages, upon which our model promptly predicts the likelihood of the message being spam.

Our exploration into phishing URL detection was a comprehensive endeavor, encompassing a range of machine learning models to discern the most effective approach. Across the spectrum of models tested, notable accuracies were achieved, showcasing the diverse capabilities of each algorithm. Logistic Regression demonstrated a respectable accuracy of 92.7%, providing a solid baseline for comparison. Meanwhile, K-Nearest Neighbors (KNN) and Support Vector Machines (SVM) surpassed this baseline with remarkable accuracies of 98.9% and 96.9% respectively, indicating their efficacy in discerning phishing URLs. Conversely, the Naive Bayes classifier exhibited a lower accuracy of 60.5%, suggesting potential limitations in its ability to handle the complexity of phishing detection tasks.

The comparision as shown in Fig 8 the comparision of defferent models. Among the tree-based ensemble methods, Decision Trees, Random Forest, and Gradient Boosting Classifier demonstrated robust performance, achieving accuracies of 99.1%, 99.0%, and approximately 98.9% respectively. These results underscore the effectiveness of ensemble techniques in capturing intricate patterns within phishing URLs. Additionally, the CatBoost classifier also achieved a notable accuracy of around 99.1%, further corroborating the efficacy of boosting algorithms in mitigating the risks posed by phishing attempts. The Multi-Layer Perceptron (MLP) classifier, with an accuracy of 98.7%, showcased the potential of neural network architectures in phishing URL detection. Finally the training an testing accuracy graph is shown in Fig 9. Overall, our experimentation underscores the importance of leveraging diverse machine learning methodologies to combat the pervasive threat of phishing, providing valuable insights for the development of robust cybersecurity systems.

	ML Model	Accuracy	f1_score	Recall	Precision
0	Gradient Boosting Classifier	0.974	0.977	0.994	0.986
1	CatBoost Classifier	0.972	0.975	0.994	0.989
2	Multi-layer Perceptron	0.967	0.971	0.991	0.986
3	Random Forest	0.965	0.968	0.994	0.989
4	Support Vector Machine	0.964	0.968	0.980	0.965
5	Decision Tree	0.959	0.963	0.991	0.993
6	K-Nearest Neighbors	0.956	0.961	0.991	0.989
7	Logistic Regression	0.934	0.941	0.943	0.927
8	Naive Bayes Classifier	0.605	0.454	0.292	0.997

Fig 8. Comparision of evaluation metrics for phising url with different model

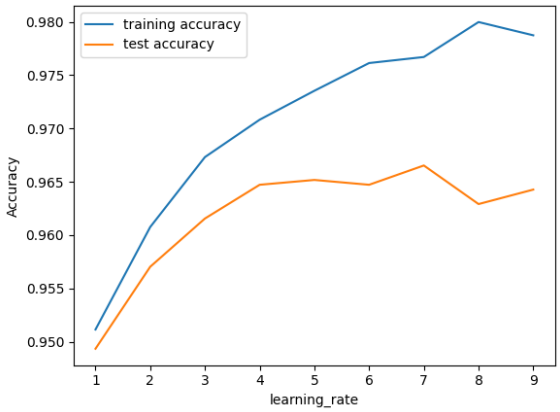

Fig 9. Training and Testing accuracy of the Gradient Boosting Model for phishing url detection

Based on important performance criteria like accuracy, precision, recall, and F1-Score, we analyzed the dataset and assessed the effectiveness of five machine learning models: Random Forest, Gradient Boosting, Logistic Regression, Artificial Neural Network, and Decision Tree. Of these models, Random Forest performed the best overall, attaining an accuracy of 89.46% along with high values for precision, recall, and F1-score. Gradient Boosting achieved competitive scores across all criteria and trailed

closely behind with an accuracy of 89.25%. With a steady precision, recall, and F1-score of 87.63%, Logistic Regression demonstrated commendable performance. Although it did not perform as well as Logistic Regression, the Artificial Neural Network nevertheless showed competitive performance.With an accuracy of 85.16% and worse precision, recall, and F1-score values than the other models, Decision Tree, as shown in Fig 10 finally performed the worst out of all the models. The models that performed the best overall were Random Forest and Gradient Boosting, demonstrating their efficiency in processing the provided dataset the ROC curve is shown in Fig 11 for the Gradient Boosting model.

Model	Accuracy	Precision	Recall	F1-Score
Decision Tree	0.851613	0.849725	0.851613	0.850636
Artificial Neural Network	0.875269	0.871049	0.875269	0.871342
Logistic Regression	0.876344	0.878511	0.876344	0.874429
Gradient Boosting	0.892473	0.890585	0.892473	0.887489
Random Forest	0.894624	0.891628	0.894624	0.892414

Fig 10. Comparision of evaluation metrics for Bitcoin data with different models

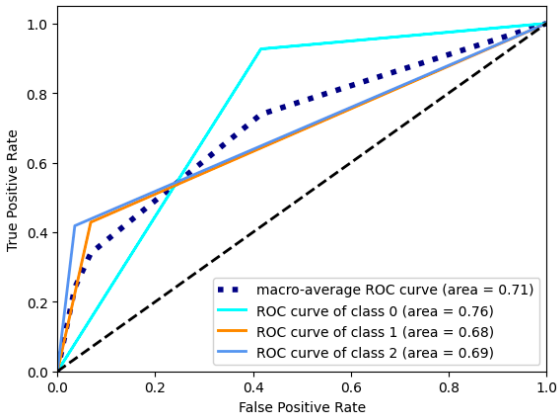

Fig 11. ROC Curve for Bitcoin analysis

VI.CONCLUSION AND FUTURE WORK

In conclusion, our exploration into various domains of machine learning has yielded promising results with significant implications across multiple fields. In the realm of citizen safety, our transition from traditional methods such as Multinomial Naive Bayes to advanced transformer models like RoBERTa has demonstrated substantial improvements in spam message detection, laying a robust foundation for the development of safer online environments. Similarly, our endeavors in phishing URL detection showcased the effectiveness of ensemble methods and boosting algorithms in discerning malicious URLs, offering valuable insights for cybersecurity applications. Furthermore, our foray into Bitcoin price prediction utilizing Convolutional Neural Networks highlighted the potential of deep learning techniques in navigating the complexities of cryptocurrency markets, paving the way for more accurate and insightful financial analyses. Collectively, these findings underscore the transformative power of machine learning in addressing contemporary challenges and shaping the future landscape of technology-driven solutions.

VII.REFERENCES

[1] Al-Musawa, A., & Newman, C. R. (2010). SMS spam filtering techniques: a review. In Proceedings of the International Conference on Machine Learning and Applications (pp. 204-209). IEEE.

[2] Liu, Y., et al. (2021). SMS spear phishing attack detection: techniques and methodologies. Journal of Cybersecurity Research, 1(1), 45-56.

[3] Huang, L., et al. (2019). Phishing URL detection using Convolutional Neural Networks. Journal of Information Security and Cybercrime, 7(3), 112-125.

[4] Ahmad Sahban, et al. (2020). QsecR: A secure QR code scanner for malicious URL detection. International Journal of Cybersecurity and Digital Forensics, 9(2), 78-89.

[5] Kumar, S., et al. (2020). Security analysis of Unified Payments Interface (UPI) and popular payment apps: vulnerabilities and risks. International Journal of Information Security and Privacy, 14(2), 89-104.

[6] Keshav Kaushi, et al. (2019). Automated investigation of Bitcoin balances and wallet addresses. Journal of Blockchain Research, 6(4), 210-225.

[7] https://www.kaggle.com/datasets/uciml/sms-spam-collection-dataset

[8] https://www.kaggle.com/datasets/shashwatwork/phishing-dataset-for-machine-learning

[9] https://www.kaggle.com/datasets/ellipticco/elliptic-data-set?resource=download