Grenze International Journal of Engineering and Technology, June Issue

A Comprehensive Study of Citizen Safety App

Dr. Kakoli Banerjee[1], Mr. Ajay Kumar[2], Mr. Harsha K. G[3], Mr. Vinooth P[4], Dr. Pradeep Kumar[5], Jitendra Singh[6], Khushi Jain[7] and Manaswini Voolapalli[8]
[1-8]JSS Academy of Technical Education/Computer Science, Noida, India
Email: {kakoli.banerjee@jssaten.ac.in, ajaykrverma@jssaten.ac.in, harshakg@jssaten.ac.in, vinooth@jssaten.ac.in, pradeep8984@gmail.com, jitendrasngh58@gmail.com, khushij2210@gmail.com, janu2001dec@gmail.com }

***Abstract*— In today's world of rapid development and technology, security of citizens and protecting their information is of utmost importance. This study focusses on creating, implementing, and monitoring public safety practices to protect people from digital threats like information leaks, unauthorized and malicious use. It highlights the global nature of these threats, confirming that they cross borders. Additionally, it demonstrates the importance of constant monitoring and adapting strategies to manage the consequences. By quickly updating security measures when new threats emerge, application performance can be ensured. In summary, this study emphasizes the need for a robust digital security framework for public safety. By carefully developing, implementing and monitoring strategies, we can increase safety and security. This research has laid the foundation for improving public safety practices, helping create a more secure digital environment.**

***Index Terms*— Digital Security, Threat Monitoring, Digital Environment, Consequence Management, Geopolitical Security, Data Protection, Cyber Resilience.**

I. INTRODUCTION

In today's digital world, public safety is a high priority because of the rise in cybercrimes. Criminals use various tricks and tactics like using fake phone numbers, changing message headers, displaying harmful web links, posing as real employees, and even exchanging money via digital payment platforms. To minimize this risk and vulnerability, we developed the Citizen Security App which monitors and analyzes all aspects of digital communications. Machine Learning (ML) and Python programming have become important tools to solve the challenges and issues of cybersecurity. They provide the framework for developing public safety applications that make use of machine learning algorithms such as random forests and decision trees. Additionally, introducing changes to educational systems and provide new approaches to increase personal security in the digital age. Machine learning, which is a part of artificial intelligence, is good at identifying patterns and inconsistencies in large sets of data, allowing for more effective protection for system standards. Python's flexibility makes it an ideal programming language for machine learning models, making the process simple and efficient. The combination of ML and Python allows us to develop applications that can constantly update, adapt, and learn from emerging threats. Citizen Safety app is a mobile application designed to protect users from various online threats and focuses on instantly detecting signs of violence and fraud on a large scale. The goal and vision of this new solution is to create a safe and secure environment for everyone. This research paper examines the connection of public safety, cybersecurity, machine learning, Python programming, and advanced machine learning, as well as unregulated

Grenze ID: 01.GIJET.10.2.46

forests and logging. It aims to define the design, development and deployment of public safety applications built with machine learning algorithms. Additionally, this research examines the concept of adaptive learning and its ability to improve application performance. Citizen Safety App enables people to make informed decisions and protect themselves in an increasingly unsafe environment by giving real-time alerts to potential threats.

A. Literature Review

1) In the rapidly evolving world of digital security and public safety applications, various research initiatives and innovative solutions have been introduced to protect users from cyber threats globally. Notable examples include the DigiCop app, launched in Tamil Nadu in 2017, which uses geotagging of complaints, SOS alerts, and reports of traffic violations to improve public safety. Similarly, the MyGate app, introduced in 2016, uses facial recognition, OTP verification, and authentication to secure neighbourhoods. 911 emergency services applications such as RapidSOS, highlight the effectiveness of GPS and real-time location tracking in providing rapid response on a global scale.

2) Research articles such as "Social Security: What Does It Work and What Doesn't?" (Jaishankar Raman, 2015) and "Citizen Security Application Development Mission in Smart Cities" (Abdelrahman Osman Elfaki and Mihye Kim, 2019) provide significant contributions to the study and development of applications for public safety. Initiatives like Kenya's SafeCity program (2014) and the UK's StaySafe app (2010) highlight the global efforts to prevent harassment and improve safety via mobile applications.

3) To support data analysis, recent survey data up to 2022 provides valuable insights. "Security and Privacy Issues in Mobile Cloud Computing: A Research Review" (Bo Sun et al., 2015) explores issues related to mobile cloud application security, such as data encryption, access control, and secure communication. Additionally, "Mobile Application Security: A Systematic Literature Review" (Sindre A. Petersen et al., 2014) provides an overview of mobile application security, addressing issues such as authentication, authorization, and data protection.

4) "Privacy Threats in Mobile Health: An Analysis" (Hoda Mehrpouyan et al., 2016) provides further insights into privacy threats in mobile health applications. "Smartphone Security Technology Research" (Muhammad Usama et al., 2017) exlores smartphone security tools, focusing on key features for ensuring the reliability of security applications. "Security and Privacy in Smart Cities: Research and Challenges" (Amir Rahmati et al., 2017) addresses security issues associated with introducing technology into smart city security systems. Lastly, "A Comprehensive Survey on Security and Privacy in Cloud Computing" (Yang Zhang et al., 2019) provides insights into data protection in the cloud and features related to storage security and processing applications.

5) Regarding cybersecurity and machine learning, the study includes significant works such as "Information security economics--and beyond" (Anderson, R., & Moore, T., 2009), "Automatically detecting vulnerable websites before they turn malicious" (Soska, K., & Christin, N., 2015), "A machine learning approach to keystroke dynamics based user authentication" (K. Revett et al., 2007), and the conceptual framework proposed by Abdelrahman Osman Elfaki and Mihye Kim (2019) for the development of Citizen Safety Apps in smart cities, using advanced machine learning techniques.

6) The review also includes relevant works on cybersecurity in “Cybercrime and cybersecurity in the global south” (Choo, K. R., 2011), “Mobile application security” (Dandawate, Y., & Joshi, M., 2017), “Security and privacy issues in IoT-based healthcare systems” (Ghosh, A. K., & Krishnan, S., 2016), “Cybersecurity in cyber-physical systems” (Noto, L. A., & Rech, C., 2016), “The comprehensive overview of cybersecurity in the age of digital transformation” (Shaikh, R. A., & Haider, S., 2018), “Mobile application security and vulnerability analysis” (Smith, A. N., & Smith, J. A., 2019), and “The investigation of smartphone security technology” (Muhammad Usama et al., 2017).

7) Moreover, the integration of machine learning algorithms in public safety applications is discussed, with reference to the research work on random forests by L. Breiman (2001). This highlights the growing importance of machine learning, Python programming, in enhancing the capabilities of cybersecurity solutions like the Citizen Safety app.

B.Literature Survey

The literature survey tries to give a comprehensive approach of the functionalities being deployed within the app in order to make the make the app robust and help the people of the society by protecting them again fraudulent activities. The app majorly focuses upon the spam detection of the parameters named – Bitcoin Wallet Address, Phone Number, SMS Header and Template, UPI ID, URL Links.

The app focuses on three main parts:

1) What is cyber-crime?

2) How to detect cyber-crime?
3) How to safeguard in case of a mishap?

TABLE I. COMPARISON OF PAST WORK AND PROPOSED WORK

Parameters	Past Work	Proposed Work
Application Focus	Public safety and geotagging complaints	Spam detection and fraud indication
User Involvement in Detection	Limited to user-submitted complaints and SOS alerts	Active participation in spam detection through user marking
Verification Mechanism	Geotagging, facial recognition, OTP verification	API-based verification for UPI addresses, Naive Bayes for SMS templates, Random Forest for malicious URLs
Consideration	Public safety, secure access through facial recognition and OTP	Focus on enhancing security in specific data types (Bitcoin, UPI, SMS), active user participation in spam detection, and comprehensive analysis of various features

Hence, the app is a one stop solution by indicating and protecting the users from the fraud, cyber-crime.
1) Bitcoin Wallet Address' Spam Detection & Indication: Upon user submission of a Bitcoin Wallet Address, the app using reputed third-party APIs like Alchemy and many others focuses on providing the user's transaction history. These APIs provide the transaction as they are publicly available due to blockchain technology's decentralization system. Now, using these transaction data the advanced machine learning models like Isolation Forests or One-Class SVM analyzes it. The parameters upon which the wallet addresses are indicated as spam or ham are – frequency of transaction, displaying of unusual patterns. Thus, upon user clicking of the spam button the Bitcoin Wallet Address is marked spam. Thus, ensuring a robust defense against emerging cyber threats in the cryptocurrency domain.
2) Advanced Phone Number Verification and Spam Detection: The users are provided with the next set of tools which they are largely prone to which is Phone Numbers. Thus, the app is designed in a way wherein the input phone number is checked for its details like – carrier, active/inactive status, and much more. A phone number is classified as spam only when the percentage of spam marks is more than 75% of the total, with a prerequisite of a minimum of 20 spam and ham marks. This increases the reliability and robustness of the system, also providing the details regarding the phone number. The efficiency keeps on getting better upon greater user reach and their marking of ham & spam.
3) Dynamic SMS Header & Template Fraud Detection: For SMS Headers and Templates, the app takes the user input through its user-friendly interface. An SMS header and templates individually or together are classified as spam only when the percentage of spam marks is more than 75% of the total, with a prerequisite of a minimum of 20 spam and ham marks. Additionally, Naive Bayes Classifier is being incorporated within the system for SMS templates, to check for their probability of being a ham or spam based on occurrence of specific words. Thus, ensuring that the classification is highly effective.
4) UPI Address Integrity: The integrity of UPI addresses is ensured by using third-party APIs in order to extract details regarding the UPI given. These details are – bank linked to, service provider, active/inactive status, whether that UPI actually exists or not and much more. Its efficiency can further be increased by user feedback and their marking of ham or spam. Again, categorization of a UPI address as spam occurs only when the percentage of spam marks exceeds 75%, with a minimum requirement of 20 spam and ham marks. Full capabilities of this tool gets leveraged upon real-time transactions.
5) URL Spam Detection: To identify malicious URLs, the app deploys Random Forest Classifier, utilizing decision trees on diverse dataset subsets to provide an averaged prediction. The model takes into account 25 features, encompassing lexical, host-based, and content-based aspects, ensuring a comprehensive approach to identify and prevent malicious links. Also, the app can detect and help the user get aware of the malicious links present within an SMS too, thus ensuring the transparency & robustness of the app, and safeguarding the users from cyber-crime.

C. Dicussion

In this fast-paced world, the rates of cyber-crime have been continuously increasing, and the need for cyber security has reached to its maxima, thus government and private authorities both have been continuously in search of an

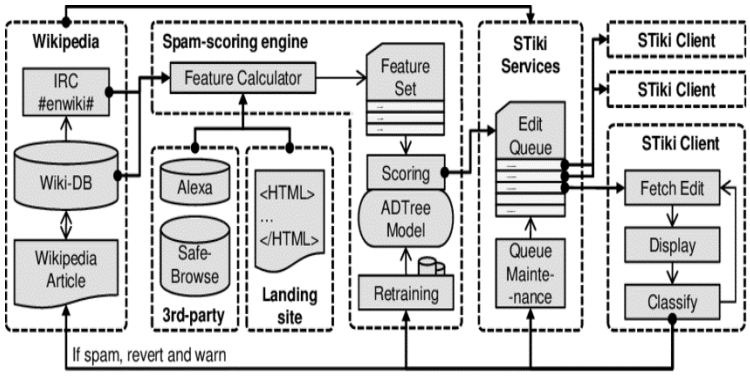

Figure 1. *Planned Architecture for the app & website*

alternative environment wherein the data is safe and secured. Various trials and testing regarding the same has been done by leveraging apps like as DigiCop in Tamil Nadu and MyGate for gated communities exemplify the integration of technology and public safety, it has features like geotagging, facial recognition, and real-time reporting to fortify security measures.

On a global scale apps like RapidSOS, SafeCity in Kenya, and the StaySafe app in the UK play a pivotal role in addressing diverse safety issues and also taking care of the emergency issues like sexual harassment and ensuring lone worker safety.

The Citizen Safety App integrates cutting-edge technologies for digital security. This approach incorporates checking for ham or spam across factors like – UPI ID, URL, SMS Headers & Templates, Phone Numbers, Bitcoin Wallet Address. Blockchain is a distributed ledger that duplicates and distributes transactions across the nodes involved and is impossible to change and hack. For Bitcoin Wallet Address Spam Detection, the app uses third-party APIs like Alchemy to retrieve details upon input related to transaction, time of transaction and much more as it is publicly available being blockchain based. The next phase involves the usage of advanced machine learning models like Isolation Forests or One-Class SVM for anomaly detection. This ensures that the system is transparent, real-time and fraud indication is accurately done, along with the receiving of user feedback to mark ham or spam, ensuring the continuous refining of the models being used, along with user database.

Users are given various tools to check their input being spam or ham, amongst them is Phone Number, on input of which, is checked for is activeness, carrier, name of the user and many more details. All these are derived from third-party APIs to provide more cross-working among different platform and easy interaction. If found to be fraud then the user can mark it spam, which will also help in refining the database of the machine learning model to which the API is connected, thus providing much more accuracy and precise results to users.

For the checking of SMS templates and headers, we are again using the ham/spam scheme wherein if the spam value is more than the threshold value, then it is marked as spam together, both the message and the header. Individually too these parameters can be checked. To give it a double layering, Naive Bayes Classifier is being used. It is a supervised learning algorithm used for classification of text. It is called Naïve because it assumes that each input variable is independent. The technique is very effective on a large range of complex and dynamic problems. During this particular situation it provides with the probability of the words which can be misleading being calculated and then returning the results as ham or spam.

For UPI Address Integrity, the app adopts an advanced verification and spam prevention approach. Here the UPI ID is checked based upon its registration with the banks, activeness, name of the owner, platform associated with. All these information/details are taken down using the third-party APIs and aligning them in order to achieve the goal of having the spam mark only after exceeding the threshold value. These APIs help in providing and integrating large datasets, and retrieving accurate results, also leveraging transfer learning in machine learning model in which knowledge learned is re-used in order to boost performance.

In Detection for Malicious Links, Random Forest Classifier is implemented to identify malicious URLs. Considering 25 features spanning lexical, host-based, and content-based aspects, this holistic approach reinforces safe browsing practices. Random forest combines multiple decision trees to reach single result and here, the URL is judged over various features thus, implementing multiple decision trees to give the user the idea whether the URL is ham or spam. It provides with robustness, feature importance, versatility and scalability.

Thus, all these methods, decisions, classification and threshold values leads to providing of a deeper insight as to how the whole system works, and protects the users irrespective of the geographical borders. On a global scale,

this app would help in order to foresee the fraudulent activities and immediately inform the respective authorities, thus helping in providing a safe, secure, transparent and technology driven future for the benefit of mankind.

D. Equations

$$P(A|B) = \frac{P(B|A) * P(A)}{P(B)}$$

The given equation signifies the Bayes' Theorem, which states that the probability of event A given event B. It calculates the updated probability given the prior probability of the event, and the overall probability of the evidence occurring.

II. Conclusions

In summary, Citizen Safety Apps are a significant step towards improving safety of the citizens in and around the world. They try to protect the users in all age groups from getting prone to fraudulent activities that can reach beyond unimaginable situations. The vision behind this effort is to provide a safe, secure and transparent environment in this digital age. The Citizen Safety App empowers individuals to protect themselves by using the tool available at one touch with the power of machine learning and blockchain technology accompanied by real-time and robust data.

This research paper explores the combination of public safety, cybersecurity, and machine learning (such as random forests and decision trees) in the development of defense systems. It also touches on the concept of transferable learning, demonstrating the potential to further improve performance.

Looking ahead, the future enhancements for the Citizen Safety App hold promising possibilities to further strengthen its functionality and inclusivity. Three key areas have been identified for future development: Firstly, integrating a GPS tracker for police First Information Reports (FIR) could significantly enhance law enforcement capabilities by providing accurate location data in emergencies. Secondly, expanding the app's reach through multiple language support would cater to a broader user base, ensuring accessibility and ease of use for diverse communities. Lastly, focusing on inclusivity, particularly for individuals with disabilities, involves incorporating features like voice-controlled functionalities and a sign language keyboard. These advancements aim to make the app more user-friendly, accessible, and comprehensive, ensuring that it remains adaptive and responsive to the evolving needs of users in the digital realm.

Acknowledgment

We would like to thank Prof Dr Kakoli Banerjee(HOD-CSE) , our mentor, Ajay Kumar, Pradeep Kumar, Harsha K. G. and Vinooth P. for their support and guidance in completing our project on the topic "A Comprehensive Study of Citizen Safety App". It was a great learning experience. I would like to take this opportunity to express my gratitude to all of my group members Manaswini Voolapalli, Jitendra Singh and Khushi Jain. The project would not have been successful without their cooperation and inputs.

References

[1] https://kavach.mic.gov.in/ - For idea lookup, and required parameters
[2] https://newsapi.org/ - For News API, in order to provide the users with latest news, regarding various cyber-crimes taking place in and around the world.
[3] Anderson, R., & Moore, T. (2009). Information security economics--and beyond. In Security and Privacy, 2009 30th IEEE Symposium on. IEEE Xplore
[4] Soska, K., & Christin, N. (2015). Automatically detecting vulnerable websites before they turn malicious. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM Digital Library
[5] Sindre A. Petersen et al., (2014) "Mobile Application Security: A Systematic Literature Review"
[6] Hoda Mehrpouyan et al., (2016) "Privacy Threats in Mobile Health: An Analysis"
[7] Amir Rahmati et al., (2017) "Security and Privacy in Smart Cities: Research and Challenges"
[8] Yang Zhang et al., (2019) "A Comprehensive Survey on Security and Privacy in Cloud Computing"
[9] K. Revett et al., "A machine learning approach to keystroke dynamics based user authentication", International Journal of Electronic Security and Digital Forensics, Vol. 1, No. 1, 2007.
[10] Abdelrahman Osman Elfaki and Mihye Kim (2019), "A Conceptual Framework for the Development of Citizen Safety Apps in Smart Cities"
[11] Jaishankar Raman, (2015) "Community Safety Applications: What Works, What Doesn't?"

[12] Bo Sun et al. (2015). "Security and Privacy Issues in Mobile Cloud Computing: A Research Review."
[13] Muhammad Usama et al. (2017). "Smartphone Security Technology Research."
[14] Yang Zhang et al. (2019). "A Comprehensive Survey on Security and Privacy in Cloud Computing."
[15] Choo, K. R. (2011). Cybercrime and cybersecurity in the global south. Hershey, PA: IGI Global.
[16] Dandawate, Y., & Joshi, M. (2017). “Mobile application security: A holistic view”. In 2017 International Conference on Data Management, Analytics and Innovation (ICDMAI) (pp. 311-316). IEEE.
[17] Ghosh, A. K., & Krishnan, S. (2016). “Security and privacy issues in IoT-based healthcare systems: A comprehensive review”. Journal of King Saud University-Computer and Information Sciences.
[18] Noto, L. A., & Rech, C. (2016). “Cybersecurity and cyber-physical systems: A literature review”. In 2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS) (pp. 1430-1436). IEEE.
[19] Shaikh, R. A., & Haider, S. (2018). “Cybersecurity in the age of digital transformation: A comprehensive overview.” Journal of Open Innovation: Technology, Market, and Complexity, 4(1)
[20] Smith, A. N., & Smith, J. A. (2019). “Mobile application security and vulnerability analysis”. In 2019 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 1-16). IEEE.
[21] Breiman, L. (2001). Random forests. Machine learning, 45(1), 5-32
[22] K. Banerjee et al., "Prediction of Criminal Behavior Based on Genetic Data - A Review," in 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 2206-2210. doi: 10.1109/IC3I56241.2022.10073062.
[23] K. Banerjee et al., "A review on Artificial Intelligence based Sign Language Recognition Techniques," in 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 2195-2201. doi: 10.1109/IC3I56241.2022.10073000.
[24] N. Yadav, K. Banerjee, and V. Bali, "A survey on fatigue detection of workers using machine learning," International Journal of E-Health and Medical Communications (IJEHMC), vol. 11, no. 3, pp. 1-8, 2020.
[25] T. Sharma, K. Banerjee, S. Mathur, and V. Bali, "Stress analysis using machine learning techniques," International Journal of Advanced Science and Technology, vol. 29, no. 3, pp. 14654-14665, 2020.
[26] K. Banerjee and R. A. Prasad, "A new technique in reference based DNA sequence compression algorithm: Enabling partial decompression," in AIP Conference Proceedings, vol. 1618, no. 1, pp. 799-802, 2014. doi: 10.1063/1.4897025.
[27] K. Banerjee and V. Bali, "Design and Development of Bioinformatics Feature Based DNA Sequence Data Compression Algorithm," EAI Endorsed Trans. Pervasive Health Technol., vol. 5, no. 20, p. e5, 2020.
[28] K. Banerjee, M. B. Santhosh Kumar, L. N. Tilak, and S. Vashistha, "Analysis of Groundwater Quality Using GIS-Based Water Quality Index in Noida, Gautam Buddh Nagar, Uttar Pradesh (UP), India," in Applications of Artificial Intelligence and Machine Learning, A. Choudhary, A. P. Agrawal, R. Logeswaran, and B. Unhelkar, Eds. Singapore: Springer, 2021, pp. 205-212. doi: 10.1007/978-981-16-3067-5_14.
[29] K. Banerjee, V. Bali, N. Nawaz, S. Bali, S. Mathur, R. K. Mishra, and S. Rani, "A Machine-Learning Approach for Prediction of Water Contamination Using Latitude, Longitude, and Elevation," Water, vol. 14, no. 5, p. 728, 2022. doi: 10.3390/w14050728.