# Uncovering Insecurity Hotspots In Rwanda Through Twitter Analytics

Igiraneza Ishimwe Nicole
Information Technology
Carnegie Mellon University
nii@andrew.cmu.edu

Bwiza Dalia
Carnegie Mellon University
Electrical and Computer Engineering
bdalia@andrew.cmu.edu

Daniel Ephraim Maduhu
Information Technology
Carnegie Mellon University
dmaduhu@andrew.cmu.edu

Uwamahoro Joyeuse
Information Technology
Carnegie Mellon University
juwamaho@andrew.cmu.edu

***Abstract*—Insecurity remains a critical concern in Rwanda, which requires innovative approaches for real-time assessment and mitigation strategies. Traditional methods often fail in capturing dynamic security sentiments. This project proposes a machine learning-based system that uses Twitter data analytics to identify insecurity hotspots and categorize incidents in Rwanda. The system collects, preprocesses, and analyzes tweets using natural language processing techniques, geolocation data, and severity assessment models. By mapping identified incidents in an interactive visualization tool, stakeholders gain actionable insights to improve situational awareness and informed decision making within Rwanda. The project. methodology, validation results and deployment guide contribute to effectively addressing security challenges in Rwanda.**

***Index Terms*—security analytics, twitter data analysis, machine learning, geospatial analysis, natural language processing.**

## I. Introduction

Rwanda has faced persistent security challenges, including rape, robbery, and murder, highlighting the critical need for improved monitoring and response mechanisms. The traditional way of reporting crimes involves individuals directly contacting law enforcement agencies or local authorities, which can lead to delays in information gathering and response coordination. This approach faces challenges such as underreporting due to fear of repercussions or lack of trust in the reporting process. Furthermore, the lack of real-time data and localized insights hinders effective decision-making and resource allocation to address security incidents. In Rwanda, a significant proportion of crimes, estimated at 60%, remain unreported [1], causing increased public safety concerns. This gap in timely reporting and response contributes to the persistence of insecurity issues in various regions in Rwanda.

There has been a notable increase in Twitter users in Rwanda, with a 34. 6% increase from early 2022 to early 2023 [2]. In early 2023, Twitter had approximately 218.4 thousand users in Rwanda [3]. Twitter has become a platform where individuals share information, including reports of security incidents, often providing real-time updates. Understanding how people use Twitter to report crimes, including the timing of posts after incidents, can provide valuable information on enhancing security monitoring and response strategies.

Using the growing Twitter user base and analyzing tweet content related to security incidents, this project aims to bridge the gap between timely reporting and response to security threats in Rwanda. The integration of machine learning and data analysis techniques will enable the identification of insecurity hotspots and the classification of incident types, ultimately contributing to improved situational awareness and more effective risk mitigation strategies.

## II. PROBLEM STATEMENT

In Rwanda, persistent security challenges, including high rates of unreported crimes such as rape, robbery, and murder, underscore the critical need for improved monitoring and response mechanisms. Traditional methods of reporting crimes often result in delays, under-reporting due to fear or lack of trust in the reporting process, and a lack of real-time data and localized insights. These challenges contribute to the persistence of security issues in various regions, indicating a significant gap in timely reporting and response to security threats.

## III. Aims and Objectives

### A. *Aims*

This project aims to develop a machine learning system capable of analyzing tweets to identify and categorize insecure areas in Rwanda.

### B. *Objectives*

1) Collecting and Preprocessing tweets using natural language processing techniques to extract relevant information.
2) Develop a severity assessment model to categorize the severity of security-related tweets
3) Incorporate geolocation data to map identified security hotspots in Rwanda
4) Create an interactive map visualization tool to enhance interpretability and user engagement.
5) Evaluate the performance and effectiveness of the machine learning system in identifying security risks and classifying incidents using appropriate metrics and validation techniques.

## IV. Methodology

This study aims to leverage the power of social media data and natural language processing techniques to analyze and visualize security incidents and criminal activities in Rwanda. By collecting and processing tweets related to security concerns, the study employs a comprehensive methodology that encompasses data collection, preprocessing, natural language processing, severity assessment, and geospatial analysis.

### A. *Data Collection and Pre-processing*

The methodology begins with the acquisition of Twitter data using a Google Chrome extension known as Tweet Scraper. This tool facilitates the collection of tweets from Rwanda that are relevant to security incidents and criminal activities. The gathered data is subjected to thorough preprocessing steps, including noise removal and standardization, to ensure data quality and consistency. Essential features such as timestamps and optional geospatial information are extracted from these tweets to form a structured dataset for analysis.

### B. *Natural Language Processing (NLP)*

As part of the data preparation process, natural language processing (NLP) techniques are utilized to sort tweets into distinct categories of security incidents. Neural Machine Translation (NMT) systems such as Google Translate are employed to translate tweets, and libraries like TextBlob and Spacy are used for word tokenization, which breaks down text into individual words or tokens. This process simplifies the analysis and categorization of crimes into three types based on the content of the tweet. These NLP-driven methods enable the classification of tweets based on the type of security threat they indicate, whether it's murder, rape, or robbery.

### C. Severity Assessment

The TextBlob sentiment analysis tool is employed to evaluate the severity of crimes reported on Twitter. TextBlob assigns a polarity score ranging from -1 to 1 to each piece of text, where -1 represents a highly negative sentiment, 0 represents a neutral sentiment, and 1 represents a highly positive sentiment. Thresholds are established for these polarity scores to categorize the tweets into different levels of severity. For instance, tweets with polarity scores below a certain negative threshold are classified as indicating a high-severity crime, while those with scores closer to 0 are classified as medium-severity, and tweets with positive scores are considered low-severity. Following the setting of these thresholds, a new column is added to the dataset that indicates the severity level for each tweet. This systematic approach enables the effective determination of the severity of security-related tweets and their subsequent classification for further analysis.

### D. Geospatial Processing and Map Visualization

A crucial component of the methodology (Figure 1) is geospatial processing, which is used to extract and validate geographical coordinates or location information from tweets. Geopy and Nominatim geocoders are utilized to map these geospatial data points, enabling the visualization of the distribution of security incidents across various regions of Rwanda. The combination of Folium and MarkerCluster libraries aids in the creation of an interactive map visualization tool. This tool not only spatially presents identified security incidents, but also customizes markers and clusters based on crime types, interaction levels, and geographical locations, thereby enhancing the interpretability and user engagement of the visualization.

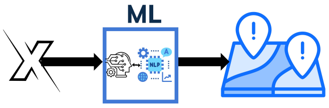

Fig. 1: Geospatial Processing and Map visualization

## V. Literature Review

Several studies have explored the use of social media data for crime analysis and prediction. Wang et al. [8] used Twitter data to infer crime rates in US cities, demonstrating the potential of social networks as a complementary data source. They found that incorporating Twitter data improved the accuracy of crime rate predictions compared to using only traditional data sources. Bendler et al. [9] investigated the relationship between Twitter activity and crime incidents in San Francisco. They discovered that certain types of Twitter posts, such as those expressing negative emotions, were associated with higher crime rates in specific areas. This suggests that analyzing the content of tweets can provide insight into crime patterns.

Gerber [10] developed a method for predicting crime using Twitter data and kernel density estimation. By analyzing the spatial and temporal patterns of tweets, the study showed that Twitter data could be used to forecast crime hotspots in Chicago. This highlights the predictive power of social media data in crime analysis.

Kounadi et al. [11] explored the ethical considerations of using Twitter data for crime analysis. They emphasized the importance of protecting user privacy and anonymity when handling sensitive data. The study also discussed the potential biases and limitations of using social media data, such as the overrepresentation of certain demographics.

Aghababaei and Makrehchi [12] proposed a framework for crime prediction using Twitter data and machine learning techniques. They used natural language processing to extract crime-related features from tweets and trained models to predict crime occurrences. The results showed promising accuracy in predicting various types of crime.

Huang et al. [13] analyzed the spatial and temporal patterns of crime-related tweets in Houston, Texas. They found that the density of crime-related tweets was higher in areas with higher crime rates reported by official data. This study demonstrated the potential of using Twitter data to identify crime hotspots and complement traditional crime mapping methods.

Mata and Quesada [14] used Twitter data to analyze the perception and fear of crime in Mexico City. They found that the sentiment expressed in tweets related to crime varied between different neighborhoods and time periods. This study highlighted the usefulness of social media data in understanding public perceptions of crime and safety.

Siriaraya et al. [15] investigated the relationship between Twitter activity and crime rates in different neighborhoods of Kyoto, Japan. They discovered that areas with higher Twitter activity, particularly during nighttime hours, tended to have higher crime rates. This study showed the potential of using social media data to identify high-risk areas and inform crime prevention strategies.

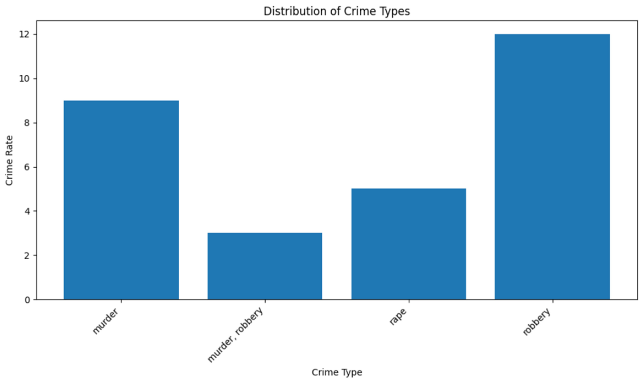

Fig. 2: Crime Type Distributions

## VI. Results and Discussion

The developed system successfully collected and analyzed a substantial volume of Rwandan crime-related tweets over a period from January 2021 to March 2024, which makes it [ 38 months or 3 years and a half ]. Geospatial location analysis revealed clusters of crime hotspots in major cities such as Kigali, as well as in certain rural areas, as shown in Figure 3. The interactive map visualization provided a user-friendly interface for exploring crime data. To differentiate the severity of incidents, a color mapping scheme was employed, where high, medium, and low interaction levels were represented by red, orange, and green markers, respectively. The color-coded markers and cluster information aids in identifying areas with high crime rates or specific crime types, while the bar chart as shown in figure 2 provides a visual representation of the distribution of crime types which are prevalence within Rwanda.This can enables police agencies in Rwanda and researchers to readily pinpoint high-risk areas and delve into specific incidents for further investigation. Furthermore, the incorporation of severity or seriousness ratings adds an additional layer of insight, underscoring the most critical cases necessitating urgent attention.

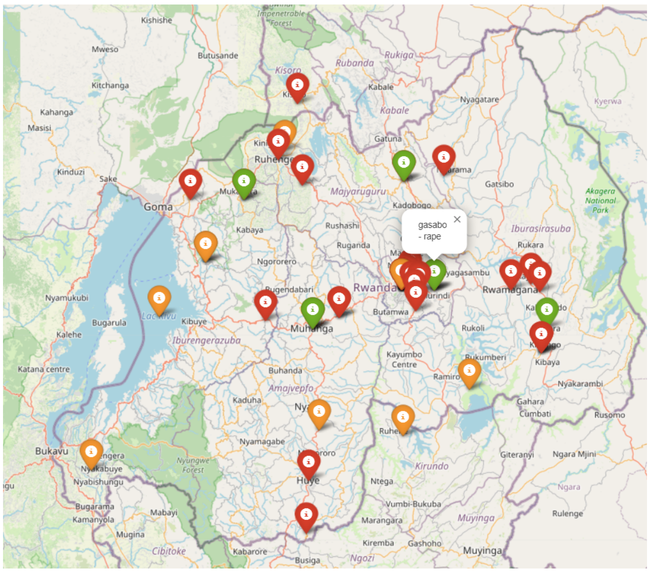

Fig. 3: Insecure Hot-spots in Rwanda

## VII. Challenges

However, the project faced several challenges and limitations. Firstly, the reliance on Twitter data means that the analysis is limited to crimes that are publicly reported on the platform. Many crimes may go unreported or unreported on social networks. Furthermore, the accuracy of geolocation data varies, as not all tweets contain precise coordinates. This can result in some incidents being mapped to incorrect locations or not being visualized at all.

Another challenge was the presence of outliers - tweets that mentioned Rwandan cities but referred to crimes occurring elsewhere. Manual inspection was required to filter out these irrelevant data points.

Despite these limitations, the project demonstrates the potential of Twitter analytics as a complementary tool for crime analysis. By outputting localized, real-time data, the police or any other person can gain a more comprehensive understanding of crime dynamics and allocate resources more effectively. The methodology developed here could be refined and extended to other countries and types of crime in future work.

## VIII. Conclusion

In conclusion, this project demonstrates the application of machine learning and geospatial/location analysis to uncover and map crime hotspots in Rwanda using Twitter data. By focusing on murder, robbery and rape incidents, our goal was to address some of the most pressing security concerns in the country.

The interactive visualization of the map, combined with severity ratings, provides a powerful tool for law enforcement and policymakers to identify high-risk areas and prioritize interventions. Although the project faced challenges related to data quality and representativeness, it highlights the potential of social media analytics to fill gaps in traditional crime reporting methods. Future research could expand the scope to include other East African countries and additional crime categories. Refine machine learning models, improve location extraction, and combine official statistics that could make the system more accurate and useful.

In conclusion, using the huge amount of information people post on social media sites such as Twitter, we can work toward building safer, more resilient communities in Rwanda and beyond.

## References

[1] D. Buil-Gil, J. Medina, and N. Shlomo, ‘Measuring the dark figure of crime in geographic areas: Small area estimation from the Crime Survey for England and Wales’, Br. J. Criminol., vol. 61, no. 2, pp. 364–388, Mar. 2021, doi: 10.1093/bjc/azaa067.

[2] ‘Digital 2023: Rwanda — DataReportal – Global Digital Insights’. Accessed: May 03, 2024. [Online]. Available: https://datareportal.com/reports/digital-2023-rwanda

[3] ‘Twitter users in Rwanda in 2023.docx - Twitter users in Rwanda in 2023 Numbers

published in Twitter’s advertising resources indicate that Twitter had — Course Hero’. Accessed: May 03, 2024. [Online]. Available: https://www.coursehero.com/file/222551445/Twitter-users-in-Rwanda-in-2023docx/

[4] Twint: An advanced Twitter scraping & OSINT tool written in Python. (2021). GitHub. https://github.com/twintproject/twint

[5] Jain, A., & Jain, N. (2018). Crime analysis using Twitter data. International Journal of Engineering and Technology, 7(3.34), 270-273. https://doi.org/10.14419/ijet.v7i3.34.18921

[6] Agarwal, S., & Sureka, A. (2015). Using a KNN and SVM based one-class classifier to detect online radicalization on Twitter. In R. Natarajan, G. Barua, & M. R. Patra (Eds.), Distributed Computing and Internet Technology (pp. 431-442). Springer International Publishing. https://doi.org/10.1007/978-3-319-14977-6$_4$7

[7] Singh, J. P., Dwivedi, Y. K., Rana, N. P., Kumar, A., & Kapoor, K. K. (2019). Classification of events and prediction of location from tweets during disasters. Annals of Operations Research, 283(1), 737-757. https://doi.org/10.1007/s10479-017-2522-3

[8] Wang, X., Gerber, M. S., & Brown, D. E. (2012). Automatic crime prediction using events extracted from Twitter posts. In S. J. Yang, A. M. Greenberg, & M. Endsley (Eds.), Social Computing, Behavioral-Cultural Modeling and Prediction (pp. 231-238). Springer. https://doi.org/10.1007/978-3-642-29047-3$_2$8

[9] Bendler, J., Ratku, A., & Neumann, D. (2014). Crime mapping through geo-spatial social media activity. Proceedings of the 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. https://doi.org/10.1109/ASONAM.2014.6921594

[10] Gerber, M. S. (2014). Predicting crime using Twitter and kernel density estimation. Decision Support Systems, 61, 115-125. https://doi.org/10.1016/j.dss.2014.02.003

[11] Kounadi, O., Ristea, A., Leitner, M., & Langford, C. (2018). Population at risk: Using areal interpolation and Twitter messages to create population models for burglaries and robberies. Cartography and Geographic Information Science, 45(3), 205-220. https://doi.org/10.1080/15230406.2017.1304243

[12] Aghababaei, S., & Makrehchi, M. (2017). Mining social media content for crime prediction. Proceedings of the 2017 IEEE/WIC/ACM International Conference on Web Intelligence. https://doi.org/10.1145/3106426.3106484

[13] Huang, C., Zhang, J., Zheng, Y., & Chawla, N. V. (2018). DeepCrime: Attentive hierarchical recurrent networks for crime prediction. Proceedings of the 27th ACM International Conference on Information and Knowledge Management. https://doi.org/10.1145/3269206.3271793

[14] Mata, F., & Quesada, A. (2020). Analyzing fear of crime using Twitter data. Proceedings of the 2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. https://doi.org/10.1109/ASONAM49781.2020.9381385

[15] Siriaraya, P., Wang, Y., Zhang, Y., Wakamiya, S., Jeszenszky, P., & Kawai, Y. (2019). Witnessing crime through tweets: A crime investigation tool based on social media. Proceedings of the 2019 IEEE/WIC/ACM International Conference on Web Intelligence. https://doi.org/10.1145/3358695.3360897