International Journal of Advance and Innovative Research
Volume 12, Issue 2 (XVII): April - June 2025

ISSN 2394 - 7780

CRIMINAL BEHAVIOR ANALYSIS PREDICTION MODEL: USING SOCIAL MEDIA

[1]Khushboo Rajesh Gupta and [2]Tejashree Parab
Department of MSc Big Data Analytics, Jai Hind College (Empowered Autonomous), Mumbai, India

ABSTRACT

Social networking has dramatically transformed how people present themselves online, creating a massive repository of data that provides deep insights into personality traits and behavioral tendencies. The focus of this research paper is to evolve the criminal behavior prediction model by utilizing digital footprints on social media platforms such as Instagram to predict potential criminal behavior in real life. By analyzing the user-generated content like posts, comments, and interactions, this model is expected to detect trends, behavioral indications, and risk factors related to criminal behavior. This research paper looks at the analysis of criminal behavior and the patterns created on social media focus is on finding AI, forensic linguistics, and cybersecurity methods for detection and prevention. On the subject of online harassment, hate speech, and cybercrime, studies help to support the role of AI in criminal justice. This study illustrates how criminal elements both have a platform for nefarious activities and serve as a source for developing better means of digital law enforcement, providing insight into more efficient analyses of criminal behavior by AI.

Keywords: *Criminal Behavior, Social Media, Hate Speech, Online Harassment, AI in Criminal Justice, Cybersecurity, Forensic Linguistics, Digital Investigations*

I. INTRODUCTION

Social media allows for online interaction through platforms like Facebook, Twitter, TikTok, and Instagram, which have drastically changed how people interact, organize, and communicate. While these social media channels present immense benefits, they are accompanied by new problems such as cyberbullying, hate speech, and crimes committed over the internet, and therefore become a point of focus for criminal behavior analysis research in these arenas. The potentials encompass the use of artificial intelligence, machine learning algorithms, and cybersecurity techniques to discover harmful behaviors which can be used to predict and improve criminal acts while helping the process of criminal investigation.

This paper will discuss the relationship between criminal behavior and social media, as well as explore how AI technologies can be used to identify and predict such activities. This study will further reinforce AI tools in the recognition of hate speech, online harassment, and other forms of digital malfeasance, thereby contributing positively towards effective law enforcement in the digital era.

II. REVIEW OF LITERATURE

Forensic Linguistic Analysis of Hate Speech on Social Media

One of the key spheres of criminal behavior on social media is the eruption of hate speech. Available at https://biarjournal.com/index.php/biolae/article/view/894, the titled "Forensic Linguistic Analysis of Netizens' Hate Speech Acts in TikTok Comment Section" investigates the real amount of hate speech on TikTok, making linguistic analysis of features that characterize online hate speech. This work will attempt to apply forensic linguistic techniques towards distinguishing between the ways hate speech manifests in online spaces and gain insights into the possible training of AI toward this end.

Forensic linguistics provides an invaluable methodology to differentiate the type of dangerous content from each other while allowing AI to distinguish them better in terms of labeling and response, making such hate speech detection in digital platforms even more effective when done through the means of AI.

Online harassment and cyber victimization of social media influencers

The paper "Too Lucky to Be a Victim? An Exploratory Study of Online Harassment and Hate Messages Faced by Social Media Influencers"

Addresses specific issues that social media influencers face, who are increasingly becoming targets of cyberbullying, defamation, and other forms of online threats. More than 70% of influencers confessed receiving hate messages and threats, which tells us that it is a widespread problem leading to mental and physical harm.

These threats can be mitigated with the help of AI-driven systems by analyzing patterns of online harassment and providing real-time alerts to influencers and their teams. Using AI to foretell potential escalation of threats and recommend preventive measures in terms of content filtering and enhanced privacy settings thus maintains a relatively safer environment online for the influencer.

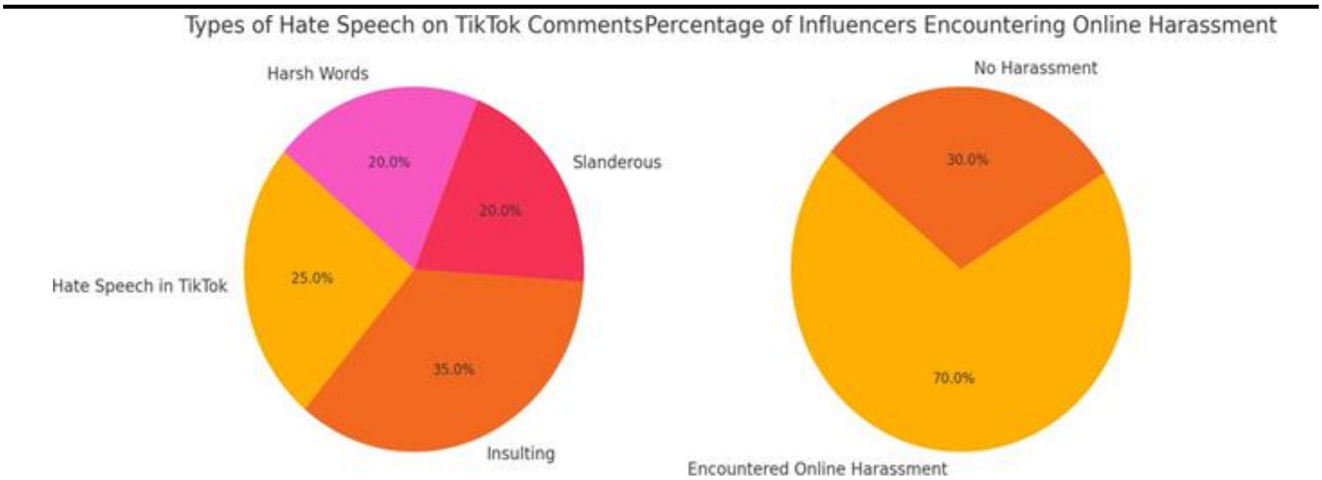

Fig. 1: Type of Hate Speech on TikTok Comments Percentage of Influencers Encountering Online Harassment

DIGITAL CRIMINAL INVESTIGATIONS AND AI

In "Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview" there is an opportunity of AI enhancing digital criminal investigations. This is because AI would be able to analyze larger datasets and allow law enforcement agencies to identify patterns, track offenders, and detect criminal behavior at its onset. Machine learning algorithms are increasingly being used to identify fraudulent activities, predict recidivism, and get into details of digital evidence more efficiently.

This paper uses various case studies of AI tools deployed in criminal investigations, such as finding cybercrime syndicates and tracking illegal activities on the dark web. This makes it possible for law enforcement agencies to make decisions quickly and accurately, leading to a more proactive approach to digital crime.

CYBER SECURITY FOR CHILDREN IN SOCIAL MEDIA

The article "Cybersecurity for Children: An Investigation into the Application of Social Media" https://www.tandfonline.com/doi/epdf/10.1080/17517575.2023.2188122?needAccess=true involves the dangers young people face in social media and how they expand with children's log-in activities to the internet. Cyberbullying, sexting, and identity theft increase with increasing children online. AI can be applied in the observation of children's activities online, tracking dangerous signals, so sending alerts to parents or guardians.

AI-based cybersecurity technologies can also save kids from the clutches of net predators by making the online world safe. The use of machine learning algorithms will be involved in identification of inappropriate content, marking probable threats, and making sure that the social media sites are safe for children.

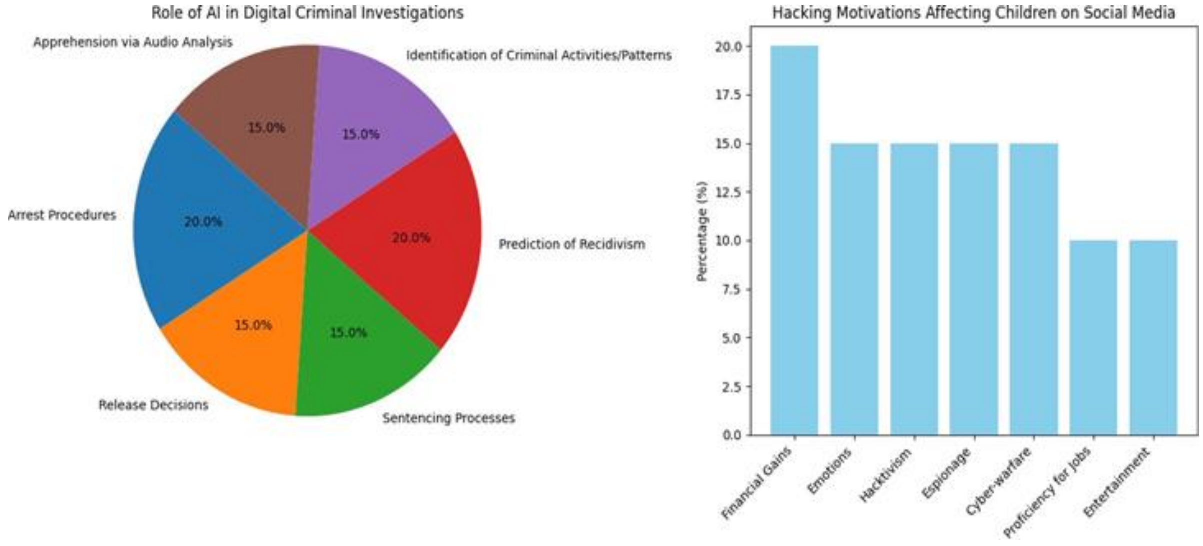

Fig.2: Role of AI in Digital Criminal Investigations

III. RESEARCH METHODOLOGY

This study has combined qualitative and quantitative approaches to shed light on criminal behavior on social media and the use of AI in identification and intervention of such activities. The components of this methodology are as follows:

Literature Review Through a comprehensive literature review on contemporary works focused on hate speech, online harassment, cybercrime, and AI-driven analysis of criminal behavior, the authors set the premise and help in identifying gaps that have emerged in the literature.

Case Studies: Specific examples of online harassment, hate speech, and cybercrimes are examined so that the scope and implications of these behaviors can be understood. The case studies highlight how criminal activity finds a medium through social media platforms and how AI tools might fight these issues.

AI and Machine Learning Models: In the study, AI models and machine learning algorithms are used to detect and prevent criminal behavior on social media through the mediums of content moderation tools, predictive analytics, and real-time monitoring systems.

Cybersecurity Analysis: AI-powered cybersecurity tools that can be integrated into social media to use them to provide safety for the users by engaging on vulnerable platforms, such as children, social media influencers, among others.

IV. DATA MINING TECHNIQUES

1. Sentiment Analysis

Purpose: Identify the sentiment and tone of user-generated content, including posts, comments, and messages, to recognize hate speech, harassment, or criminal intent.

Methodology:
Natural Language Processing tools.

Algorithms: Naïve Bayes, Support Vector Machines (SVM), or transformer models like BERT.

Tools: Python libraries, including NLTK, TextBlob, VADER, or HuggingFace.

2. Text Mining

Purpose: Uncover valuable patterns from vast text-based data sources, such as social media comments, messages, and posts.

Topic Modeling: Find thematic trends by using Latent Dirichlet Allocation (LDA).

Identify keywords and phrases that are indicative of criminal behavior by using Term Frequency-Inverse Document Frequency (TF-IDF).

Group similar content using clustering techniques like K-Means, DBSCAN.

3. Predictive Modeling

Objective: Based on user activity patterns, predict the likelihood of criminal behavior. Methodology:

Train models on historical data containing known cases of online criminal behavior.

Algorithms: Logistic Regression, Decision Trees, Random Forest, or Gradient Boosting (e.g., XGBoost, LightGBM).

Use features such as frequency of posting, language utilized, or type of engagement.

4. Classification

Objective: Classify a piece of content into predefined categories, such as hate speech, online harassment, or neutral.

Methodology: Supervised learning classifiers, such as Naïve Bayes, SVM, or deep learning techniques (Convolutional Neural Network, Recurrent Neural Networks).

Tools: Tensor Flow, PyTorch, and Scikit-learn libraries for developing classifiers.

5. Social Network Analysis (SNA)

Objective: Explore user-user relationships and connections to identify possible criminal organizations or key influencers who perpetuate malicious activities.

Approach: Graph-based algorithms in modeling social media users as nodes and connections as edges Centrality measures: Degree, Betweenness, and Clustering Coefficients

Use: NetworkX (python) or Gephi for visualization

6. Association Rule Mining

Objective: Discover behavior patterns that are likely to occur together at the same time, including specific types of comments often appearing before online harassment occurrences.

Approach: Use Apriori or FP-Growth algorithms to extract rules like: "If a user posts X, they are likely to post Y within Z days."

Applications: Detecting early signs of escalating online behavior.

7. Clustering

Purpose: Group similar users or content for further analysis, such as identifying clusters of users engaging in harmful behavior.

Methodology: Use algorithms like K-Means, Hierarchical Clustering, or DBSCAN.

Example: Grouping users based on posting frequency, sentiment, or content topics.

8. Anomaly Detection

Purpose: Uncover unusual patterns that might signify illegal activities, such as abrupt surges in aggressive speech or odd posting behavior.

Methodology: Isolation Forests, One-Class SVM, or Auto encoders (deep learning). Tools: Scikit-learn, PyOD (Python Outlier Detection).

9. Web Scraping and Data Collection

Purpose: Collect large datasets from social media platforms for analysis. Methodology:

Use tools like Beautiful Soup, Selenium, or Scrapy to scrape data.

Make sure to comply with the ethical and legal guidelines that may be involved, for example, data anonymization and permissions.

10. Time Series Analysis

Purpose: Analyzing time-dependent patterns in the user activity, like certain events increase hate speech and harassment.

Methodology: Sequence prediction through algorithms such as ARIMA or Long Short-Term Memory (LSTM) networks.

Application: Patterns that change with time, for example, increased online threats during particular periods.

11. Feature Engineering

Purpose: Meaningful feature creation to improve the performance of the model. Methodology:

Extract features including:

Linguistic patterns- word choice and sentiment scores. Interaction metrics likes, shares, and retweets.

Network metrics (e.g., centrality, clustering).

Tools: Python libraries such as Pandas, NumPy, and Featuretools.

12.Ethical Considerations in Data Mining

Objective: Address privacy issues and minimize biases in the dataset or algorithms. Methodology:

Use differential privacy techniques.

Apply bias detection algorithms to ensure fairness in predictions. Tools: IBM AI Fairness 360, Google Tensor Flow Privacy.

V. OBJECTIVES OF STUDY

The main objectives of this research are:

- Exploring how such criminal behaviors as hate speech and online harassment emerge on social media.
- Detection, prediction, and prevention of criminality in cyberspace with the help of AI.
- Assessing whether the implementation of AI-based tools enhances the investigation of crime and strengthens cybersecurity for users, the minors and influencers alike.
- To develop a comprehensive model for digital criminal investigations, using AI technologies to improve the performance of law enforcement.

VI. SCOPE AND LIMITATIONS

The scope of this research considers criminal behavior through social media and the role of AI in improving digital criminal investigations. However, despite the possibility of AI greatly making the processes more efficient and accurate, the following limitations apply:

Ethical Issues: The concern over privacy is still to be conquered because the monitoring of a person's online activity with AI has difficulties balancing security and privacy.

Algorithmic Bias: AI models are prone to bias, depending on datasets used, leading to false positives or over-identification of individuals.

Availability of Data: This paper suffers from the restriction of proprietary data from social media. Access to this data can even improve deeper understanding of online criminal behavior.

VII. CONCLUSION

The research demonstrates that the importance of AI in the analysis of criminal behavior on the social network is growing. With the above view, this paper scrutinizes contemporary studies on hate speech, online harassment, and digital criminal investigations with a view of improving potential law enforcement against such crimes and protecting vulnerable people online through AI. AI-driven systems can identify patterns, predict criminal behavior, and improve cybersecurity for social media users. However, there are also limitations and ethical considerations, and therefore, this level of AI induction into criminal investigations takes one step further in how people can combat online crime and ultimately create a safer digital environment.

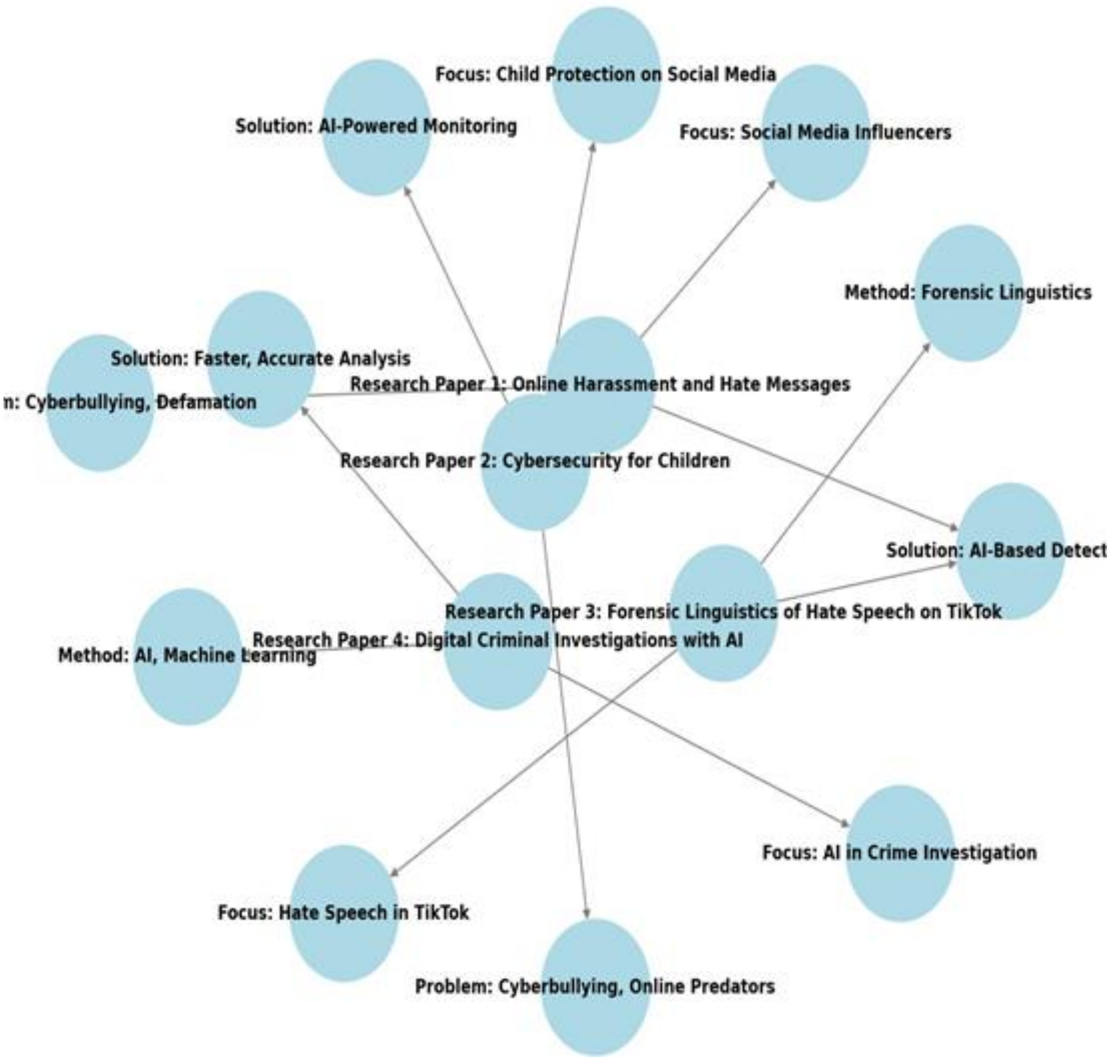
Focus: Child Protection on Social Media
Solution: AI-Powered Monitoring
Focus: Social Media Influencers
Method: Forensic Linguistics
Solution: Faster, Accurate Analysis
Research Paper 1: Online Harassment and Hate Messages
n: Cyberbullying, Defamation
Research Paper 2: Cybersecurity for Children
Solution: AI-Based Detect
Research Paper 3: Forensic Linguistics of Hate Speech on TikTok
Research Paper 4: Digital Criminal Investigations with AI
Method: AI, Machine Learning
Focus: AI in Crime Investigation
Focus: Hate Speech in TikTok
Problem: Cyberbullying, Online Predators

Fig.3: Graph Structure of Research Paper Summary

REFERENCES

1] Martens, M., & Neudert, L.-M. (2023). Too lucky to be a victim? An exploratory study of online harassment and hate messages faced by social media influencers. *European Journal on Criminal Policy and Research.* https://doi.org/10.1007/s10610-023-09542-0

2] Alabdulkareem, K. F., & Alsulami, H. (2023). Cybersecurity for children: An investigation into the application of social media. *Enterprise Information Systems, 17*(4), 679–696. https://doi.org/10.1080/17517575.2023.2188122

3] Nugroho, R. A., Rukmini, D., & Sutopo, D. (2023). Forensic linguistic analysis of netizens' hate speech acts in Tik-Tok comment section. *BIAR Journal: Bioinformatics and Applied Research*, *4*(2), 88–99. https://biarjournal.com/index.php/biolae/article/view/894

4] Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2023). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *arXiv*. https://arxiv.org/abs/2309.07064