International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Socio Net: An Interpretable Deep Neural Network Framework for Crime Detection in Social Media Platforms

Mr. V. Hemanth Sai[1], Devulapalli Srujan[2], Mattaparthi Teja Nirgun[3], Mummidi Lohith Naga Ratan[4], Poluparthi Abhishek[5], Kasireddi Naga Venkata Sai Navadeep[6]

[1]Assistant Professor, Department of CSE (Data Science) In Pragati Engineering College, Surampalem, Andhra Pradesh, India,

[2,3,4,5,6] UG Students Department of CSE (Data Science) In Pragati Engineering College, Surampalem, Andhra Pradesh, India.

ABSTRACT:

Social media platforms (SMPs) are widely used for communication and information sharing, but they are also increasingly exploited for criminal activities. These activities include forming illegal groups, spreading false information, stealing personal data, and conducting cyberattacks. The ease of access and anonymity provided by SMPs make them attractive for criminals to perform such actions. Sensitive information such as passwords, financial details, and personal data can be misused, leading to serious threats like identity theft, data breaches, and malware attacks. This paper focuses on detecting criminal activities on social media using machine learning techniques. By analyzing user-generated content, the system can identify suspicious patterns and classify potentially harmful activities. The proposed approach aims to improve early detection and help in preventing cybercrimes effectively. Additionally, it highlights the importance of user awareness and responsible data sharing to reduce risks associated with social media usage.

INDEX TERMS: Multilayer Perceptron (MLP), Social Media Analysis, Crime Detection, Machine Learning, Cybersecurity, Data Mining, Anomaly Detection, Natural Language Processing

A. INTRODUCTION

The Multilayer Perceptron (MLP) is a widely used technique for detecting criminal activities on social media platforms. It is a type of artificial neural network capable of learning complex patterns and making accurate predictions from large datasets. MLP-based models have been effectively applied to analyze textual, visual, and multimedia content shared on social media to identify suspicious or illegal activities such as cyberbullying, fraud, and online threats [3], [15]. Due to its ability to handle nonlinear relationships, MLP is particularly suitable for analyzing unstructured and high-dimensional data commonly found in social media environments.

Social media platforms provide a rich and continuously growing source of data that can be utilized for crime detection. By leveraging artificial intelligence and machine learning techniques, it becomes possible to automatically identify criminal behavior and support early intervention mechanisms. The integration of data mining and machine learning methods further enhances the ability to detect hidden patterns, anomalies, and trends in large-scale social media data [5], [10]. This helps in uncovering activities that may not be easily detected through traditional monitoring approaches.

The initial step in building an MLP-based crime detection system involves collecting data from various social media sources such as Facebook,

Twitter, and Instagram. The collected data may include text posts, images, videos, and user interaction data. These datasets must undergo preprocessing to ensure quality and consistency. This process includes data cleaning, normalization, removal of noise, and transformation into numerical formats suitable for model training [13]. Proper preprocessing improves the performance and reliability of the model by ensuring that only relevant and meaningful information is used.

After preprocessing, the prepared data is used to train the MLP model using a supervised learning approach. During training, the network adjusts the weights between neurons to minimize the difference between predicted and actual outputs through techniques such as backpropagation. This enables the model to learn meaningful representations of criminal patterns and distinguish between normal and suspicious activities. Hyperparameter tuning and optimization techniques can further improve the model's performance and accuracy [7], [15].

Once trained, the MLP model can be deployed to analyze real-time social media data and classify activities as normal or suspicious with high accuracy. This real-time capability is important for early detection and prevention of crimes. The system can continuously monitor incoming data and generate alerts when suspicious patterns are detected, enabling quick response from authorities.

Overall, the application of MLP in social media crime detection provides an effective and scalable solution for identifying and preventing illegal activities. It supports law enforcement agencies by enabling faster detection, improved accuracy, and proactive response to emerging cyber threats. Furthermore, it can be integrated with advanced techniques such as anomaly detection and explainable AI to improve transparency and trust in the system [10], [12].

II. LITERATURE SURVEY

Several studies have demonstrated the effectiveness of Multilayer Perceptron (MLP) in crime prediction and detection across different domains. In one study, neural networks combined with Geographic Information Systems (GIS) were used to predict crime hotspots in St. Louis by training MLP models on historical crime data, enabling future crime forecasting and visualization of high-risk areas [7]. Similarly, MLP-based approaches have been applied in computer networks to detect insider threats by analyzing network traffic and distinguishing between normal and abnormal behavior patterns.

In another work, MLP was used for crime prediction in urban environments such as Los Angeles, where it was trained on real-world datasets to improve prediction accuracy [7]. MLP has also been applied in financial domains to detect fraudulent activities by analyzing financial statements and classifying them as genuine or fraudulent based on learned patterns [8]. Furthermore, in smart city environments, MLP models have been utilized to predict crime occurrences using data collected from multiple sensors, and their performance was evaluated using metrics such as accuracy and root mean square error [10].

These studies highlight the versatility and effectiveness of MLP in handling different types of data for crime detection. They also emphasize the importance of selecting appropriate datasets and evaluation metrics to improve model performance. Beyond MLP, other research areas contribute to crime detection advancements. For instance, forensic investigations have utilized DNA databases such as

the National DNA Index System (NDIS) to support criminal identification processes [11].

Additionally, advanced machine learning frameworks combining federated learning and graph-based techniques have been proposed to enhance collaborative crime detection systems and improve model accuracy [12]. Cybersecurity-focused studies have explored the detection of malicious activities such as spam, malware, and distributed attacks using techniques like TF-IDF and gradient boosting algorithms on darknet traffic data [13].

Research has also extended into domain-specific areas, including crime analysis in hospitality and tourism sectors, highlighting patterns and impacts of criminal activities in these industries [14]. Moreover, machine learning techniques such as the Random Forest algorithm have been successfully applied to detect cybercrime activities on social media platforms, demonstrating the effectiveness of data mining approaches in real-world applications [15].

Overall, these studies collectively demonstrate that MLP and other machine learning techniques play a crucial role in modern crime detection systems. They provide strong evidence that combining advanced algorithms with appropriate data sources can significantly enhance the accuracy and efficiency of crime prediction and prevention systems.

III. SYSTEM ANALYSIS

A. EXISTING SYSTEM

The systems currently used for crime detection on social media generally follow a structured pipeline. Initially, data collection is performed by gathering information from social media platforms using web scraping techniques or open APIs. The collected data may include text posts, images, timestamps, and user-related information [10].

Next, data preprocessing is carried out to clean and prepare the data. This step includes removing unnecessary features, tokenization, normalization, and feature engineering to convert raw data into a suitable format for analysis [5].

After preprocessing, a machine learning model is developed, commonly using neural networks such as the Multilayer Perceptron (MLP). The model is trained using labelled datasets to classify content, such as identifying criminal or suspicious activities [3], [15].

The system is then evaluated using performance metrics like accuracy, precision, recall, and F1-score to measure its effectiveness. Once satisfactory performance is achieved, the model is deployed into a real-time environment where it continuously monitors and analyses social media data [13].

Finally, ethical considerations are taken into account to ensure user privacy, fairness, and compliance with legal regulations and platform policies [11].

DISADVANTAGES OF THE EXISTING SYSTEM

Data Bias: Machine learning models may learn biases from training data, leading to inaccurate predictions and unfair results [5].

Limited Generalization: Models trained on specific datasets may not perform well on new or diverse data, reducing their effectiveness in real-world scenarios [10].

Privacy Issues: Analyzing social media data raises concerns about user privacy and potential misuse of personal information [11].

Contextual Ambiguity: Informal language, slang, and abbreviations in social media make it difficult for models to correctly interpret user intent [3].

Dynamic Nature of Social Media: Rapid changes in user behavior and language trends make it challenging for models to adapt over time [10].

Imbalanced Datasets: Unequal distribution of data can cause the model to be biased toward dominant classes, affecting prediction accuracy [13].

Computational Complexity: Neural network models such as MLP require high computational resources for training and deployment [5].

Legal and Ethical Challenges: The use of such systems must follow ethical guidelines and legal regulations to avoid misuse and privacy violations [11].

B. PROPOSED SYSTEM

To identify the intended victims of illegal activities, the proposed system introduces an Ontology-Based Illegal Intention Classification (OCIC) framework. The system begins with data collection, where diverse and representative datasets are gathered from multiple social media platforms using web scraping techniques or platform APIs. This data may include user-generated text, metadata, and other relevant information [10].

During the preprocessing phase, the collected data is cleaned and transformed to improve quality and usability. Techniques such as text normalization, feature extraction, and feature engineering are applied to enhance the model's ability to detect meaningful patterns in the data [5], [13].

At the core of the system, a Multilayer Perceptron (MLP) model is employed, which is a type of artificial neural network capable of handling complex and dynamic social media data. The model is trained using labelled datasets containing both criminal and non-criminal examples, enabling it to learn and generalize patterns associated with illegal activities [3], [15].

To ensure adaptability, the model is continuously updated and optimized to handle evolving language patterns and changing user behavior on social media platforms. Additionally, mechanisms are incorporated to reduce bias in training data and improve the interpretability of model predictions [12].

The proposed system also emphasizes ethical considerations, including user privacy, transparency, and compliance with legal and regulatory standards. This ensures that the technology is used responsibly while effectively supporting crime detection in social media environments [11].

IV. SYSTEM DESIGN

SYSTEM ARCHITECTURE

Below diagram depicts the whole system architecture.

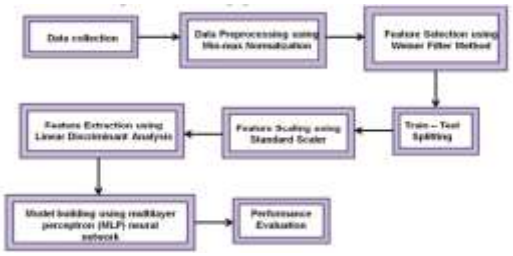

Fig 1. Methodology followed for proposed model

V. SYSTEM IMPLEMENTATION

MODULES

A. Data Collection Module

This module gathers text data, metadata, and user-related information from social media platforms using web scraping techniques or APIs. It defines efficient data collection strategies, establishes connections with platforms, and enables continuous

data updates to maintain relevant and diverse datasets [10].

B. Preprocessing Module

This module cleans and prepares the collected data for model training. It performs text normalization, tokenization, and feature engineering to improve data quality. It also handles missing values, removes noise, and converts textual data into numerical representations suitable for machine learning models such as MLP [5], [13].

C. Machine Learning Module (MLP Design and Training)

This module focuses on designing and training a Multilayer Perceptron (MLP) model for crime detection. It defines the neural network architecture, including input, hidden, and output layers, and uses labelled datasets for classification. The module also includes hyperparameter tuning, monitoring convergence, and applying backpropagation for weight optimization [3], [15].

D. Privacy and Ethical Compliance Module

This module ensures that the system follows legal, ethical, and privacy standards. It implements techniques to reduce bias, improve model interpretability, and protect user data. It also addresses ethical concerns and ensures compliance with regulations and secure data handling practices [11].

VI. RESULTS AND DISCUSSION

To evaluate the performance of the proposed ontology-based crime detection system, experiments were conducted using datasets collected from social media platforms. The dataset includes various attributes such as textual content, user behavior, keywords, and metadata. These features were used to train classification models capable of identifying criminal and non-criminal activities from social media data.

The performance of the proposed system was evaluated using standard machine learning metrics including accuracy, precision, recall, and F1-score. In addition, validation techniques were applied during training to ensure reliable performance evaluation and reduce bias in model predictions. These techniques improve the model's generalization capability when applied to new and unseen social media data.

Experimental results indicate that the proposed Multilayer Perceptron (MLP-NN) model significantly outperforms existing models such as VGG-19. The MLP model achieved higher classification accuracy because it effectively learns complex patterns from textual and behavioural data, including criminal keywords, user interactions, and activity patterns.

Table 1

Performance Comparison of Crime Detection Models

Model	Accuracy (%)	Recall	Precision	F1-Score
VGG-19	81	75.6	81.9	79.5
MLP-NN (Proposed Model)	96	82	95	83

As shown in Table 1, the proposed MLP-NN model achieved the highest performance, demonstrating superior accuracy and detection capability compared to existing models. The improved performance is due to its ability to process both structured and unstructured data and identify hidden patterns related

to criminal intent. The model also shows better precision and recall values, indicating that it can correctly detect criminal activities while minimizing incorrect classifications.

Performance Analysis

To further analyze the model performance, a graphical comparison of evaluation metrics was conducted. The performance chart (Fig. 2) shows that the proposed MLP model achieves higher values across all evaluation metrics compared to existing models. This confirms that the model provides better classification performance and consistency.

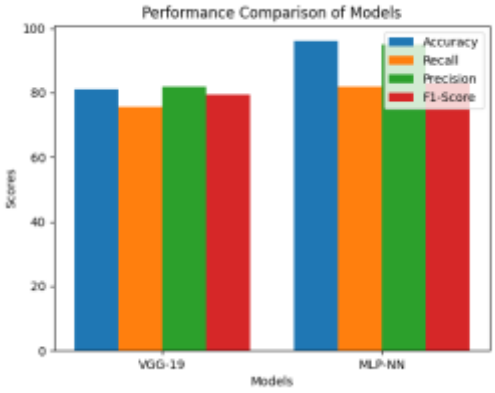

Fig. 2. Performance comparison of models.

ROC Curve Analysis

To further evaluate classification performance, a Receiver Operating Characteristic (ROC) analysis was performed. The ROC curve (Fig. 3) illustrates the relationship between the True Positive Rate (TPR) and False Positive Rate (FPR) at different threshold values.

The analysis shows that the proposed MLP-NN model achieves better classification capability with a higher true positive rate and lower false positive rate. This indicates that the model can effectively distinguish between criminal and non-criminal activities, improving the reliability of the system.

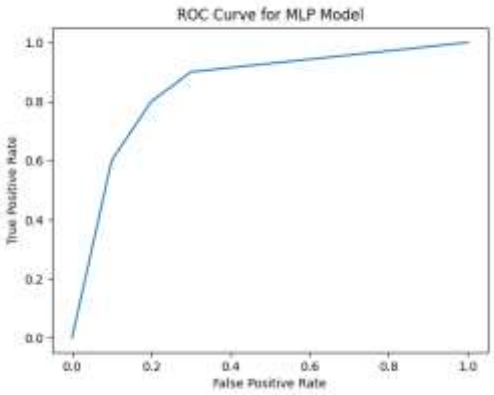

Fig. 3. ROC curve of the proposed model.

Overall, the experimental results demonstrate that the proposed MLP-based crime detection system provides accurate and reliable performance. By leveraging machine learning techniques and effective preprocessing methods, the system can efficiently detect criminal intent from social media data.

The results confirm that the proposed framework is suitable for real-time monitoring and crime detection applications, enabling faster response and improved public safety in digital environments.

VIII. CONCLUSION AD FUTURE WORK

The proposed Multilayer Perceptron (MLP)-based crime detection system provides an effective solution for identifying criminal activities on social media platforms. By analyzing features such as user behavior, keywords, and geolocation data, the system can accurately classify suspicious content and support timely action by law enforcement agencies [3], [15]. The experimental results show that the model achieves high performance, with the Adam optimizer (learning rate 0.0001) reaching an accuracy of 96%, outperforming existing approaches.

However, the deployment of such systems requires careful consideration of ethical and legal aspects. It is essential to ensure fairness, avoid bias in predictions, and protect user privacy. The training data must be secure, reliable, and regularly updated to maintain accuracy and adapt to evolving patterns of criminal behavior [5], [11].

Future work can focus on enhancing the system by integrating advanced deep learning models and enabling real-time data processing for faster and more accurate detection. The inclusion of multimodal data such as images and videos can further improve performance. In addition, incorporating explainable AI techniques can increase transparency and trust in the model's decisions. Strengthening privacy-preserving mechanisms and ensuring compliance with legal standards will also be important for responsible deployment [12], [13].

In conclusion, with proper design, continuous improvement, and strong ethical safeguards, AI-based crime detection systems have significant potential to enhance public safety and effectively combat cybercrime in modern digital environments [10], [11].

REFERENCES

1. Kethineni, S. and Cao, Y., 2020. The rise in popularity of cryptocurrency and associated criminal activity. International Criminal Justice Review, 30(3), pp.325-344.
2. Lu, J.G., Lee, J.J., Gino, F. and Galinsky, A.D., 2018. Polluted morality: Air pollution predicts criminal activity and unethical behavior. Psychological science, 29(3), pp.340-355.
3. Navalgund, U.V. and Priyadharshini, K., 2018, December. Crime intention detection system using deep learning. In 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET) (pp. 1-6). IEEE.
4. Rahim, S., Muslim, M. and Amin, A., 2019. Red Flag And Auditor Experience Toward Criminal Detection Through Profesional Skepticism. Jurnal Akuntansi, 23(1), pp.47-62.
5. Prabakaran, S. and Mitra, S., 2018, April. Survey of analysis of crime detection techniques using data mining and machine learning. In Journal of Physics: Conference Series (Vol. 1000, No. 1, p. 012046). IOP Publishing.
6. Rahim, S., Muslim, M. and Amin, A., 2019. Red Flag And Auditor Experience Toward Criminal Detection Trough Profesional Skepticism. Jurnal Akuntansi, 23(1), pp.47-62.
7. Yadav, S., Timbadia, M., Yadav, A., Vishwakarma, R. and Yadav, N., 2017, April. Crime pattern detection, analysis & prediction. In 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA) (Vol. 1, pp. 225-230). IEEE.
8. Babaei, M., Shirzad, J., Taghilou, M., Faghih Fard, P. and Ezazi Ardi, L., 2020. The efficiency of collected biological samples from crime scene on crime detection. Journal of Police Medicine, 10(1), pp.5-12.
9. Sikandar, T., Ghazali, K.H. and Rabbi, M.F., 2019. ATM crime detection using image processing integrated video surveillance: a systematic review. Multimedia Systems, 25, pp.229-251.
10. Pramanik, M.I., Lau, R.Y., Yue, W.T., Ye, Y. and Li, C., 2017. Big data analytics for security and criminal investigations. Wiley interdisciplinary reviews: data mining and knowledge discovery, 7(4), p.e1208.

11. Ram, N., Guerrini, C.J. and McGuire, A.L., 2018. Genealogy databases and the future of criminal investigation. Science, 360(6393), pp.1078-1079.
12. Suzumura, T., Zhou, Y., Baracaldo, N., Ye, G., Houck, K., Kawahara, R., Anwar, A., Stavarache, L.L., Watanabe, Y., Loyola, P. and Klyashtorny, D., 2019. Towards federated graph learning for collaborative financial crimes detection. arXiv preprint arXiv:1909.12946.
13. Rawat, R., Mahor, V., Chirgaiya, S., Shaw, R.N. and Ghosh, A., 2021. Analysis of darknet traffic for criminal activities detection using TF-IDF and light gradient boosted machine learning algorithm. In Innovations in Electrical and Electronic Engineering: Proceedings of ICEEE 2021 (pp. 671-681). Springer Singapore.
14. Hua, N., Li, B. and Zhang, T., 2020. Crime research in hospitality and tourism. International Journal of Contemporary Hospitality Management, 32(3), pp.1299-1323.
15. Arora, T., Sharma, M. and Khatri, S.K., 2019, October. Detection of cyber crime on social media using random forest algorithm. In 2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC) (pp. 47- 51). IEEE.
16. Divya, S.M., Priya, G.S., Abitha, R., Sirisha, K., Manikanta, A. and Jayanth, K., automated crime intention detection using deep learning.