International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Crime Detection in Social Media Platforms Using Multi-Layer Perceptron

Mr. M. V.Ramana[1], V.Sai Kiran[2], H.V.V.S.Amarnath M[3], S.S.S.V.L.Narayana[4], N.V.S.D.Karthikeya[5], S.Durga Devi[6], Y.Dhana Sri[7]

[1]M.Tech(Ph.D), Associate Professor, Cse Department, Vsm College Of Engineering, Ramachandrapuram, Egdist, Andhrapradesh-533255.
[2]Students, Cse Department, Vsm College Of Engineering, Ramachandrapuram, Egdist, Andhrapradesh-533255.

ABSTRACT:
Social media platforms, or SMPs, have become more and more used by criminals to accomplish various illicit objectives. The formation of illicit online communities, the dissemination of user data, and data breaches are a few examples of these objectives. SMPs are frequently used by these criminal organizations to exchange private information and plan illegal actions. SMPs are an effective tool for criminals because of their accessibility and anonymity. One of the biggest worries about SMPs is data breaches. SMPs provide thieves access to financial and personal data, such as passwords and credit card numbers. SMPs can also be used by them to disseminate malware and malicious software, which can infect mobile devices and computers. An additional concern for SMPs is the sharing of user information. SMPs are a tool that criminals can use to gather personal information about people, information that they can then use for malicious purposes like identity theft. Additionally, criminals can harm a person's or an organization's reputation by disseminating false information about them using SMPs. SMPs are a potent weapon that criminals may use. Users should also exercise caution when disclosing personal information and keep an eye out for any questionable activity on SMPs.

INTRODUCTION :

1.1 ABOUT PROJECT:

In the never-ending fight against financial fraud, which causes significant financial losses and harms the reputations of banking institutions and their clients, Fraud Detection in Banking Data Using Machine Learning is a crucial frontier. Although they can be somewhat successful, traditional rule-based systems are becoming less and less capable of identifying sophisticated fraud techniques that change quickly over time. As a result, it is imperative to use increasingly sophisticated and flexible strategies that make use of artificial intelligence and machine learning. With the goal of addressing important issues like data quality, imbalanced datasets, overfitting and underfitting, scalability, and false positives and negatives, this paper presents a novel machine learning-based approach to fraud detection. The suggested system looks for correlations between particular characteristics and fraudulent activity by evaluating intelligent algorithms that were trained on public datasets. This allows for the development of more precise and effective detection techniques.

The system ensures that machine learning models can effectively learn from both fraudulent and

legitimate transactions by mitigating the impact of class imbalance in banking datasets through the use of resampling techniques and rigorous model evaluation processes. Furthermore, the system can adjust and change in response to shifting fraud patterns by integrating feedback loops and continuous monitoring mechanisms, maintaining high levels of accuracy and dependability over time.

In the end, implementing a machine learning-based fraud detection system in banking data is a proactive, data-driven strategy to combat financial fraud. It helps banks better identify and mitigate fraudulent activity, protect the interests of their clients, and maintain their own integrity and reputation in the financial sector.

1.2 EXISTING SYSTEM:

Currently in use, the multilayer Perceptron system for crime detection in social media plot forms employs Random Forest, an ensemble learning technique that combines several decision trees to generate predictions. Every tree in the forest gains knowledge of various aspects of the data on its own, and the combined outputs of all the trees arrive at a final prediction. Random Forest can be applied to regression tasks (predicting the number of incidents) as well as classification tasks (predicting crime categories, identifying high-risk areas, etc.). Random Forest models are appropriate for real-time crime prediction applications because, once trained, they can produce predictions rapidly.

Based on the degree to which input features enhance the purity of the tree nodes, they can automatically rank the features' significance. Restricted in managing intricate, non-linear connections within data, Couldn't precisely adjust to changing patterns of crime. Utilize fundamental statistical analysis to forecast crimes.

Disadvantages:

- **Overfitting:** Random forests can overfit noisy datasets with a large number of trees, despite their design to minimize overfitting in comparison to individual decision trees.
- **Model Training Time:** Because multiple decision trees must be grown and their results aggregated, training a random forest model can be more time-consuming than training simpler algorithms.
- **Problems with Data Quality:** Both the quantity and quality of data are crucial to ML algorithms. Inaccurate, biased, or incomplete crime data can have an impact on the algorithm's dependability and performance.
- **Unbalanced Datasets:** When dealing with extremely unbalanced crime datasets—where some crime types are noticeably more frequent than others—random forests might not function as well as they should.
- **Data Availability:** Current and pertinent data are necessary for ML algorithms to function. The algorithm's performance might be affected in places where there is a lack of data or where some crimes are not reported to the authorities.

1.3 PROPOSED SYSTEM:

The suggested framework MLP features an intuitive and user-friendly interface. An input layer, one or more hidden layers, and an output layer make up the layers of an MLP.

A directed cyclic graph is formed by connecting all of the neurons in one layer to all of the neurons in the layer below. Each neuronal connection between neighboring layers has a weight attached to it.

Using methods like gradient descent and backpropagation, these weights are modified during training to maximize the network's performance.

Using past data, TMLPs can be trained to forecast the likelihood of crimes. MLPs can be used to identify trends in cybercrime, including fraud, identity theft, and hacking attempts, by examining past crime patterns. This aids in targeting organized crime groups and policing with an intelligence-led approach. In the proposed system, data collection would be concentrated on obtaining diverse and representative

datasets from various social media platforms. MLPs can detect unusual patterns in crime data that detect from normal behavior. A Multi-Layer Perceptron (MLP), a kind of artificial neural network, would be at the center of the system. MLPs are made to analyze the complex and dynamic nature of social media content. Using labeled datasets that include examples of both criminal and non-criminal behavior, the MLP would be trained.

Advantages:

- **Capacity to Handle Multi-class Issues:** Multi-class classification tasks, like forecasting distinct crime kinds depending on different characteristics or attributes, can be handled by MLPs.
- **Feature Learning:** MLP automatically extracts relevant features from the input data during the training phase. When the network becomes adept at extracting pertinent features from unprocessed data, it often eliminates the need for human feature engineering.
- **Real-time Analysis:** Because MLP algorithms are fast at processing large amounts of data, they are appropriate for real-time crime analysis.
- **Continuous Learning:** MLPs can be adapted for continuous learning, allowing models to be updated with new crime data over time, improving their accuracy and relevance.
- **TheParallel Processing:** MLP training and inference can be effectively parallelized, particularly with contemporary computing architectures such as GPUs.

LITERATURE REVIEW:

The surge in interest in cryptocurrencies and the related illegal activity.

For many drug dealers and extortionists, cryptocurrency like bitcoin, Ethereum, and, more recently, Monero, has become the preferred form of payment. The illicit activities range from ransom kidnapping to tax evasion, money laundering, Ponzi schemes, and cryptocurrency theft. As cryptocurrency demand rises, criminals have more opportunity to hide behind the anonymity and presumed privacy of cryptocurrencies. Law enforcement has faced difficulties in identifying these cryptocurrency-related crimes because of the cross-border nature of transactions, the use of evasion technology to conceal users' identities, and the inconsistent regulations.

Air pollution predicts criminal activity and unethical behavior.

Globally, air pollution is a severe issue that impacts billions of people. The current study examines the ethical costs of air pollution, despite the fact that its effects on the environment and human health are widely recognized. We suggest that anxiety caused by air pollution may contribute to an increase in criminal and unethical behavior. The present study examines the ethical costs of air pollution, which are well known despite being associated with negative health and environmental effects. A nine-year panel of 9,360 U.S. cities revealed that air pollution predicted six major categories of crime.

Deep learning-based system for detecting criminal intentions. The 2018 International Conference on Digital Enterprise Technology's Circuits and Systems

Circuit television cameras, or CCTVs, are commonly used to reduce the number of crimes that occur nearby. Despite the fact that CCTV is installed in a variety of public and private spaces to monitor the environment, crime prevention has not improved. This is due to the fact that CCTV needs human supervision, which increases the risk of human error. For example, a human may overlook some significant criminal events when watching multiple screens that are simultaneously being recorded by CCTVs. In order to solve this problem, we developed the Crime Intension Detection System, which recognizes criminal activity in real-time photos and videos and notifies the human supervisor to take the

appropriate action. to report any crimes committed to the local police station or supervisors.

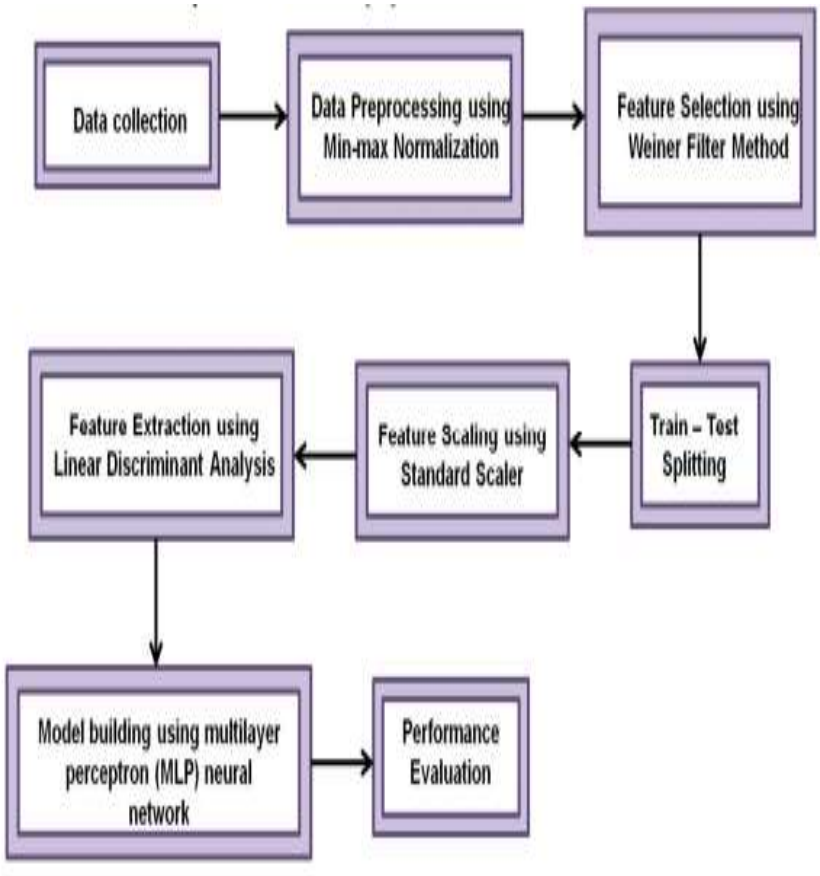
Red Flag and Auditor Experience with Professional Skepticism in Criminal Detection.

The purpose of this study was to investigate how professional auditor skepticism, work experience, and red flag variables affect fraud detection. The purpose of the test is to determine how professional auditor skepticism is influenced by red flag variables and work experience. Additionally, the red flag variables test and the auditor's work experience with professional auditor skepticism are used to detect fraud. Using the census method, 40 samples were drawn from eight Makassar City public accounting offices. Questionnaires are used in data collection research to obtain data. The Partial Least Square (PLS) Method is the data analysis technique that is applied.

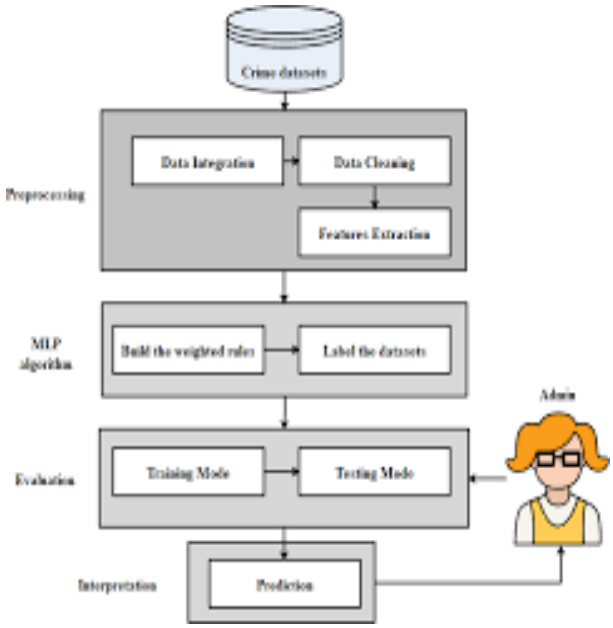
SYSTEM ARCHITECTURE:

System The system architecture for a fraud detection system in banking is crucial for ensuring scalability,reliability,security,and performance.

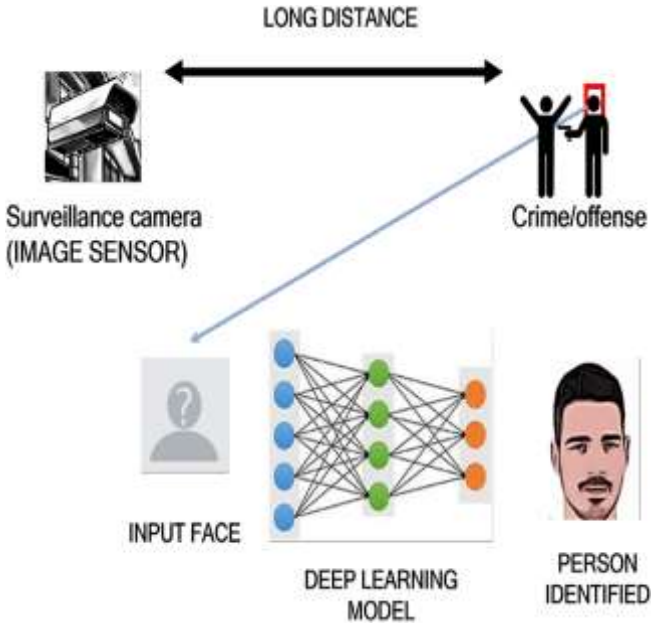
1. Data Ingestion Layer
2. Data Processing Layer
3. Machine Learning Model Layer
4. Real-time Transaction Verification Layer
5. Model Evaluation and Monitoring Layer
6. Security and Compliance Layer
7. Integration Layer
8. Monitoring and Alerting Layer



FOR USER:



FOR ADMIN:



CONCLUSION:

The recommended MLP (Multilayer Perceptron) model for the Crime Detection System is an effective tool for law enforcement organizations to identify criminal activity early on. It can be trained to identify posts or messages as possibly connected to criminal activity using a variety of features, including user behavior, keywords, and geolocation data. Law enforcement can act appropriately and promptly thanks to this approach. But it's crucial to understand the moral and legal ramifications of utilizing an MLP model to identify and categorize possibly illegal behavior. It is crucial to guarantee that the model is not being unfairly used to target particular groups or individuals, and that the data used to train the model is safe and secure.

Ultimately, a thorough analysis of the model's output is necessary to guarantee that any decisions made

by law enforcement are legitimate and compliant with the law. After experimenting with different learning rates, Optimizers, and a learning rate of 0.0001, Adam Optimizer produced 96% accurate results. The proposed system yields superior results when compared to other existing criminal detection techniques. In conclusion, employing an MLP model for social media platform crime detection has the potential to improve public safety. As with any technology, it's crucial to make sure the system is created and operated in an ethical and responsible manner. This entails considering data security and privacy in addition to making sure the AI model is continuously checked and updated with the most recent data. It's crucial to think through the possible effects of utilizing such a system and take the necessary precautions to reduce any risks. Artificial intelligence (AI)-based crime detection on social media platforms has the potential to be a potent weapon in the fight against crime, given the appropriate methodology and security measures.

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. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. Ram, N., Guerrini, C.J. and McGuire, A.L., 2018. Genealogy databases and the future of criminal investigation. Science, 360(6393), pp.1078-1079.