**Abstract**

The rapid expansion of social networking platforms has significantly transformed communication and digital interaction but has also created a ground for fraudulent activities such as fake account creation, phishing, spamming, and misinformation spread. Traditional rule-based systems and classical machine learning (ML) models, although widely adopted, often struggle with real-time adaptability, interpretability, and handling complex relational data inherent in social networks. While prior research has explored both ML and deep learning (DL) methods, gaps remain in scalability, contextual understanding, and cross-platform effectiveness.

To bridge these gaps, this study proposes a hybrid fraud detection framework that integrates diverse ML algorithms—Random Forest, XGBoost, and Support Vector Machine—with DL models such as Convolutional Neural Networks (CNN), Long Short-Term Memory networks (LSTM), and Graph Neural Networks (GNN). The system processes multi-modal data including user behavior, account attributes, and network interactions. The ensemble learning technique is employed to combine the outputs of individual models, enhancing prediction robustness and reducing false positives.

Experiments were conducted on three datasets: an Instagram profile dataset, the Youtube01-Psy comment dataset, and video metadata collected via the YouTube Data API. The ensemble model achieved the highest accuracy across all datasets, with perfect scores on the Youtube01-Psy dataset. CNN and Random Forest also showed strong individual performance. These results confirm the effectiveness of the hybrid approach in accurately detecting fraud across different types of social media data. The proposed system highlights the importance of model diversity and structural awareness in combating evolving fraud threats in online social networks.