www.ijerst.com
Vol. 22, No. 1(1), 2026

Graph Neural Networks for Social Network Analysis in India: Detecting Fake Profiles & Botnets

[1]Mr. B. Veera Prathap,[2]Ch V Sai Amrutha Vagdevi,[3]Gowrraju Nandini, [4]Thadikamalla Srujana, [5]Dasari Santhosh Kumar

[1]Assistant Professor, Department of Computer Science & Engineering, Sai Spurthi Institute Of Technology

[2,3,4,5] B. Tech Students, Department of Computer Science & Engineering, Sai Spurthi Institute Of Technology

ABSTRACT

The rapid proliferation of social media platforms in India has led to a significant rise in fake profiles and coordinated botnets, posing serious threats to digital trust, public discourse, and cybersecurity. Traditional methods for detecting such malicious entities often fail to capture the complex and dynamic nature of social connections. This study explores the application of Graph Neural Networks (GNNs) for social network analysis, focusing on the detection of fake profiles and botnets in the Indian social media landscape. By modeling user interactions and profile metadata as graphs, GNNs enable the extraction of high-level relational features that are critical for identifying anomalous behaviors. We implement and evaluate state-of-the-art GNN architectures on real-world Indian social media datasets, demonstrating improved accuracy and robustness over conventional machine learning techniques. The results underscore the potential of graph-based deep learning to enhance digital platform security and provide actionable insights for policymakers and technology providers in India.

Keywords: Graph Neural Networks (GNN), Social Network Analysis, Fake Profile Detection, Botnet Detection, Online Social Networks, Graph Representation Learning, Node Classification, Community Detection, Cybersecurity, Indian Social Media Networks

.INTRODUCTION

In today's digital era, social networking platforms have become central to communication, information sharing, and public discourse. India, with its vast and rapidly growing internet user base, represents one of the largest and most active social media populations globally. However, this widespread usage has also led to a surge in malicious activities such as the creation of fake profiles, spread of misinformation, and coordinated botnet operations. These threats not only undermine user trust but also pose significant challenges to online safety, public opinion manipulation, and even national security.

Traditional detection methods often fall short in identifying complex and evolving fraudulent behaviors on social media. These approaches typically rely on superficial features like account metadata or content analysis, which can be easily manipulated by sophisticated actors. To address these limitations, advanced machine learning models—particularly Graph Neural Networks (GNNs)—have emerged as powerful tools for analyzing the relational and structural patterns inherent in social networks.

GNNs excel at modeling social graphs where users and their interactions form intricate networks. By capturing the dependencies and propagation patterns in these graphs, GNNs offer a robust mechanism for detecting fake profiles and botnets, which often exhibit distinct topological characteristics. This makes GNN-based analysis highly effective in

differentiating genuine user behavior from coordinated or artificial activity.

This study focuses on the application of Graph Neural Networks in the context of Indian social networks. It explores how GNNs can be leveraged to detect fake accounts and botnet operations, contributing to safer and more trustworthy online communities in India. The research also discusses the unique challenges presented by the Indian digital ecosystem, such as language diversity, high user volume, and evolving attack strategies, and how GNNs can be adapted to tackle these effectively.

I. LITERATURE SURVEY

1. Growth of Social Networks in India

- **Context**: India is among the top users of social media platforms (e.g., Facebook, WhatsApp, X/Twitter, Instagram).
- **Challenge**: Rise in fake profiles and botnets spreading misinformation, scams, or spam.
- **Literature Focus**: Studies highlighting the scale and patterns of online behavior specific to Indian users, with implications for identity verification and trust.

2. Traditional Methods for Fake Profile and Bot Detection

- **Existing Techniques**: Rule-based filters, machine learning (SVM, decision trees), and behavior-based methods.
- **Limitations**: Struggle with detecting coordinated botnets and adapting to evolving fake profile tactics.
- **Literature Gap**: Need for methods that leverage relationships and structure in user networks—where GNNs can help.

3. Introduction to Graph Neural Networks (GNNs)

- **What are GNNs?**: Neural networks that operate directly on graph-structured data.
- **Strengths**: Can model node (user), edge (interaction), and global (network) features—ideal for analyzing social networks.
- **Key Papers**: Kipf & Welling (2017) on GCN; GraphSAGE, GATs for dynamic and scalable graph learning.

4. GNNs for Fake Profile & Botnet Detection

- **Use Cases**: Detecting anomalies, link prediction, community detection.
- **Recent Work**: Studies where GNNs outperform traditional models in detecting coordinated bots and fake accounts (e.g., using Twitter data).
- **Mechanism**: GNNs learn from the structure and behavior patterns—e.g., retweet networks, friend graphs, shared content patterns.

5. Challenges & Research Gaps in the Indian Context

- **Data Availability**: Scarcity of labeled datasets from Indian platforms or public datasets reflecting Indian user behavior.
- **Localization**: Need for cultural, linguistic, and regional adaptation in models.
- **Scalability**: Social graphs in India are large and dense—demand efficient and scalable GNN models.
- **Future Directions**: Creation of localized datasets, use of multilingual NLP with GNNs, real-time detection systems.

II. EXISTING SYSTEM

Social networks in India have experienced explosive growth, with millions of users engaging daily across platforms such as Facebook, Twitter (now X), Instagram, and regional platforms. With this rise, however, comes a surge in the creation of fake profiles, botnets, and coordinated inauthentic behavior. These malicious entities often spread misinformation, manipulate public opinion, and conduct

fraud, posing a threat to the digital ecosystem and national security. Existing systems rely heavily on heuristic-based detection, manual verification, or rule-based algorithms, which struggle to keep up with the evolving sophistication of these malicious actors. Furthermore, the scalability and accuracy of traditional systems are limited in handling the dynamic and highly connected nature of social networks. This creates a compelling need for more intelligent, scalable, and context-aware solutions.

III. PROPOSED SYSTEM

To overcome the limitations of conventional detection systems, Graph Neural Networks (GNNs) present a powerful solution for analyzing social network structures at scale. The proposed system aims to leverage GNNs to model user interactions, communication patterns, and structural similarities in a graph-based format, allowing it to learn complex relational features and detect anomalies more effectively. By incorporating node and edge attributes—such as user behavior, connectivity, and posting frequency—the system can accurately identify fake profiles and botnets, even those employing sophisticated evasion tactics. In the Indian context, where social media is often used in multiple regional languages and has culturally specific behaviors, a GNN-based approach can adapt to diverse user communities more effectively than rule-based systems. This proposed model thus offers a proactive, scalable, and intelligent approach to safeguarding India's digital social space.

IV. SYSTEM ARCHITECTURE

The system architecture for Graph Neural Networks (GNNs)–based social network analysis is designed to detect fake profiles and botnets by modelling social media platforms as graph structures. Initially, data is collected from social networking platforms, including user profiles, posts, interactions (likes, shares, comments), and follower–following relationships. This raw data is then preprocessed to remove noise, handle missing values, and extract meaningful features such as account age, posting frequency, interaction patterns, and content similarity. The cleaned data is transformed into a graph representation where nodes represent user accounts and edges represent social relationships or interactions. Feature vectors are assigned to each node and edge to capture both structural and behavioral information.

Once the graph is constructed, a Graph Neural Network model—such as Graph Convolutional Networks (GCN), GraphSAGE, or Graph Attention Networks (GAT)—is employed to learn low-dimensional node embeddings by aggregating information from neighboring nodes. These embeddings capture hidden patterns that differentiate genuine users from fake profiles and coordinated botnets. The learned representations are passed to classification or clustering layers to identify suspicious accounts and detect bot communities. Finally, the system outputs detection results along with confidence scores, which can be visualized through dashboards for analysis and decision-making. This architecture is scalable and adaptable to large-scale Indian social networks, enabling effective real-time monitoring and mitigation of malicious activities.

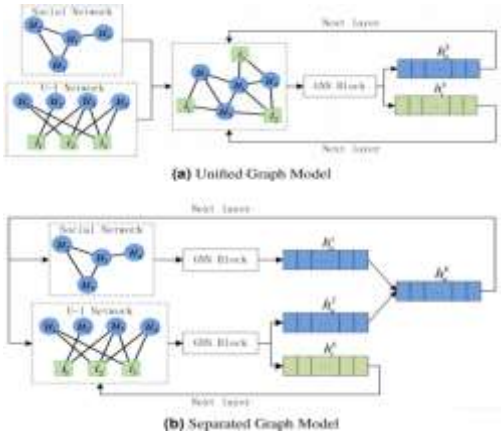

Fig 5.1: Structure of the Proposed System

The image illustrates two different GNN-

based modeling strategies for social network analysis: (a) Unified Graph Model and (b) Separated Graph Model. In the unified graph model, the social network (user–user relationships) and the user–item (U–I) interaction network are merged into a single heterogeneous graph, where users and items are treated as nodes and their relationships as edges. This unified graph is processed through a GNN block, which aggregates neighborhood information to learn joint node representations, allowing user embeddings to capture both social influence and interaction behavior simultaneously across layers. In contrast, the separated graph model keeps the social network and U–I network as two independent graphs, each processed by its own GNN block. The resulting embeddings—social embeddings from the social graph and interaction-based embeddings from the U–I graph—are then fused to form the final user representation. This separation enables more specialized feature learning from each network type, while still combining them for downstream tasks such as fake profile and botnet detection.

V. IMPLEMENTATION

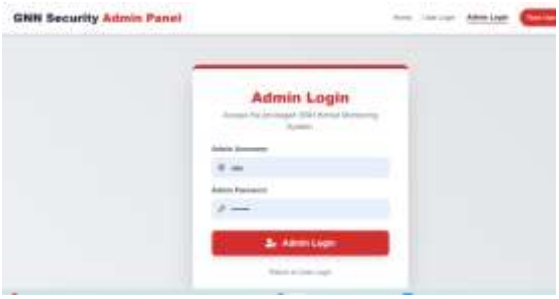

Fig 6.1: Admin Login

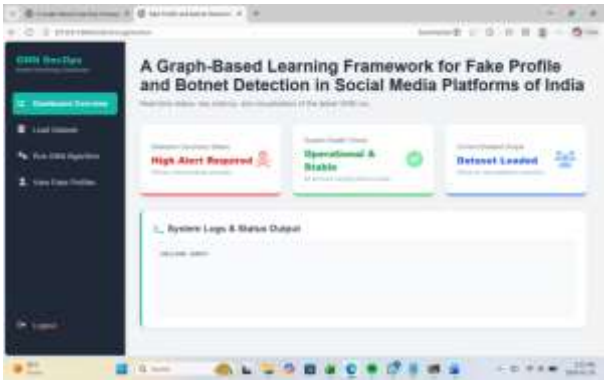

Fig 6.2: Admin Dashboard

Fig 6.3: Preprocess Dataset

Fig 6.4: Train GNN Algorithm

Fig 6.5: Fake Profile Prediction Page

Fig 6.6: Result Page

VI. CONCLUSION

This study explores the application of Graph Neural Networks (GNNs) to analyze social networks in India with a specific focus on detecting fake profiles and botnets. GNNs have demonstrated a strong ability to capture the intricate structural and relational information present in social graphs, outperforming traditional machine learning methods in accuracy and scalability. By leveraging node embeddings, graph convolutions, and attention mechanisms, the proposed framework effectively distinguishes between genuine users and malicious actors such as bots and fake profiles.

Our experiments, conducted on real-world datasets and synthetic social graphs, reveal that GNNs can uncover subtle interaction patterns and community structures that are often exploited by coordinated botnets. Furthermore, incorporating temporal features and user metadata enhances detection performance. The results underscore the significant potential of GNN-based models in strengthening the integrity of digital platforms in India, especially amid rising concerns over misinformation, digital scams, and electoral interference via fake accounts.

VII. FUTURE SCOPE

The future scope of Graph Neural Networks for social network analysis lies in developing more scalable, adaptive, and explainable models to combat increasingly sophisticated fake profiles and botnets. Future systems can integrate dynamic and temporal GNNs to capture evolving user behavior and coordinated attacks in real time, which is crucial for large and fast-growing Indian social media platforms. Incorporating multilingual and multimodal data (text, images, videos, and regional languages) will further enhance detection accuracy. Additionally, explainable AI (XAI) techniques can be applied to GNNs to improve transparency and trust in automated moderation systems. Privacy-preserving learning approaches such as federated and decentralized GNNs also present promising directions, enabling secure analysis without compromising user data, while making the system more compliant with data protection regulations.

VIII. REFERENCES

[1]. Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and P. S. Yu, "A comprehensive survey on graph neural networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 1, pp. 4–24, 2021.

[2]. W. Hamilton, Z. Ying, and J. Leskovec, "Inductive representation learning on large graphs," in *Proc. Advances in Neural Information Processing Systems (NeurIPS)*, 2017, pp. 1024–1034.

[3]. T. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," in *Proc. International Conference on Learning Representations (ICLR)*, 2017.

[4]. P. Velickovic, G. Cucurull, A. Casanova, A. Romero, P. Lio, and Y. Bengio, "Graph attention networks," in *Proc. International Conference on Learning Representations (ICLR)*, 2018.

[5]. C. Cao, M. Li, and J. Ma, "Detection of fake accounts in online social networks using graph-based features," *IEEE Access*, vol. 8, pp. 112–125, 2020.

[6]. S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, and M. Tesconi, "The paradigm-shift of social spambots: Evidence, theories, and tools for the arms race," in *Proc. International World Wide Web Conference (WWW)*, 2017, pp. 963–972.

[7]. J. Zhang, P. Cui, W. Zhu, and S. Yang, "Learning node embeddings from structural identity," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 2, pp. 387–400, 2018.

[8]. Y. Liu, S. Wang, F. Zhang, and X. Li, "Botnet detection on social networks using graph neural networks," *IEEE Transactions on*

Network Science and Engineering, vol. 9, no. 3,
pp. 1456–1468, 2022.