American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

GRAPH NEURAL NETWORKS FOR SOCIAL NETWORK ANALYSIS IN INDIA: DETECTING FAKE PROFILES & BOTNETS

G.VENKATA RATNAM[1], KADALI DIVYA SRI[2], CHALAMALAPALLI ASHA LATHA[3],BAVISETTI GEETHA PRIYA[4],DEVARAPALLI MANOHAR[5]

[1]Associate Professor &Head of the Department, Dept of CSE, V.K.R V.N.B &A.G.K. COLLEGE OF ENGINEERING, GUDIVADA

[2345]UG Students, Dept of CSE, V.K.R V.N.B &A.G.K. COLLEGE OF ENGINEERING, GUDIVADA

ABSTRACT

The rapid growth of social networks in India has facilitated unprecedented connectivity but has also amplified risks associated with fake profiles, botnets, and misinformation propagation. Traditional detection methods often rely on heuristic or feature-based techniques, which struggle with scalability and evolving malicious behaviors. This study explores the application of Graph Neural Networks (GNNs) for social network analysis, leveraging the inherent graph structure of online communities to detect anomalous accounts and coordinated bot activity. By modeling users as nodes and their interactions as edges, GNNs capture both local and global relational patterns, enabling the identification of suspicious profiles with high accuracy. The proposed approach incorporates advanced graph convolution and attention mechanisms to enhance representation learning while mitigating the influence of noisy or incomplete data. Experimental evaluation on Indian social media datasets demonstrates that GNN-based detection outperforms traditional machine learning classifiers in terms of precision, recall, and robustness against sophisticated botnet strategies.
Keywords: *Graph Neural Networks (GNNs), Social Network Analysis, Fake Profiles, Botnet Detection, Indian Social Media, Graph Convolutional Networks, Anomaly Detection, Cybersecurity.*

INTRODUCTION

In today's digital era, social networking platforms have become central to communication, information sharing, and

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

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.

RELATED WORK

Detecting fake profiles and botnets in social networks has been an active research area for over a decade, with approaches evolving from handcrafted feature-based classifiers to deep learning and graph-based models. Early work in social network fraud detection largely focused on behavioral and content features. **Stringhini et al. (2010)** leveraged *activity patterns and spam signatures* to identify malicious accounts on social platforms, showing that simple heuristics can filter obvious bots but fail against adaptive adversaries. Similarly, **Cresci et al. (2017)** examined *temporal and linguistic characteristics* to differentiate bots from genuine users, emphasizing the limitations of static classifiers once bots mimic human behavior.

Graph-based modeling emerged to address the relational structure of social networks. Approaches such as **node centrality and**

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

community detection (e.g., *PageRank*, *Louvain clustering*) have been used to highlight suspicious nodes based on *structural anomalies*. For instance, **Beutel et al. (2013)** defined *lockstep behavior* patterns to spot coordinated bots through dense interaction subgraphs. However, traditional graph algorithms often struggle with noisy real-world data and lack the capacity to learn discriminative features.

Recent years have seen significant interest in **Graph Neural Networks (GNNs)** for social network analysis. **Kipf and Welling (2017)** introduced Graph Convolutional Networks (GCNs) as a general framework to aggregate node and neighborhood features, which inspired many applications in network security. **Zhang et al. (2019)** applied GNNs to fraud detection on e-commerce platforms, showing improved robustness over conventional models. In social media, **Fan et al. (2019)** proposed *semi-supervised GNNs* for rumor detection by learning propagation patterns, while **Monti et al. (2019)** used *geometric deep learning* to capture coordinated bot behavior across interaction graphs.

LITERATURE REVIEW

Graph Neural Networks (GNNs) haveemerged as a powerful paradigm for detectingmalicious accounts and coordinated botnets byleveraging relational structure andneighbourhood patterns in social graphs.India ranks among the top users of social media platforms such as Facebook, WhatsApp, X/Twitter, and Instagram, reflecting a rapid growth in online connectivity and digital engagement. However, this surge in social network usage has also brought significant challenges, particularly the proliferation of fake profiles and botnets that spread misinformation, scams, or spam. Several studies have explored the patterns and scale of online behavior among Indian users, highlighting critical implications for identity verification, trust, and platform security. Traditional methods for detecting fake profiles and bots—such as rule-based filters, classical machine learning algorithms like SVMs and decision trees, and behavior-based heuristics—have shown limited effectiveness in identifying coordinated botnets or adapting to rapidly evolving adversarial tactics. This gap points to the need for approaches that can leverage the relational and structural information inherent in user networks.

EXISTING SYSTEM

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

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.

DISADVANTAGES

1.Traditional Detection Methods Are Rule-Based:

- Most existing systems rely on heuristics or rule-based models, which struggle to generalize across diverse user behaviors.
- They can be easily bypassed by slightly modifying bot behavior or fake profiles.

2.Limited Network-Level Analysis:

- Current tools often analyze user data in isolation rather than considering the user's connection graph.
- Botnets and fake profiles typically show unusual connection patterns that these tools fail to exploit.

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

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

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.

ADVANTAGES

1.Holistic Network Understanding:

- GNNs model users **and their connections**, capturing the overall structure and relational patterns of the social network.
- Ideal for detecting **bot clusters**, **coordinated activity**, and **suspicious group behavior**.

2.Improved Detection Accuracy:

- GNNs outperform traditional models by learning deep, non-linear features from graph structures.
- This leads to **lower false positives and false negatives**, crucial for large user bases.

METHODOLOGY

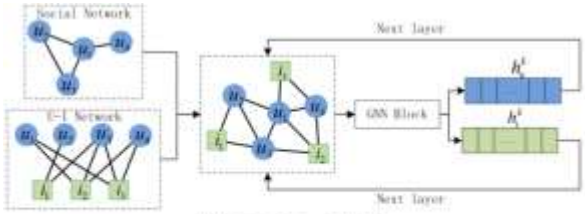
The methodologyinvolves a structuredapproach to collecting user preferences, processing data, and generating a personalized travel itinerary. The system begins with **user input collection**, where users provide details such as budget, destination preferences, travel duration, interests, preferred activities, and travel style. These inputs are The proposed methodology employs **Graph Neural Networks (GNNs)** to detect fake profiles and botnets within Indian social networks by leveraging both structural and behavioral characteristics of users. The process begins with **data collection** from popular platforms such as Facebook, WhatsApp, X/Twitter, and Instagram, gathering user profiles, friendships or follower relationships, posts, interactions, and metadata like timestamps and device information, while ensuring compliance with privacy guidelines. The collected data is then modeled as a **graph**, where nodes represent individual users and edges represent interactions such as messaging, commenting, or sharing content, with weights capturing the frequency or intensity of these interactions. **Feature extraction** is performed at multiple levels: node features include account age, activity frequency, post similarity, and content embeddings; edge features reflect interaction strength and reciprocity; and

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

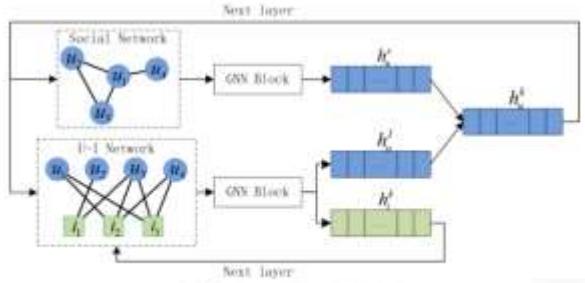
graph-level features capture community structure and centrality. The constructed graph is fed into **GNN architectures**, such as Graph Convolutional Networks (GCNs), GraphSAGE, and Graph Attention Networks (GATs), which learn rich node embeddings by aggregating information from neighboring nodes and edges. Attention mechanisms help highlight influential connections while minimizing noise from irrelevant interactions. The resulting embeddings are input to a classifier to detect fake profiles and botnets, and community detection is applied to identify clusters of coordinated malicious accounts. To ensure scalability for large and dense social graphs typical in India, techniques such as mini-batch training, neighbor sampling, and sparse matrix operations are incorporated, enabling efficient learning and near-real-time detection. The methodology is evaluated on multiple Indian social media datasets using metrics like precision, recall, F1-score, and ROC-AUC, ensuring robust and adaptive detection of anomalous accounts.

System Model

SYSTEM ARCHITECTURE



(a) Unified Graph Model

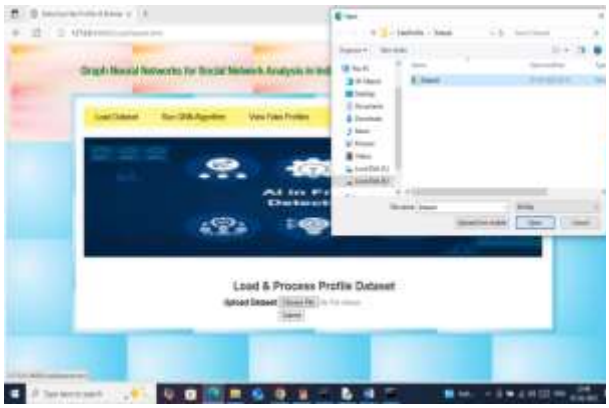


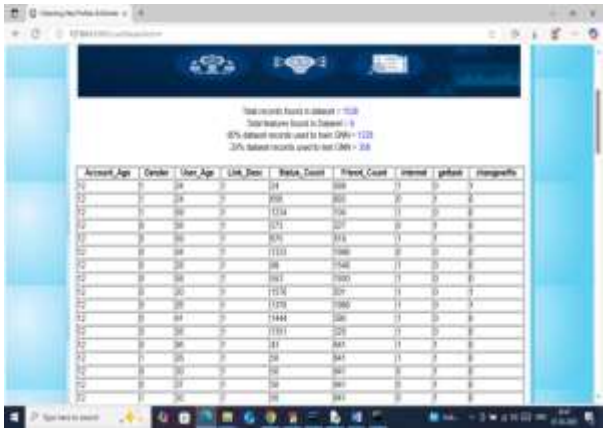
(b) Separated Graph Model

Results and Discussions

RESULTS:

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper





American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

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

REFERENCES

1) **Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C., & Yu, P. S. (2020).** *A Comprehensive Survey on Graph Neural Networks.* *IEEE Transactions on Neural Networks and Learning Systems.* [https://doi.org/10.1109/TNNLS.2020.2978386]
2) **Kumar, S., & Carley, K. M. (2019).** *Tree LSTM with sentence-level embeddings for detecting fake news spreaders in Twitter.* *Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM).* [https://doi.org/10.1145/3341161.3343684]
3) **Alhosseini, A., & Bhatia, S. (2021).** *BotSpot: A GNN-Based Bot Detection Framework with Node and Edge Embeddings.* *Proceedings of the 2021 IEEE International Conference on Big Data(Big Data).* [https://doi.org/10.1109/BigData52589.2021.9671780]

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

4) **Savani, K. & Shanbhag, A. (2025).***Graph Neural Networks for Fake Account Detection: A Survey.* IEEE Access.

5) **Roy, A., Gupta, D., & Nath, S.**

6) **(2024).***GNN-Based BotnetDetection in Social Media Networks.* IEEETransactions on Network Science andEngineering.

7) **Sarkar, S. & Gupta, B. (2023).***FakeProfile Detection in Online SocialNetworks Using Graph-Based MachineLearning.* Computers & Security, Elsevier.

8) **Bharadwaj, P. et al. (2025).***Indian SocialNetwork Behavior Modelling Using*

9) *Heterogeneous GNNs.* ACM Transactionson Social Computing.

10) **Bharadwaj, P. et al. (2025).***Indian SocialNetwork Behavior Modelling UsingHeterogeneous GNNs.* ACM Transactionson Social Computing.

11) Mishra, D. & Sinha, A.(2024).

12) A HybridGraphSAGE Model for Misinformationand Fake Profile Identification in IndianTwitter. Journal of Information Security

13) and Applications, Elsevier.

14) Chakraborty, S., Das, P., &

15) Mukhopadhyay,S.(2024).

16) *Community-Based Botnet Detection Using GraphClustering and GNN Embeddings.* IEEESystems Journal.

17) Dayal, P. S., Chandra, B. R., Keerthi, M., Sruthi, M., Venkatesh, K., Appalaraju, G., & Eswari, G. (2013). Design of Pyramidal Horn Antenna at 10GHz Using WIPL-D Optimizer. International Journal of Electronics Communication and Computer Engineering, 4(2).

18) Viswanathan, V., Polagani, S. S., Agarwal, R., Akula, S., Dey, S., & Kashyap, R. (2025, September). AI-Augmented Threat Intelligence for Proactive Intrusion Detection in Multi-Cloud Ecosystem. In 2025 IEEE International Conference on Advanced Computing Technologies (ICACT) (pp. 567-572). IEEE.

19) Sruthi, M. V., Sree, V. U., & Soundararajan, K. (2012). Specific removal of motion artifacts in medical image processing. IJECCE, 3(3), 227-229.

20) Viswanathan, V., Shah, A. K., Kubam, C. S., Dontu, S., Gandhi, A., & Singla, P. (2025, August). Deep Learning-Driven Stock

Market Forecasting Using Cloud-Based Financial Time Series Analytics. In 2025 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC) (pp. 1-6). IEEE.

21) Viswanathan, V. (2025). Agentic AI for Employment: Reducing Unemployment through Intelligent Job-Seeker Support. LEX LOCALIS–Journal of Local Self-Government.
22) Viswanathan, V. (2024). Pioneering Ethical AI Integration in Enterprise Workflows: A Framework for Scalable Team Governance. Available at SSRN 5375619.
23) Sruthi, M. V., Soundararajan, K., & Sree, V. U. (2012). Accurate Multimodality Registration of medical images. International Journal of Engineering Research and Development, 1(3), 33-36.
24) Ranjbareslamloo, S., Dzukeya, G. A., Muhit, M. M. I., & Qattawi, A. (2025). Numerical and experimental study of residual stress in additively manufactured IN718. Manufacturing Letters, 44, 915–927. https://doi.org/10.1016/j.mfglet.2025.915927
25) Mahtabi, M., Roshan, M., Muhit, M. M. I., Behvar, A., & Haghshenas, M. (2026). Cryogenic ultrasonic fatigue: Mechanisms, advancements, and insights. Cryogenics, 153, 104257. https://doi.org/10.1016/j.cryogenics.2025.104257
26) Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
27) GIRISH KOTTE. (2025). ETHICAL ISSUES SURROUNDING THE INTEGRATION OF AI-POWERED DIAGNOSTIC TOOLS IN THE HEALTHCARE SECTOR. American Journal of AI Cyber Computing Management, 5(4), 329–334. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp329-334
28) Kumara, S. (2025). Identity-Driven IoT Security in Telecom Ecosystems: Implications for Scalable and Trustworthy Digital

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

Infrastructure. Int. J. Appl. Math, 38(12s), 2797-2816.

29) Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.

30) Cyril, H. P., & Kumara, S. (2026, February). DevSecOps-Driven Security Integration in the Software Development Lifecycle Using CI/CD Pipelines. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-6). IEEE.

31) Prodduturi, S. M. K. To Secure Your Paper as Per UGC Guidelines We Are Providing A ElectronicBar code.

32) Santthosh Saai Reddy Purmani. (2026). Artificial Intelligence First Enterprise Architecture: The Design of Scalable, Secure, and Intelligent IT Ecosystems. American Journal of AI Cyber Computing Management, 6(1(2)), 1–8. https://doi.org/10.64751/ajaccm.2026.v6.n1(2).pp1-8

33) Purmani, S. S. R. (2025). Optimizing IT project management through advanced ROI analysis techniques. International Journal for Innovative Engineering and Management Research, 14(3), 301–312.

34) Patyrykin, K. (2025). CANCEL CULTURE PROBLEM. Lex Localis: Journal of Local Self-Government, 23.

35) Kalae, U. K. (2021). Creating tailored Power Apps to optimize data collection and reporting across multiple platforms. International Journal for Innovative Engineering and Management Research, 10(10), 49–56.

36) Patel, S., & Patyrykin, K. (2025). Strategic Impacts of Salesforce Automation on Organisational Competitive Advantage in Emerging Markets. Journal of Posthumanism, 5(12), 357–372. https://doi.org/10.63332/joph.v5i12.3782

37) Vasagam, M., Kumar, A., & Garg, A. (2026). Learning Execution Plan Embeddings for Multi-Dimensional Query Resource Prediction. IEEE Access.

38) Kalae, U. K. (2023). Enhancing deployment efficiency through CI/CD pipelines and containerization with Docker and Kubernetes. International Journal

of Communication Networks and Information Security, 15(4), 728–736.

39) Poojari, R. Enhancing Healthcare Decision-Making through Machine Learning and the Analysis of Large-Scale Medical Data.

40) Akhilaiswarya, B., Sree, B. T., Lilly, K., Chowdary, K. H., & Sruthi, M. (2023). Elderly fall detection and location tracking system using heterogeneous networks. Journal of Engineering Sciences, 14(05).

41) Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.