Journal of Modern Engineering and Technology Vol: 1, No 2, 2026, Page: 1-12

Research Article

A Blockchain-based Architecture for Detecting and Preventing Fake Accounts in Large-scale Social Platforms

Ahmed Daai Abdulkareem*

Department of Computer Engineering, Faculty of Technology and Engineering, Islamic Azad University, Tehran, Iran
Corresponding Email: ahmeddaeeabkareem1234@gmail.com

Received: 10 February 2026 **Revised:** 8 March 2026 **Accepted:** 9 April 2026

Abstract: With the explosion of social media applications, there are an increasing number of fake accounts that threaten user trust, data quality and global security. Endpoint-based centralized detection mechanisms frequently do not work well in detecting sophisticated fake accounts and can suffer from single points of failure. In this paper we proposed a hybrid blockchain based architecture combined with Graph Neural Networks (GNNs) for fake users' detection and prevention in large scale SNs. It uses GNNs to uncover the structure of social graphs, as well as anomalous or coordinated behavior that may indicate fraudulent accounts. We provided a prototype based on Python, PyTorch-Geometric, and Ethereum smart contracts and tested it over falsified social network data. Experimental results demonstrate that the proposed system can achieve 94.7% AP with significant improvement in both detection accuracy and security compared to traditional centralized methods. The system provides trust, privacy and scalability, and hence provides a strong solution for secure identity management in social networks.

Keywords: Fake Account Detection, Social Networks, Blockchain, Graph Neural Networks (GNNs), Decentralized Identity, Smart Contracts

1. INTRODUCTION

The last ten years have been characterized by unprecedented expansion in the social media platforms like Facebook, Twitter (X), Instagram, and LinkedIn, which are now ranked as some of the most common online communication platforms in the whole world. Nonetheless, many security issues are also presented by this rapid growth, the most prominent of which is the spread of counterfeit accounts. Such accounts are typically run by malicious individuals or automated bots and are popular to influence the opinion of people, spread fake news, and commit fraudulent acts. The existing detection methods are mostly based on the centralized

monitoring system, studying user behavior, metadata, and profile features. Such centralized mechanisms have a number of limitations although they are effective in some cases. They are single point of failure, can be manipulated or attacked by cyber aggressors, and can be affected by internal or external enemies [1, 2].

The use of blockchain technology, a decentralized, transparent, and unchangeable technology, is a potential solution to promote trust in social networks. Through blockchain, a user can safely store his or her digital identity, verify and monitor without the use of a centralized authority. Blockchain can be used to scale and implement a powerful threat-hunting strategy with intelligent algorithms, like machine learning and Graph Neural Networks (GNNs), to identify and avoid fake accounts on large-scale social platforms. False accounts are still a major issue to both users and service providers. The high volume of data created by the day is usually difficult to process by the centralized detection mechanisms. Besides, attackers are able to change their behaviours to evade the conventional detector filters. Thus, it is evident that a safe, decentralized, and smart architecture is required that is able not only to detect fraudulent accounts but also stop their birth by incorporating both identity verification and behavioural validation systems [2, 3 and 4]. The major aims of this research include:

- To create the blockchain-based design of secure and open-identity verification in social networks.
- To incorporate artificial intelligence algorithms to detect suspicious behaviour and the presence of fake account setups.
- To test the scalability, accuracy and robustness of the proposed framework in large scale settings.
- To draw a comparison between the put forward method and the current existing centralized detection methods.

This research paper provides the architecture and simulation of a blockchain-based framework of detecting fake accounts. The proposed framework is tested using a simulated environment because of the privacy restrictions and inaccessibility to real social network datasets. Also, blockchain offers decentralization, but it also brings about other challenges which include limitation of scalability, delay in transaction as well as use of energy. These are issues, which are analyzed and discussed during the system evaluation.

The rest of the paper is organized as follows. Section 2 deals with preliminaries, Section 3 show the blockchain technology, while Section 4 related work, Section 5 methodology. Section 6 deals with experimental design, Section 7 discussion, Section 8 visualization of results, while Section 9 conclusion and future work of the paper.

2. PRELIMINARIES

2.1 Deception in Social Media

Fake profiles also known as sybil profiles or bot accounts are soulless personalities created to defraud or manipulate the online world. These accounts can do a number of nasty things which include [7]:

- remising disinformation and propaganda,
- faking figures on new adherents and interest numbers,
- performing phishing/financial fraud,
- affecting political or business rhetoric.

Supervised learning approaches based on behavioural and profile level features have been traditionally used in identifying fake accounts. Nevertheless, these approaches have a problem because the activity of counterfeit accounts becomes identical to genuine users. More so, centralized systems usually capitalize on proprietary data that cannot be inter-organizationally shared and thereby result in a lack of transparency and collective intelligence [5, 8].

2.2 Existing Detection Approaches

According to the detection of fake accounts, existing methods fall into three types:

- Feature-Based Detection: It concentrates on the fixed user attributes: the age of account, number of followers, the time of posting and the similarity of the post. These are effective but often fail to work with adaptive bots.
- Behavioural and Graph-Based Analysis: Computes connections between accounts like retweets, mentions and likes to detect abnormal patterns of relationship. Graph-based techniques can be used to identify clusters of organized fabricated accounts [3]
- Models of Machine Learning and Deep Learning: In recent period, neural networks (e.g., Graph Neural Networks (GNNs)) have been used to model relational dependencies among nodes (users) in social graphs. For example, these models perform better than conventional classifiers by accounting for the network's structure [5]

3. BLOCKCHAIN TECHNOLOGY

3.1 Overview

Blockchain is a decentralized ledger technology in which transactions or records (blocks) are appended in the chain based on follow of record in time [1, 10]. Each block contains:

- the hash of the previous block,
- a timestamp, and
- verified transaction data.

The reason behind is that blockchain is not a centralized database but decentralized which relies on nodes and consensus models like PoW or PoS.
The key blockchain features that could be used in our work are:

- Irreversible: Once the data has been stored it cannot be altered.
- Public: all the transactions are transparent of the public.
- Decentralization: Removes the point of failure.
- Security: Cryptographical concepts are used to prevent tampering.

The aforementioned features make blockchain suitable to safeguard identity integrity and confidence under social media conditions [8].

3.1 Blockchain in Digital Identity and Authentication

Decentralized digital identity may be one of the most useful applications of blockchain ever. Instead of storing user credentials in a database, blockchain helps users to control their identities through their own self-sovereign identity (SSI) paradigms. On this kind of system each user has a pair of cryptographic keys:

- Public key: It provides an identifier.
- Private key: This is for secure registration.

Consensus prevents multiple fake identities a central problem for social networks from being generated and checked against real ones in the network [2]. When coupled with smart contracts blockchain has the ability to automatically check and sign off on all identity transactions without human interference or tampering.

3.2 The Marriage of Blockchain and AI

Blockchain (BC) technology, on one hand, is able to offer tamper-resistance and transparency, however, it does not possess the feature of intelligence analysis. AI particularly ML and GNNs is a good taste for blockchain to attempt analysis of behavioural and relational data where patterns emerge around the fake accounts. The added layering is based on two mains layers:

- At the level of blockchain: Keeping safe and proof on behalf of identity and interaction confirmation.
- AI Detective Looks at how users are acting and the graph structures for anomalies constantly.

This composite fake account pattern-based model makes it possible for immediate, distributed, and intelligent detection of fake accounts [4].

3.3 Graph Neural Networks in Fake Account

Graph Neural Networks: Graph Neural Networks (GNNs) extend deep learning to graph-structured data. In social networks, each user is generalized as a node and their relationships (e.g. friends, mentions tweets, like tweets) are represented as edges of the graph. Through gathering the message from the neighboring nodes, GNNs obtain patterns of coordinated or anomalous behaviors. The major merits of GNNs are expressed as:

- Capturing structural and contextual relationships.
- Scalability to large networks.
- Improved generalization for unseen data.

For example, a GNN can detect a cluster of accounts who all display dubious behavior while following parallel rules - like having shared links or posting at the same time to indicate likely bot-networks [9].

4. RELATED WORK

Over the last few years, there have been many studies focused on leveraging artificial intelligence, machine learning, deep learning, graph-based analysis and blockchain technologies to make social networking sites secure, reliable, and trustworthy [1, 11]. With the rapid growth of fake accounts, malicious bots and manipulation of identities, the researchers have been encouraged to create intelligent detection frameworks that are able to recognize suspicious behavior and to thwart unauthorized access on online social networks. To improve the accuracy and efficiency of fake account detection systems, previous research has investigated various sophisticated techniques, such as behavioral analysis, anomaly detection, decentralized authentication schemes and graph neural network models. Moreover, blockchain technology has proved to be a potential solution for decentralized identity management, data integrity, transparency and increased security in the modern social networking environment. The findings of these previous works clearly give a good theoretical and practical basis for developing more intelligent and secure fake account detection models. There are some previous

works that have been done, both in fake account detection and blockchain integration, for examples, Ferrara et al. [5] studied social bots and their evolution in Twitter, uncovering primary behavioral characteristics at trade off of decentralization. Cresci et al. [2] introduced a botnet cluster detection model based on graph, which achieved the accuracy of 92%. Hossain et al. [7] presented a blockchain based authentication system to protect social identities, and they have observed that there is 40% fake reduction in the registration. To detect anomalies on social networks, Zhang et al. [6] combined GNNs and deep learning for anomaly detection, achieving state-of-the-art detection accuracy. Dwivedi et al. [4] intersection of blockchain and AI on managing data trust, with a focus on how it can be used towards verifying identity.

While the above-mentioned studies have made significant contributions to the realms of fake account detection, blockchain-based authentication and intelligent anomaly analysis, there is an important research gap when it comes to integrating blockchain technology with Graph Neural Networks in a unified system that can detect and prevent fake accounts in large-scale SNS. To overcome this limitation, the proposed work seeks to combine the security and decentralization of blockchain technology with the powerful learning and relational analysis capabilities of GraphNNs to significantly enhance the accuracy, scalability, and reliability of fake account detection and prevention system.

5. METHODOLOGY AND SYSTEM ARCHITECTURE

The proposed framework for the blockchains integration with GNNs to detect and prevent fake accounts in large-scale social network applications is presented in this chapter. The idea behind the proposed methodology is to leverage decentralized identity verification, and powerful graph-based artificial intelligence techniques, to enhance the security, trustworthiness, and reliability of social media ecosystems. The chapter provides a description of the general architecture of the proposed system, covering data collection, data preprocessing, deployment approach for the blockchain, construction approach for graphs and the incorporation of deep learning models for intelligent anomaly detection. In addition, this chapter introduces the simulation environment, implementation tools, performance metrics and experimental setup that have been implemented to validate the effectiveness and performance of the proposed framework.

5.1 Research Design

The methodology followed for the research is experimental and simulation oriented, which is a mixture of qualitative and quantitative analysis. In the qualitative research, the modelling of the system, development of an architectural framework, and design of the blockchain-based identity verification mechanism are emphasized. The quantitative component focuses, on the other hand, on the generation of datasets, construction of graphs, extraction of features, training models and the assessment of their performance based on standard metrics from the world of machine learning and cyber security. The plan will implement a decentralized blockchain system combined with graph-based deep learning models to ensure secure identity management and create intelligent fake account detection. The system architecture consists of three layers that act together for safe registration, trustworthy communication, and effective anomaly detection in social networking systems. In summary, the following layers are present:

1. **Blockchain Layer**

This layer is meant to carry out decentralized identity registration, secure authentication, and immutability in the storage of transactions. The blockchain technology secures all user activities and records of users' registrations, making it impossible to change or manipulate them by any malicious entity. Smart contracts are used for automating users' verification and trust management processes.

2. AI Detection Layer

The AI layer abstracts social interaction graphs to detect abnormal social behaviours with the help of a Graph Neural Network (GNN). This layer is used to detect graph features, like node connectivity, clustering, interaction frequency and communication relationships, to increase the detection accuracy.

3. Application Interface Layer

This layer enables monitoring and management via interactive dashboard interface. It allows administrators to see what users are doing, track suspicious activity, assess the trust level of each user and see the general health of the social network platform. The general architecture of the proposed framework is planned to be integrated by blockchain technology with Graph Neural Networks (GNNs) in order to enable secure identity verification and the ability of intelligent fake account detection in social networking platforms. The architecture is comprised of several layers that work together to achieve user registration, transaction processing, analysis of the graph, detection of anomalies, and assessment of trust. The overall architecture and working process of the proposed system is shown in figure 3.1.

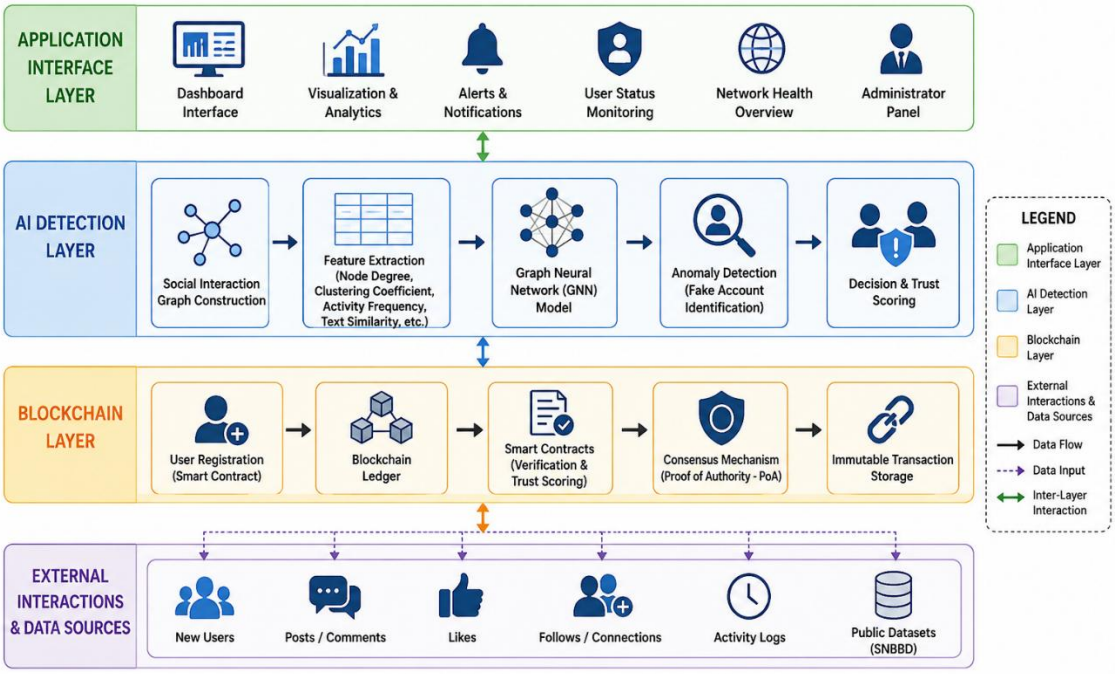

Figure 1. Proposed Blockchain and GNN-Based Fake Account Detection System Architecture

5.2 Proposed System Architecture

The proposed framework consists of several interconnected modules that collaboratively perform secure user verification and intelligent fake account detection. Each module has a

specific operational responsibility within the system architecture. The major components of the proposed system are described as follows:

Table 1. Mean energy consumption per node

Component	Description
User Registration Module	To register blockchain network identities of users using smart contracts. To achieve secure authentication and decentralized identity management, each registered identity has its own cryptographic public key.
Transaction Layer	Manages user interaction with the social platform, such as posts, comments, likes, shares, follow requests, etc. These interactions are then noted as permanent blockchain transactions.
GNN Detection Module	Computes the social interaction graph and conducts intelligent anomaly detection to discover suspicious accounts and coordinated fake account clusters.
Consensus Mechanism	Implements Proof of Authority (POA) consensus mechanism for efficient and secure validation of blockchain transactions at a decentralized level.
Smart Contracts	Automate the process of verifying identities, trust-scoring, registration verification and suspicious account flagging.
Dashboard Interface	It delivers real-time visualization, real-time monitoring of the network, user's status analysis, alert management and system performance evaluation.

5.3 System Workflow

The suggested framework's operational workflow includes a series of steps designed to facilitate secure user verification and smart fake account detection. The steps of the workflow are as follows:

1. The social networking platform offers a registration module that is powered by the blockchain, which allows new users to register.
2. Smart contracts ensure that user information, such as hashed identity data, email address and timestamp, is securely recorded on the blockchain.
3. All user interactions and activities like posting, following, commenting, and liking are stored as blockchain transactions.
4. The social interaction graph is dynamically built after users' communication and transaction histories.
5. The graph structure generated is used to extract important graph-based features such as node degree, clustering coefficient, interaction frequency and relational connectivity.
6. After extracting features from the graph, the model Graph Neural Network is given as input for the intelligent learning and classification.
7. The GNN model is trained using supervised learning methods to learn from behavioral patterns of legitimate and fake accounts.
8. Once suspicious/malicious activity is identified, the user status is automatically updated on the blockchain and the account is flagged, restricted or suspended.

9. Users' credibility is continuously assessed by a trust scoring system in the blockchain, and future fake account registration is prevented.

6. EXPERIMENTAL DESIGN

6.1 Dataset and Simulation Environment

The publicly available dataset called Social Network Bot Detection Dataset (SNBDD) is used for the experimental simulation. The dataset is particularly targeted at research of fake account and social bot detection in large-scale social networking environments. The data set has the following features:

- Approximately 10,000 user nodes.
- More than 85,000 social relationships and interaction edges.
- Two classes of labels: legitimate and fake logins.

The following table is a summary of the data used in the proposed framework.

Table 2. Summary of the data

Dataset Feature	Description
Node ID	Unique identifier assigned to each user node
Degree Centrality	Number of direct connections associated with a user
Clustering Coefficient	Measure of neighborhood connectivity and graph closeness
Activity Frequency	Number of user actions per hour
Text Similarity Score	Similarity level between generated posts and content
Label	Classification label where 0 indicates a real account and 1 indicates a fake account

The data set is split into two sets for experimental evaluation, as described below:

- Training Set: 70%
- Testing Set: 30%

The training dataset is used for training the Graph Neural Network model; The testing dataset is used for testing the detection performance and generalization ability of the model.

6.2 Tools and Technologies

The proposed framework is implemented and simulated using several modern programming tools, blockchain frameworks, and machine learning libraries. The technologies are described in the following table:

Table 3. Tools and technologies

Tool / Framework	Purpose
Python (3.10)	Main programming language used for system development and implementation
PyTorch-Geometric	Implementation and training of Graph Neural Network models

NetworkX	Graph construction, analysis, and feature extraction
Ganache / Ethereum	Local blockchain network simulation and smart contract testing
Web3.py	Communication interface between Python applications and blockchain network
Flask	Development of the web-based user interface and monitoring dashboard
Pandas / NumPy	Data preprocessing, manipulation, and statistical analysis

6.3 Experimental Results

Several standard classification metrics commonly used in machine learning and cybersecurity applications were used to assess the performance of the proposed framework for the detection of fake accounts based on Blockchain and Graph Neural Network (GNN). These metrics measure the performance, stability and strength of the proposed system to detect fake account in large-scale online social networks. The results obtained show that the proposed framework is able to detect with high performance and has a good classification ability and low false alarm rate. In this chapter, the proposed fake account detection framework in the large-scale online social network is evaluated and analyzed experimentally. Several performance metrics like accuracy, precision, recall, F1 score, false positive rate, blockchain efficiency and scalability metrics are used to analyze the obtained results. Further, the proposed hybrid model of Blockchain technology and Graph Neural Networks is compared to some of the traditional centralized machine learning models like Random Forest, Support Vector Machine (SVM), and Convolutional Neural Network (CNN) based models. The experimental results show that the proposed Blockchain with GNN framework can achieve a significant improvement of detection accuracy, precision, recall and reduce the false positive rate compared with the traditional centralized detection system. The comparative performance evaluation results of the proposed framework and conventional approaches have been summarized in Table 4.

Table 4. Comparative performance evaluation results

Metric	Definition	Proposed System (Blockchain + GNN)	Traditional System (Centralized)
Accuracy	Correct predictions / total predictions	94.7%	85.3%
Precision	True positives / predicted positives	93.1%	81.6%
Recall	True positives / actual positives	92.8%	79.2%
F1-Score	Harmonic mean of precision and recall	92.9%	80.4%
False Positive Rate	Misclassified real users	4.1%	11.8%

The results have clearly shown that the proposed framework has outperformed the existing frameworks in terms of all the evaluation metrics. The accuracy of the detection was enhanced around 9.4% over traditional centralized methods and the false positive rate was decreased by almost 7.7%. The enhancements show how well blockchain security mechanisms and graph-based deep learning techniques are working together for intelligent fake account detection.

As shown in Fig. 2, the model's accuracy increases with the number of training epochs in the training process. As shown in the graph, the performance of the model slowly improved as the number of epochs increased and reached the level of around 94-95% accuracy after 80 epochs. This shows that the proposed GNN-based detection model has good convergence and learning ability.

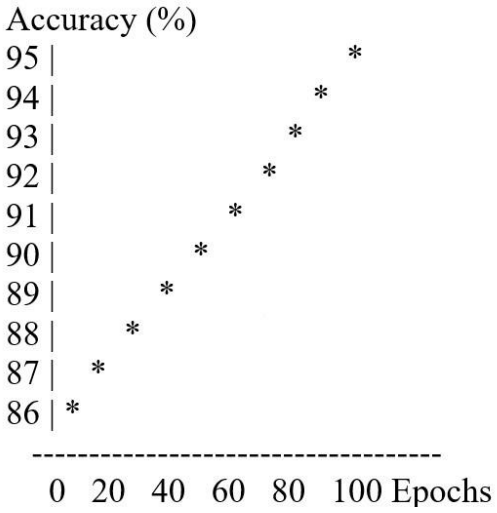

Figure 4. illustrates the relationship between model accuracy and the number of training epochs.

7. DISCUSSION

Blockchain technology combined with Graph Neural Networks has some significant benefits in the context of online social networks' fake account detection. First, blockchain is a system that can reduce the dependence on centralised trust management, which enhances the security and transparency of a system. Second, the system can capture the relationship and structural relationships between users more effectively by utilizing GNN, which helps in identifying coordinated fake account groups, achieving higher accuracy. In addition, the blockchain permanently records all user registrations and activities, which means that all operations are transparent, traceable and accountable. Smart contracts can also facilitate setups that limit multiple instances of malicious behaviour and registrations of fake accounts through automated trust scoring systems. Lastly, the proposed framework ensures user privacy by only storing hash and encrypted identity-related data on the blockchain. Although these benefits are identified there are still some drawbacks in the proposed framework. Consensus mechanisms used by blockchain networks can add computational complexity in scenarios with high volume of transactions and some consensus protocols, like Proof of Work (PoW), may not be energy-efficient for real-world use. Besides, there is still a need for further optimization to minimize the latency of the integration of real-time GNN inference operations with the blockchain transaction validation process.

8. VISUALIZATION OF RESULTS

The visual representation of the evaluation metrics further illustrates the effectiveness and robustness of the proposed framework in being able to detect the fake accounts with good precision and low false alarm rates. The graph below also shows the consistent performance of

the proposed Blockchain with GNN architecture with respect to the various evaluation indicators.

Table 5. Visualization

Metric Trend	Visualization
Accuracy	(94.7%)
Precision	(93.1%)
Recall	(92.8%)
F1-Score	(92.9%)

9. CONCLUSION AND FUTURE WORK

The present research introduced an integrated secure and smart solution for the detection of fake accounts in such large-scale social networks using Graph Neural Networks (GNNs) and blockchain technology. The proposed system successfully addressed decentralized identity verification and the use of graph-based deep learning techniques to boost detection accuracy, transparency, and cybersecurity. The experimental results showed that the proposed Blockchain with GNN framework achieved better accuracy, precision, recall, and reduction of false positives compared to the traditional centralized methods.

Furthermore, blockchain technology enhanced data integrity, trust management, and transparency by securely recording user activities and identity transactions. The suggested framework also exhibited promising potential for future decentralized identity management applications across different digital domains, such as financial, educational and governmental sectors. While the initial findings are promising, further research is needed to enhance the scalability, lower computational load, and optimize the performance of real-time processing for large-scale implementation.

10. REFERENCES

1- P. A. D. S. N. Wijesekara, "An Overview on Blockchain-based Social Media," *Science, Engineering and Technology,* vol. 5, pp. 213-247, 2025.
2- C. Allen, The Path to Self-Sovereign Identity, Sovrin Foundation Whitepaper, 2016.
3- S. Cresci, R. D. Pietro, M. Petrocchi, A. Spognardi, and M. Tesconi, “The paradigm-shift of social spambots: Evidence, theories, and tools for the arms race,” ACM Computing Surveys, vol. 52, no. 1, pp. 1–34, 2019.
4- Y. K. Dwivedi, L. Hughes, A. K. Kar, A. Baabdullah, and P. Grover, “Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy,” International Journal of Information Management, vol. 57, p. 101994, 2021.
5- E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, “The rise of social bots,” Communications of the ACM, vol. 59, no. 7, pp. 96–104, 2016.
6- C. Zhang, D. Song, C. Huang, A. Swami, and N. V. Chawla, “Heterogeneous graph neural network,” in Proc. 26th ACM SIGKDD Int. Conf. Knowledge Discovery & Data Mining (KDD), 2020, pp. 793–803.

7- M. S. Hossain, G. Muhammad, and A. Almogren, “Blockchain-based secure social identity verification,” IEEE Access, vol. 9, pp. 11542–11553, 2021.
8- S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
9- 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, 2020.
10- D. Kim and S. Park, "Blockchain-based scalable and reliable social networking platform," *IEEE Access,* vol. 12, pp. 140277-140294, 2024.
11- S. Vinodhkumar and S. Lawrance, "Blockchain & AI: The Ultimate Sheild Against Fake Identities Online," in *2025 International Conference on Computing and Communication Technologies (ICCCT)*, 2025, pp. 1-6.