Journal of Information Systems Engineering and Management
2025, 10(15s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Proposed Model to Find Most Prominent Node in Social Media Network for Cyber Crime Detection Using Modified Cluster Walktrap and Analytical Hierarchy Process

Faz Mohammad[1], Dr. Rakesh Kumar Yadav[2]
[1]*Research Scholar, CSE Department, Maharishi University of Information Technology, Lucknow, email: faiz.contactid@gmail.com*
[2]*Associate Professor, CSE Department, Maharishi University of Information Technology, Lucknow, email: rkymuit@gmail.com*

ARTICLE INFO

Received: 30 Nov 2024

Revised: 25 Jan 2025

Accepted: 03 Feb 2025

ABSTRACT

With the proliferation of extensive network structures and real-time information exchange, social media platforms have become pivotal sources for the detection of criminal activities. This study presents a two-phase computational framework designed to identify and analyze criminal communities within social media networks. In the initial phase, a modified Cluster Walktrap algorithm is employed to detect criminal communities by leveraging the graph-theoretic properties of social media interactions. This approach enhances the accuracy of community detection by optimizing the clustering process to address the distinctive characteristics of criminal networks. In the subsequent phase, the Analytical Hierarchy Process (AHP) is utilized to identify the most influential node within the detected criminal communities. AHP integrates multiple parameters, including degree centrality, betweenness centrality, and mean distance, to systematically evaluate and rank nodes based on their influence within the network. The incorporation of multiple parameters enhances the robustness and reliability of the results. The proposed framework represents a significant advancement in criminal network analysis by integrating sophisticated clustering methodologies with multi-criteria decision-making techniques, thereby improving the accuracy and interpretability of criminal activity detection in social media environments.

Keywords: Social Media Networks Analysis, Criminal Community Detection, Modified Cluster Walktrap, Analytical Hierarchy Process, Degree of Node, Betweenness, Mean distance of the ndoes

INTRODUCTION

Social Media Network

Online social networks (OSNs) have emerged as a crucial platform for digital interactions, providing users with various online social services, including image sharing, messaging, and advertising. These platforms facilitate virtual relationships, enabling seamless communication and content dissemination. Prominent OSNs such as Facebook, LinkedIn, Twitter, Telegram, Instagram, MyGov.in, and YouTube have experienced continuous growth in popularity due to their widespread adoption [1].

Despite their numerous benefits, OSNs also present significant cybersecurity risks. The disclosure of personal information on these platforms increases users' vulnerability to cybercrimes. Victims may refrain from reporting such incidents due to factors such as perceived insignificance, social stigma, or lack of awareness [2]. To complement conventional crime reporting mechanisms, social media monitoring can serve as an alternative approach for detecting and addressing cybercrimes. As with other emerging communication technologies, OSNs have also become a medium for illicit activities, necessitating robust security measures and regulatory interventions to mitigate cyber threats effectively. [3].

Criminal Community on Social Media

In the context of social media networks, a community is defined as a group of individuals who share common interests or objectives and engage collectively to pursue similar activities. Within this framework, the present study focuses on communities comprising cybercriminals or individuals who exploit social media platforms to facilitate criminal activities [4]. Understanding the structural and behavioral patterns of such criminal communities is essential for developing effective detection and intervention strategies. By analyzing these networks, it is possible to gain insights into their operational mechanisms, thereby contributing to the advancement of cybersecurity measures and digital forensic investigations [5].

Social Media Network as Graph

A social structure represents the interconnectedness of individuals and organizations through various forms of social relationships, ranging from casual acquaintances to close familial bonds. This interconnectedness can be effectively modeled using a social network graph, where nodes denote discrete entities such as individuals or organizations, and edges represent the relationships or interactions between them [6]. Social network analysis (SNA) provides a systematic approach to understanding these connections, enabling the identification of key patterns, influential entities, and community structures within the network. Such representations play a critical role in diverse applications, including behavioral analysis, information dissemination, and cybersecurity investigations [7].

Node attributes

Node attributes can represent information about the node, e.g. personal information such as name, age, sex, or organization and graph based information such as degree, betweenness, mean distance, triangle formed etc [8, 21].

Visualization

Social network graphs can be visualized to reveal hubs, which are nodes with a large number of social links [9].

Graph-based methods

Graph-based methodologies have proven effective in detecting malicious accounts within social networks. The intricate structure of social graphs arises from the diverse relationships between nodes, including common acquaintances, shared interests, and ideological affiliations, making these connections interdependent. Due to the vast number of nodes and the complex interconnections among them, social networks often exhibit a highly intricate graphical structure, comprising millions of nodes and thousands of edges [9]. In computational terms, a graph represents a network of entities, referred to as nodes or vertices, which are linked through edges that define their relationships [10]. Graph theory serves as the foundation for understanding social media networks, wherein individuals are modeled as nodes, and their interactions—whether based on friendships, mutual interests, or affiliations—are represented as edges [11].

Despite the numerous advantages of social media platforms, they also present significant risks related to cybercrime. The exposure of personal information online can lead to various criminal activities, including harassment, threats, stalking, hacking, fraud, unauthorized transactions, dissemination of illicit content, and vacation thefts [10]. Victims often hesitate to report such incidents due to factors such as perceived insignificance, social stigma, or lack of awareness. To enhance traditional crime reporting mechanisms, social media monitoring can be leveraged as a supplementary tool for crime detection and prevention. As emerging digital communication platforms evolve, so do the methods employed by criminals to exploit these networks for illicit purposes. Therefore, it is imperative to systematically identify and analyze behavioral patterns and trends in criminal activities within social media networks, facilitating the development of robust cybersecurity measures and crime prevention strategies. [11].

Criminal Community Detection using Graph

The analysis of criminal networks has emerged as a significant subfield within social network analysis (SNA), offering valuable insights into the structural and behavioral patterns of illicit activities. Given the extensive range of attributes examined, criminal event data extracted from social media platforms is inherently high-dimensional. However, the application of Criminal Network Analysis (CNA) is well-suited for processing and structuring this data, facilitating a more systematic investigation [12].

Recent studies indicate that SNA plays a pivotal role in uncovering hidden or covert networks, commonly referred to as dark networks. More importantly, it enables the identification of key nodes within criminal networks, allowing security and law enforcement agencies to strategically target and disrupt these networks. By leveraging advanced analytical techniques, CNA enhances the effectiveness of crime prevention and intervention strategies, contributing to improved cybersecurity and law enforcement operations [13].

The four major characteristics of the criminal networks are [14]:

- Size of the criminal network database
- Incompleteness of the data
- Fuzzy boundaries of the network

- Dynamic nature of the network

Community detection in bipartite graphs presents greater challenges compared to traditional graph structures due to their inherent constraints. Unlike standard graphs, bipartite networks consist of two distinct sets of vertices, requiring comprehensive consideration of all vertices during analysis. Community detection in such networks is often achieved by optimizing modularity, which is based on the probability of an edge existing between two vertices and the structural properties of their connections [15]. Furthermore, graphs provide detailed characteristics for each node, facilitating node identification. However, in large-scale social media networks, where nodes exhibit diverse attributes and interactions, identifying specific nodes becomes increasingly complex. Given the vastness and dynamic nature of social media networks, a single approach may not be sufficient for effective node identification. Therefore, employing multiple analytical strategies is essential to enhance the accuracy and efficiency of node detection within these networks [11].

Analytical Hierarchy Process

The Analytical Hierarchy Process (AHP), developed by Thomas Saaty, is a structured decision-making methodology designed to analyze and prioritize complex problems involving multiple criteria. AHP organizes the decision problem into a hierarchical framework, beginning with the overall goal at the top level, followed by criteria, sub-criteria, and ultimately, the alternatives at the lowest level [15]. Decision-makers conduct pairwise comparisons at each hierarchical level, assigning numerical values to represent the relative importance of elements. These comparisons generate a priority scale, which is synthesized using mathematical techniques to rank alternatives systematically. By integrating subjective judgments with quantitative data, AHP provides a logical and consistent approach to decision-making, making it a valuable tool for resource allocation, project selection, and strategic planning in various domains [16].

LITERATURE REVIEW

Social Network Vs. Cyber Culture

The evolution of the web has significantly transformed modern society, leading to the widespread adoption of network-based interactions. The concept of community has been extensively studied across various sociological perspectives, each offering distinct definitions and interpretations. In the context of online communities, a novel form of social interaction and engagement has emerged, reshaping traditional modes of communication and collective behaviour in the digital era [17].

Extensive research has been conducted on cyber-cultural theories, particularly concerning identity formation within online communities. An individual's intentions are reflective of their behaviour, perceptions, cognitive processes, and activities, all of which contribute to the development of cyber culture. Consequently, a community is formed by individuals who share common cyber-cultural attributes, reinforcing the interconnected nature of digital societies [17].

Net War and Information Technology

The term "Net War" refers to the strategic exploitation of information technology as a consequence of the information revolution. Terrorist organizations, particularly in the Middle East, have increasingly adopted network-centric approaches to execute destabilizing cyber-attacks. These groups leverage information technology to conduct various forms of cyber warfare, including website defacement through spam attacks and the deployment of electronic bombs (e-bombs) to disrupt computer systems [5].

Raising awareness about such cyber threats is crucial in mitigating potential risks and preventing individuals from becoming victims. To effectively detect and counteract suspicious online activities, the implementation of robust and adaptive cybersecurity models is essential. Developing advanced frameworks for threat identification and response will enhance digital security and contribute to counterterrorism efforts in the cyber domain [5].

Social Informatics or Technological Determinism

The importance of social media for young individuals has grown significantly, as it has become a primary tool for making connections, communicating, and acquiring knowledge. However, this rise in social media usage raises critical concerns regarding its impact on adolescent development, particularly in relation to cyberbullying and social

interactions. One key issue is whether excessive use of social media exposes teenagers to higher risks of cyberbullying or whether it facilitates their social development and relationship building. Another important question is whether time spent on social media detracts from students' academic performance and overall success in school. To better understand these phenomena, the concept of "Social Informatics" is more applicable than "technological determinism," as it emphasizes the role of cultural norms, behavioral patterns, and social pressures in shaping technology use. Additionally, "Warranting Theory" posits that individuals form perceptions of others based on their online profiles, which are shaped by how they present themselves and the people they interact with on social media platforms [13].

Sentimental Analysis of Social Media Network

With the rapid expansion of online infrastructure, sentiment analysis has become an essential tool across various domains, including cyber-vulnerability assessments, tracking harmful movements through online diaries, optimizing targeted websites, and investigating the activities of cyber-criminals within informal networks. In these contexts, the strategies and choices employed to capture the attention and resonate with the sentiments and worldviews of others are frequently adapted to align with current trends. Consequently, to make informed decisions, conduct thorough research, and assess the work of others, the traditional approach of critically reviewing and analyzing information remains a fundamental practice [18].

Data Mining for Fraud Detection

Data mining technologies can be effectively applied to fraud detection through various methods, including the development of models for scam detection, illustrating the process of model construction, and initiating the data modeling process with appropriate classifiers. The proliferation of internet-based scams presents a significant opportunity for fraudsters, particularly with the rapid growth of online shopping platforms, making them an increasingly attractive target for fraudulent activities [19].

Social Media Network to Graph Techniques

To construct a graph representing a social media network, users are represented as nodes, while their interactions or relationships are depicted as edges. These edges may carry additional attributes, such as weight or direction, to further characterize the nature of the connections. Several techniques and tools are available to effectively model and visualize these networks. Notable methods include the Cluster Walktrap, Modified Cluster Walktrap, Louvain, and Girvan-Newman algorithms, among others. These approaches offer different strategies for community detection and the identification of significant structural patterns within social media graphs [12].

Identification of Node

Graph construction algorithms capture various node characteristics, such as degree, betweenness, mean distance, the number of triangles formed by edges, k-core number, eccentricity, and others. A node with the highest degree, for example, may be identified as a prominent node, while a node forming the maximum number of triangles may similarly be regarded as significant. However, identifying nodes based on a single parameter limits the assessment to the value of that particular attribute alone [14]. A more robust approach would involve utilizing multiple parameters simultaneously to determine the most prominent nodes. Techniques such as Analytical Hierarchy Process (AHP), Weighted Scoring Method, Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), Decision Tree, and Elimination and Choice Translating Reality (ELECTRE) offer more comprehensive methods for this multi-criteria decision-making process [20].

PROPOSED MODEL FOR COMMUNITY DETECTION

The proposed model, titled "Finding the Most Prominent Node in Social Media Networks for Cyber Crime Detection Using Modified Cluster Walktrap and Analytical Hierarchy Process," aims to identify key nodes within a social media network that are most likely associated with cybercrime activities. The model processes a bipartite graph representation of the social media network as input and, through its application, successfully identifies both the criminal community and the most prominent node. For empirical evaluation, the KONECT Facebook dataset, a publicly available social media dataset, is utilized [21]. The proposed model operates in two distinct phases, which are outlined as follows:

Phase 1: Criminal Community Identification

In the first phase of the proposed model, criminal communities within the social media network are identified using the Modified Cluster Walktrap method. This algorithm facilitates the detection of densely connected subgraphs, which are likely to represent communities involved in cybercrime activities.

Phase 2: Identification of Most Prominent Node

In the second phase, the most prominent node within the identified criminal community is detected using a multiparametric decision-making model, specifically the Analytical Hierarchy Process (AHP). The parameters considered for this evaluation include the node's degree, betweenness centrality, and mean distance within the network. These metrics provide a comprehensive assessment of each node's significance and potential involvement in cybercrime activities.

Process Flow

Figure 1 illustrates the process flow of the proposed model, highlighting the sequential steps involved in community identification and prominent node detection.

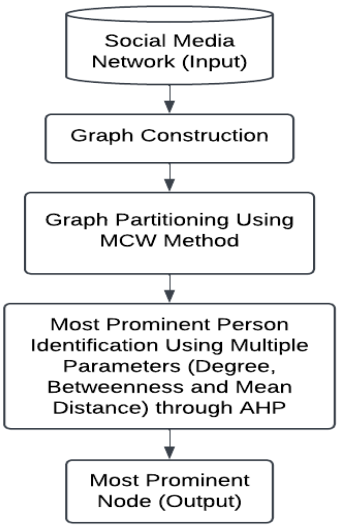

Figure 1: Process flow of proposed model

Phase 1: Criminal Community Grouping Using Modified Cluster Walktrap:

The structural similarity of vertices and communities in a two-mode network is evaluated using the Modified Cluster Walktrap method. This technique employs random walks to capture the areas of the network with the highest density. The process is repeated iteratively, merging communities at each phase based on the minimum distance, until maximum modularity is achieved. Partitioning the graph at each step facilitates the calculation of node membership within the identified communities [22].

Modularity Calculation

To compute the modularity of the network, the membership values obtained from the community partitioning process are utilized. The methodology can be adapted for use in two-mode networks by modifying the standard Walktrap algorithm accordingly. In the Modified Cluster Walktrap method, the probability distance value serves as a metric to quantify the similarity between communities and vertices, enhancing the accuracy of community detection and structural analysis within the network [23].

Input:

bg –Bipartite graph

Output:

C - Clusters formed

Method:

1. *procedure commDetec(bg){*
2. *for each vertex in bg {*
3. *if(i ≠ 1) then*
4. *Partition into community (C_i)*
5. *Else*
6. *Stop partition*
7. *for each vertex in bg{*
8. $PM_i = \frac{n}{c}$
9. *}*
10. *if($PM_i < PM_{i-1}$) then {*
11. $dist_i = \frac{n(n-1)}{2}$
12. $PD_i = \frac{dist_i}{\sum_{i=1}^{n} dist_{i_i}}$
13. *}*
14. *for each k {*
15. *if($PD_i < r$) then {*
16. $PT_k = \{C_1, C_2\}$
17. $C_3 = C_1 \cup C_2$
18. $PT_{k+1} = C_3$
19. *}}*
20. *for each vertex in PT_k{*
21. $memb_i = \frac{n}{c}$
22. *}*
23. $pm_{ij} = \frac{m_i m_j}{\sum_{i,j=1}^{n} m_i m_j}$
24. $PM = \frac{1}{2n} \sum_{i,j=1}^{n} \left(IM_{ij} - \frac{Pm_{ij}}{2n} \right) \delta(C_i, C_j)$
25. *}*

The Modified Cluster Walktrap (CWT) method begins with a bipartite graph as the input. The algorithm initially partitions the graph into *n* communities, each of which is reduced to a single vertex, denoted as P1={{v},v∈V}P_1 = \{ \{v\}, v \in V \}P1={{v},v∈V}. Following this, the distance between all adjacent vertices, denoted as disti\text{dist}_idisti, is computed [23]. A probability-based distance, labeled as PDiPD_iPDi, is then calculated for all vertices. The algorithm identifies communities and merges them based on the measured distance PDiPD_iPDi, updating the distance values in accordance with a predefined distance limit Γ\GammaΓ. Additionally, metrics such as membership values (membi\text{memb}_imembi), which denote the division of nodes into communities, and probability-based modularity (PM) are computed [23, 24].

The Modified Cluster Walktrap method produces communities with similar characteristics. However, identifying the most prominent node within these communities is a challenging task. This task is simplified through the second phase of our proposed model, which aids in the detection of the most significant node within the identified criminal community.

Phase 2: Finding Most Prominent Node Using Analytical Hierarchy Process

The Analytical Hierarchy Process (AHP) is a structured and systematic methodology for addressing complex decision-making problems, integrating principles from psychology and mathematics. AHP provides a comprehensive

framework for organizing decision problems, quantifying and visualizing their components, aligning these components with broader objectives, and evaluating potential solutions. This approach is widely applied across various sectors, including government, business, industry, healthcare, and education. AHP aids in establishing priorities among different alternatives and evaluates them according to predefined criteria.

The process begins by determining the relative importance of each criterion to achieve the overall goal. Subsequently, priorities are assigned based on how well the alternatives perform on each individual criterion. These priorities are derived through pairwise comparisons, utilizing judgments or, when available, ratio-based measurements from a scale [20].

Application of AHP in Identifying the Most Prominent Node

In the context of the proposed model, Phase 1 identifies communities containing several nodes, from which the most preferred or prominent node needs to be determined. The AHP method is employed to select this node by considering multiple parameters. The parameters used in the decision-making process include the degree, betweenness centrality, and mean distance of the nodes. These parameters, along with their respective preferences, are used in the AHP framework to make a final, informed decision on the most significant node within the community.

AHP processing completes in four steps mentioned below:

1. Develop pairwise weight for parameters
2. Develop the individual rating of node for each parameter
3. Calculation of average weighted rating for each node
4. Selection the node with maximum weighted as most prominent

IMPLEMENTATION

Implementation of CCD-MCW+AHP on Konect Facebook Network:

Phase 1: Criminal Community Grouping using Modified Cluster Walktrap

Konect Facebook Network

The Konect Facebook Network is a publicly available dataset that represents a social network extracted from Facebook, a popular social media platform. This dataset consists of nodes, which represent individuals, and edges that denote the friendship relationships between these individuals [21].

Bipartite Graph Representation

In the proposed technique, the dataset is represented as a bipartite graph, BG={P,C,R}BG = \{P, C, R\}BG={P,C,R}, where PPP denotes the set of people, CCC represents the set of crimes, and RRR indicates the relationships between the two sets, people and crimes [23].

Community Detection

The first step in the proposed approach involves identifying the communities present within the graph. To achieve this, the Modified Cluster Walktrap method is applied to the constructed bipartite graph. This method processes the graph and produces a clustering set as its output, where each cluster represents a group of individuals connected by a particular intention or activity, such as criminal involvement.

Dataset Origins

The dataset is grounded in police records from St. Louis, which document criminal incidents. These police reports were analyzed by Norm White and Rick Rosenfeld, who subsequently entered their findings into a person-to-crime event matrix. The graph constructed from the Konect Facebook dataset is depicted in Figure 2.

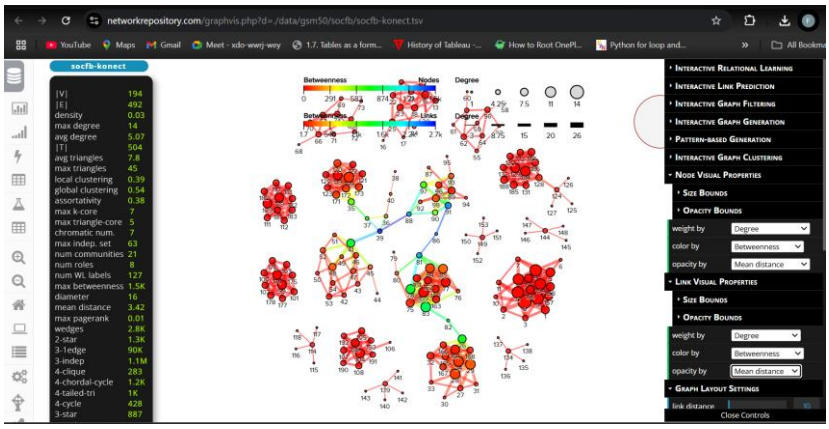

Figure 2: Graph Construction from Konect Facebook Dataset

The graph corresponding to the Konect Facebook dataset is generated using the online tool available at NetworkRepository.com [21]. In this visualization, the size of each node is proportional to its degree, reflecting the number of connections it has with other nodes. The color of the nodes varies based on the betweenness centrality value of each node, with a different color representing varying levels of centrality. The opacity of each node is determined by its mean distance, providing additional insight into the node's position within the network.

Phase 2 of the proposed model is applied to each community identified based on similar intentions. The three key parameters—degree, betweenness centrality, and mean distance—are calculated for each node within the community. Figure 3 illustrates the details of one such node, with Node ID 159 highlighted, showcasing its corresponding values for these parameters.

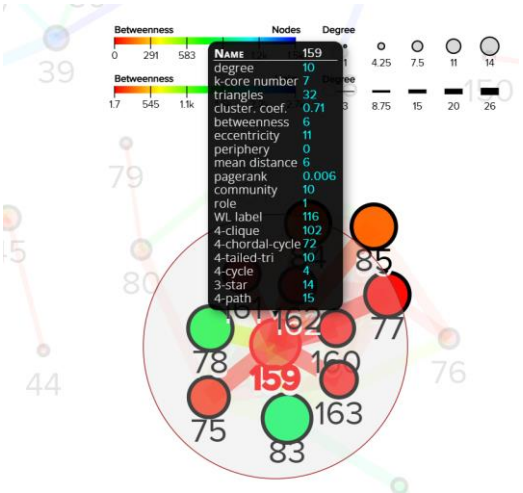

Figure 3: Details of Node with id 159 shows values of parameters (Degree, Betweenness and Mean Distance)

Value of all three parameters from graphs are captured in table 1, shown below:

Parameter (Row)/ Node ID (Column)	Degree	Betweenness	Mean Distance
159	10	6	6
77	9	5	5
78	9	8	6
83	10	11	7
85	12	6	5

Table 1: Value of parameters (Degree, Betweenness and Mean Distance) for all majorly connected nodes with node id 159

Above table is passed to phase 2 of proposed model in which the most prominent node is selected using AHP method.

Phase 2: Finding Most Prominent Node Using Analytic Hierarchy Process

The Analytical Hierarchy Process (AHP) consists of three distinct steps, as illustrated in Figure 4. In the context of decision-making, we apply the AHP method to identify the most influential individual within a given community.

Step 1: The first step of AHP involves assigning weights to the criteria. These weights represent the relative importance of each parameter in the decision-making process.
Step 2: In the second step, weights are assigned to the alternatives based on their performance or relevance to the predefined criteria.
Step 3: The final step calculates the overall weightage of each alternative, considering its performance across all criteria. The alternative with the highest overall weightage is identified as the most influential node.
The AHP process is applied to the data generated in Phase 1, as presented in Table 1. The overall procedure and flow of the AHP method are summarized in Figure 4.

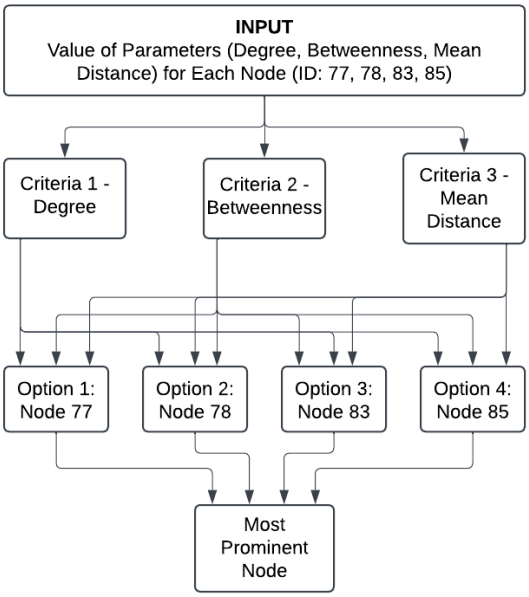

Figure 4: Working of Phase 2 (AHP on Parameters Degree, Betweenness, Mean Distance and Options Node with id 77, 78, 83, 85)

Working of AHP

1. Develop weight for parameter:

According to AHP, pair-wise comparison of parameters (degree, betweenness and mean distance) can be finalized with assigning values between 0 to 9. Higher the weight of a parameter in comparison with other parameter shows higher preference than other and vice versa. Pair-wise value 1 shows equal preference between two parameters.

Weight for parameter can be assigned as per the environment and preferable situation. Pairwise weight for parameters is shown in below table 2.

Parameters	Degree	Betweenness	Mean Distance
Degree	1.00	7.00	5.00
Betweenness	3.00	1.00	3.00
Mean Distance	5.00	8.00	1.00

Table 2: Pairwise weight for parameters

After getting pairwise comparison of parameters, priority vector is calculated as per the process defined below:

a. Calculate third root of multiplication

b. Priority Vector = Third root of multiplication/ Sum of third root of multiplication

c. Column-wise sum is also calculated.

Table 3 shows the calculation of priority vector after pairwise comparison of parameters.

	Degree	Betweenness	Mean Distance	3rd root of multiplication	Priority Vector
Degree	1.00	7.00	5.00	3.27	0.37
Betweenness	3.00	1.00	3.00	2.08	0.24

Mean Distance	5.00	8.00	1.00	3.42	0.39
Sum	9.00	16.00	9.00	8.77	1.00

Table 3: Priority vector calculation

2. Develop the rating for each node for each parameter.

According to step two of AHP we had calculated the priority vector for each node. Rating of each node according to Degree, Betweenness and Mean Distance are show in table number 4, 5 and 6 respectively.

Rating of each node for Degree Parameter

Node ID	77	78	83	85	3rd root of multiplication	Priority Vector
77	1.00	1.00	3.00	2.00	1..82	0.11
78	1.00	1.00	3.00	2.00	1.82	0.11
83	5.00	5.00	1.00	3.00	4.22	0.27
85	9.00	9.00	7.00	1.00	8.28	0.51
	14.00	20.00	14.00	12.00	16.14	1.00

Table 4: Priority vector of each node for degree parameter

Rating of each node for Betweenness Parameter

Node ID	77	78	83	85	3rd root of multiplication	Priority Vector
77	1.00	3.00	2.00	3.00	2.29	0.12
78	7.00	1.00	3.00	5.00	4.77	0.26
83	9.00	7.00	1.00	8.00	7.99	0.43
85	7.00	3.00	2.00	1.00	3.47	0.19
	12.00	24.00	9.00	13.00	18.52	1.00

Table 5: Priority vector of each node for Betweenness parameter

Rating of each node for Mean Distance Parameter

Node ID	77	78	83	85	3rd root of multiplication	Priority Vector
77	1.00	3.00	2.00	1.00	1.82	0.12
78	7.00	1.00	3.00	7.00	5.28	0.34
83	9.00	3.00	1.00	9.00	6.24	0.42
85	1.00	3.00	2.00	1.00	1.82	0.12
	18.00	10.00	8.00	18.00	15.16	1.00

Table 6: Priority vector of each node for Mean distance parameter

3. Calculation of the average weighted rating for each node, choose the node with maximum score:

In the last step of AHP we calculate the score for each node according to each parameter by below formula.

Score = ∑ (Criteria Weight * Option Weight)

Table 7 shows final score calculation of each node for each parameter

Criteria	Degree	Betweenness	Mean Distance	Score
Options	0.37	0.24	0.39	1.00
77	0.11	0.12	0.12	0.1163
78	0.11	0.26	0.34	0.2357
83	0.27	0.43	0.42	0.3669
85	0.51	0.19	0.12	0.2811
SUM	1.00	1.00	1.00	1.0000

Table 7: Final score calculation of each node for each parameter.

RESULT

Table 7 demonstrates that the node with ID 83 is identified as the most prominent node under the given conditions, based on the selected parameters and their associated preferred values. It is important to note that variations in the

parameters and their preferences will yield different results. When considering only a single parameter at a time, the resulting identification may overlook the impact of other parameters, which can affect the accuracy of the findings. By incorporating multiple parameters simultaneously and applying the Analytical Hierarchy Process (AHP), a more comprehensive and accurate determination of the most prominent node is achieved.

CONCLUSION

Social media data is represented as a graph consisting of vertices and edges, where nodes represent individuals and edges represent interactions or relationships. This model focuses on three key properties of the graph: the degree of the node, the betweenness centrality between pairs of nodes, and the mean distance between any two nodes. These properties serve as the foundation for the application of the Analytical Hierarchy Process (AHP).

The proposed model, CCD-MCW+AHP, identifies the most prominent node within a social media network based on the given environmental conditions. The primary strength of this model lies in its ability to prioritize one parameter over another when determining the most prominent node. This prioritization means that the process of identifying the most prominent node is entirely dependent on the specified preferences and priorities for each parameter.

The parameters influencing the graph or the selection of the most prominent node may vary depending on the specific context or environment in which the model is applied. In the scenario discussed, when focusing on a single parameter at a time, the identified most prominent node differs. However, when considering the preferences of each parameter, Node 83 emerges as the most prominent, highlighting the significance of parameter prioritization in the model's decision-making process.

FURUTE WORK

The current model identifies a single most prominent node in each run. However, an additional phase can be incorporated to enhance the model's functionality. This new phase would control the iterations of Phases 1 and 2, providing the most prominent node in each iteration, which can then be appended to a list of prominent nodes.

In Phase 3, a selection approach—either the same as used in earlier phases or an alternative method—can be applied to the list of prominent nodes. This phase would determine the single most prominent node from the list, thereby providing a more refined and final selection based on the results from multiple iterations.

REFRENCES

[1] E. P. Agara, F. E. Ojong, J. O. Emeka, A. M. O. Agba, A. I. Akintola, O. V. Ogunsola, "Social Media Platforms: Exposing students to cybercrime", in ARRUS journal of Scoial Sceinces and Humanities, Vol. 1, No. 1 (2021), doi: 10.35877/soshum490

[2] Z. K. Abdalrdha, A. M. Al-Barry, A. K. Farhan, "A Survey on Cybercrime Using Social Media", in Iraqi Journal for Computers and Informatics, Vol.[49], issue [1], Year(2023).

[3] Lama Almadhoor, Faiz Alserhani, Mamoona Humayun, "Social Media and Cybercrimes", in Turkish Journal of Computer and Mathematics Education, vol. 12 No. 10 (2021), 2972-2981

[4] M. C. Benard, M. Charles, J. S. Charo, M. Mvurya, "Cyber-Crimes Issues on Social Media Usage Amanong Higher Learning Institutions Students in Dar ES Salaam Region, Tanzania", in International Journal of Scientific Research in Sceince, Engineering and Technology (2021), ISSN: 2394-4099, doi:10.32628/IJSRSET218418.

[5] Ritesh Dwivedi, "Proliferation of cyber Crime via Social Media", in international journal of Novel Research and development, Vol. 09, Issue April 2024, ISSN: 2456-4184.

[6] Swati Sharma, Vikash K. Sharma, "Cyber Crime Analysis on Social Media", in BSSS Journal of Computer (2023), Vol. XI, Issue – I, doi: 10.51767/jc1104.

[7] A. Chakraborty, T. Dutta, A. Nath, "Application of Graph Theory in Social Media", in International Journal of Computer Sciences and Engineering (2018), Vol. 6, Issue-10, ISSN: 2347-2693.

[8] A. Majeed, I. Rauf, "Graph Theory: A Comprehensive Survey about Graph Theory Applications iin Computer Science and Social Networks (2020)", in international journal Inventions 2020 (MDPI), doi:10.2290/inventions5010010.

[9] M. E. J. Newman, D. J. Watts, S. H. Strogatz, “Random graph models of social networks (2002)”, Colloquium, Vol. 99, Suppl.1, doi:10.1073, pp-2566-2572.

[10] M. Pachayappan, R. Venkatesakumar, “A Graph Theory Based Systematic Literature Network Analysis”, in Theoretical Economics letters, 2018, 8, 960-980, ISSN: 2162-2086.

[11] Fei Hu, Z. Li, C. Yang, Y. Jiang, “A graph-based approach to detecting tourist movement patters using social media data (2019)”, in International Journal of Cartography and Geographic Information Science, Vol. 46, Issue-4, doi: 10.1080/15230406.2018.1496036.

[12] O. Elezaj, S. Y. Yayilgan, E. Kalemi, “Criminal Network Community detection in Social Media”, in Intelligent Technologies and Applications 2020, doi:10.1007/978-3-030-71711-7_31.

[13] M. Ahmed, N. E. Sharif, I. Abuiram, “Risk online behaviors and cybercrime awareness among undergraduate students at AI Quds University: a cross sectional study”, in International Journal Crime Science (2024) , doi: 10.1186/s40163-024-00230-w.

[14] Elezaj, O., Yayilgan, S.Y., Kalemi, E., Wendelberg, L., Abomhara, M., Ahmed, J. (2020), “Towards Designing a Knowledge Graph-Based Framework for Investigating and Preventing Crime on Online Social Networks” In: Katsikas, S., Zorkadis, V. (eds) E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age. e-Democracy 2019. Communications in Computer and Information Science, vol 1111. Springer, Cham. https://doi.org/10.1007/978-3-030-37545-4_12

[15] O. S. Vaida, S. kumar, “Invited Review Analytical Hierarchy Process: An overview of applications”, in European Journal of Operational Research, Vol-169, Issue 1, pages 1-29, doi:10.1016.

[16] C. Ozgur, “The analytical hierarchy process method to design applicable decision making for the effective removal of 2-MIB and geosmin in water”, in International journal of Environmental Science and pollution research (2024) 31:12431-12445, doi: 10.1007/s11356-024-31848-7.

[17] B. Jain, R. Jain, “Cyber Law’s Appropriation of Social Media and Difficulties with its Enforcement in India”, in International Journal of Emerging Technologies and Innovation Research (2024), Vol. 10, Issue 2, ISSN – 2349-5162.

[18] Rawat, Romil & Mahor, Vinod & Chirgaiya, Sachin & Shaw, Rabindra & Ghosh, Ankush. (2021). Sentiment Analysis at Online Social Network for Cyber-Malicious Post Reviews Using Machine Learning Techniques. 10.1007/978-981-16-0407-2_9.

[19] D. F. Nettleton, “Data Mining of Social Networks represented as graphs”, in Computer Science Review, Vol. 7, Pages 1-34, doi:10.1016/j.cosrev.2012.

[20] Amandeep, F. Mohammad and V. Yadav, "Automatic decision making for multi-criteria load balancing in cloud environment using AHP," *International Conference on Computing, Communication & Automation*, Greater Noida, India, 2015, pp. 569-576, doi: 10.1109/CCAA.2015.7148473.

[21] The Network Data Repository with Interactive Graph Analytics and Visualization, Ryan A. Rossi and Nesreen K. Ahmed, booktitle=AAAI, *https://networkrepository.com*, year=2015

[22] M. Brusco, D. Steinley, A. L. Watts, “Improving the Walktrap Algorithm Using K-Means Clustering”, in Multivariate Behavioral Research 2024, Vol 59, Issue-2, doi:10.1080/00273171.2023.2254767.

[23] G. Pugalendhi, S. Kumaresan, “Customized CWT-CCA: Discovery of Prominent Persons in the Crime Network,” in international journal of applied mathematics and information sciences, 13, no.4, 665-678 (2019).

[24] F. Hu, Y. Zhu, Y. Shi, J. Cai, L. Chen, S. Shen, “An algorithm walktrap-SPM for detecting overlapping community structure”, in international journal of moder physics, vol 31, no. 15, 1750121.