12 Methods of Complex Network Analysis to Screen for Cyberbullying

Santhosh Kumar Rajamani
MAEER MIT Pune's MIMER Medical College and DR. BSTR Hospital

Radha Srinivasan Iyer
SEC Centre for Independent Living

12.1 INTRODUCTION

12.1.1 Definition of Cyberbullying

Cyberbullying is defined as using electronic forms of communication to bully someone. Examples include sending unwanted messages, spreading rumors online, hacking into someone's social media accounts, impersonating another person online, and posting embarrassing photos or videos without permission (Wright & Wachs, 2023). Cyberbullying Research Centre redefines the act of cyberbullying as "wilful and repeated harm that is inflicted through the use of computers, cell phones, and other electronic devices" (Hinduja & Patchin, 2014).

The definition of cyberbullying as stated by American National Crime Prevention Council is as follows: "online bullying, often known as cyberbullying, occurs when someone utilises the Internet, a mobile phone, or any other device to email or upload text or images meant to harm or humiliate another person" (Zhu et al., 2021).

Cyberbullying is the deliberate use of some form of technology to annoy, threaten, or hurt other people. The following are some of the prevalent examples of the menace of cyberbullying, sending threatening or hurtful messages, disseminating untrue information, sharing humiliating or private images or videos without the individual's permission, or removing someone from online social networks without the consent of the user (Zhao & Yu, 2021).

12.1.2 Current Cyberbullying Statistics

The reported incidence of cyberbullying from various studies latest up to 2023 ranges from 6.3% to 32% of adolescent internet users. About 10%–20% adolescent users report bullying someone online (Zhao & Yu, 2021). To better understand the experiences and opinions of 1,316 U.S. teenagers, Pew Research Center conducted

DOI: 10.1201/9781003393061-16

a survey in 2022. The results showed that name-calling (32% of the time) was the most common cyberbullying behavior experienced by 46% of teenagers ages 13–17 (Vogels & Atske, 2022).

Unlike traditional bullying that can be found in school premises, cyberbullying can become a 24×7 harrowing experience for the victim, with the victim being bullied in the security of homes, through several electronic devices, like cell phones (web forums, groups, chats, messages) desktops, and laptops. The anonymity offered by the social media with peer approval encourages the more aggressive behavior of the bully (Camacho et al., 2023).

12.2 PATHOLOGY OF CYBERBULLYING

People who are the victims of cyberbullying may have depressive disorders, anxiety, low self-esteem, and even suicidal thoughts (Tozzo et al., 2022).

12.2.1 Pathology of Cyberbullying

Cyberbullying can have a variety of effects, from mild distress to serious psychological and social issues like poor academic performance, an increase in absences from school, a sense of danger at school, mood disruption (anxiety), and despair. This form of harassment can even have serious negative effects on an individual's mental health, self-esteem, and even their physical safety (Schodt et al. 2021). Victims may feel overwhelmed, anxious, and isolated because of these behaviors (Camacho et al., 2023). Cyberbullying in victims is linked to psychological depression and dysphoria, anxiety, loss of sleep, palpitations, poor academic performance, poor concentration in classroom, nightmares, loss of appetite or increased appetite, and suicidal tendency (Bitar et al., 2023). In addition, bullying victims have lower self-esteem, higher risk substance abuse, and cigarette or alcohol addiction. Boys are more likely to be victims than girls (Martínez-Valderrey et al., 2023).

Unchecked actions can, in certain severe cases, cause victims to suffer from serious mental illness or, even worse, to be killed. As a result, cyberbullying has drawn the attention of policymakers, educators, and parents (Shin & Choi, 2021).

12.2.2 Psychology of Cyberbullying

As cyberbullying is a learnt conscious habit, psychology learning theories were applied to the phenomenon of cyberbullying. This has led to Barlett Gentile Cyberbullying Model (BGCM) which is considered as the most acceptable cognitive model of cyberbullying (Barlett, 2023). Cyberbullying aggressive behaviors are reinforced by a loop of peer and family approval, with bystander and supporter appraisal. This is essentially a community-approved and acceptable aggressive behavior in certain communities. In many cases, the aggressive behaviors are trivialized and even normalized (Wright & Wachs, 2023).

Individuals suffering from autism or autistic spectrum disorder were significantly more likely to be victims of cyberbullying. Traditional bullying victims were more likely to become victims of cyberbullying (Sampasa-Kanyinga et al., 2018).

12.2.3 Krohn's Network Theory of Delinquent Behavior

Marvin Krohn in 1986 advanced the "network theory of delinquency," as an explanation for delinquent behaviors (Krohn, 1986). Social control theories propose that weak social bonds especially in family, friends, school, community, etc. (support networks) are responsible for evolving of innate tendencies or genetic predispositions toward delinquent behavior. A lack of social control is at the heart of the problem (Hirschi, 1969). Differential association theory postulates that criminal and delinquent attitudes are learnt from peer groups and not innate (Edwin Sutherland et al., 1992). Peer influences are mainly responsible for nefarious attitudes and behaviors (criminal networks). Krohn's network theory of delinquency is a composite theory with elements of both social control theory and differential association theory (Armitage 2021). There are two levels in this combination approach. At the individual level, social acceptance and social bonding are balanced by (both criminal and anticriminal) acceptable behaviors in his personal network. At the community level, the levels of delinquency will be affected by number of such social networks which support the individual (support networks) or encourage delinquent behaviors (criminal networks). For example, Krohn found that young men who had strong support network of family, church, and friends were less likely to take up the habit of smoking cigarettes (Krohn et al., 1988).

12.2.4 Spectrum of Online Behaviors That Constitute Cyberbullying

There are a variety of aggressive online behaviors that form the spectrum of cyberbullying like cyberstalking (stalking the victim online) excluding (removing a victim from a group against their wilk), doxing (revealing socially sensitive information about the victim like intimate photos, sexual orientation), fraping (maligning in the victim in a group, by posting negative content pretending to be the victim), masquerading (creating a false identity in a group using victims name or photographs), flaming (insulting the victim via comments and messages), ewhoring (pretending to be friendly females and sexually soliciting explicit/nude images from males or explicit chat conversations or explicit live video sessions, with main intend to blackmail and bully the male victim), and sexual harassment by sending explicit images to the victim (Aboujaoude & Savage, 2023; Floros and Mylona 2022).

12.3 COMMUNITY SUPPORT FOR PREVENTING CYBERBULLYING

Cyberbullying can have major repercussions for the kids who are subjected to it; it is crucial for instructors to adopt a proactive approach to preventing it. These are the mitigating steps that can be taken by parents, teachers, social media network administrators, and social media platform owners.

12.3.1 Role of Parents in Preventing Cyberbullying

A subfield of network cyberbullying can happen via a variety of online communication channels, including social networking, texting, and messaging applications

(Gabrielli et al. 2021). Parents must be vigilant about their ward's online behavior, particularly, their use of social media and messaging services. Parents must pay close attention to any modifications in their behavior, such as a tendency to withdrawn or get tense or signs of emotional disturbance.

Use monitoring software: There are many tools that can assist you in keeping an eye on your child's online activity and notifying you of any worrying conduct (Henares-Montiel et al. 2022).

Teach your child: Instill the value of online safety in your child and urge them to speak up if they encounter or see cyberbullying.

Use parental controls: Many gadgets and social media sites provide parental controls that let you limit your child's access to content or how much time they spend online.

Report cyberbullying: If you have reason to believe that your child is a victim of cyberbullying, you should inform the relevant parties, such as the school, the social media site, or police enforcement.

Cyberbullying can have serious social and psychological harm to the victims; it is vital for parents to take this seriously and to address cyberbullying as soon as possible (Alfakeh et al., 2021).

12.3.2 Role of Teachers in Preventing Cyberbullying

Teachers can take the following actions to stop cyberbullying.

Education of students: Students can be educated by teachers about the negative effects of cyberbullying and the value of showing kindness and respect online (Kim et al. 2021).

Encourage open communication: Teachers can promote open communication by establishing a secure, encouraging environment in the classroom where students feel at ease sharing their experiences and asking for assistance if they are being bullied. Teachers can keep an eye on their students' internet conduct and take appropriate action if they notice any worrying behavior.

Use of Software: Detect and prevent cyberbullying with the aid of monitoring software. Teachers can use monitoring software to do this.

Working with parents: To combat cyberbullying and promote online safety, teachers can collaborate with parents.

Report cyberbullying: Teachers should notify the proper authorities, such as the school administration or law enforcement, if they become aware of any cyberbullying involving students.

Teachers can make the internet environment safer and more encouraging for all students by putting these preventative strategies into practice (Ademiluyi et al., 2022).

12.3.3 Role of Social Media Network Administrators in Preventing Cyberbullying

Network administrators can take the following actions to stop cyberbullying on their social media networks or in their online communities.

Setup ground rule based on quality: Establish clear rules and guidelines that forbid cyberbullying and other forms of online harassment. Admins should implement these rules and guidelines. All community members should be made aware of these regulations in a straightforward manner.

Using AI-based moderation tools: Using moderating tools will help admins find and delete content that contains cyberbullying (Maheswaran & Rajamani, 2022). These tools include automated filters and human moderators.

Content promotion: Admins can promote content that encourages compassion and respect, and they can award users who uphold these principles. Admins can offer users who are experiencing cyberbullying resources and support, including reporting mechanisms and information on how to obtain help.

Liaison with other support groups: Admins can collaborate with outside groups to combat cyberbullying and advance online safety, such as schools and law enforcement.

Support and resources: Social media platforms can offer users who are experiencing cyberbullying tools for reporting incidents and information on how to receive assistance (Fazeen et al., 2011).

12.3.4 Role of Social Media Platforms in Preventing Cyberbullying

Social media platforms can make the online environment safer and more gratifying for all users by putting these prevention measures in place. Social media platforms can take the following actions to stop cyberbullying:

Adopt stringent community standards: Social media platforms should have explicit policies prohibiting cyberbullying and other types of online abuse.

Utilize moderating tools: To detect and delete information that promotes cyberbullying, social media platforms can make use of tools like automated filters and human moderators.

Encourage positive behavior: Social media platforms can promote content that encourages compassion and respect, as well as rewarding users that uphold these principles.

Collaboration: To combat cyberbullying and advance online safety, social media platforms can collaborate with outside entities like law enforcement and educational institutions.

Proactive attitude: Social media platforms and their admins must be proactive in combating cyberbullying since it can have major repercussions for those who are targeted (Huang et al., 2021).

12.4 GRAPH THEORY, COMPLEX NETWORK ANALYSIS, ARTIFICIAL INTELLIGENCE, AND MACHINE LEARNING

12.4.1 A Brief Background in Graph Theory and Complex Network Analysis

In graph theory, complex networks are represented as graphs where nodes represent entities (such as individuals, organizations, or cities) and edges represent connections

(such as friendships, business partnerships, or roads). By studying these graphs through techniques like centrality measures, clustering coefficients, and degree distributions, researchers can gain insights into how the system functions, who holds the most influence, and how resilient it may be under different conditions (Gongane et al., 2022; Rajamani & Iyer, 2022).

A graph is made up of a collection of nodes, also known as vertices, and a set of connecting links or edges or ties. The entities in the problem like webpages, cities, and molecules are represented by the vertices, and their connections are shown by the edges like HTML links in a web documents, roads between cities, and bonds between molecules. The discipline of mathematics that studies networks is called graph theory (Newman, 2010).

The difference between graph and network is that graph is an abstract mathematical object, existing on a paper or a computer, while network is the real-world analogy or application of a graph. Programmatically, a graph is represented by **G=(V, E)**, where V is the vertex set V = $\{v_1, v_2, v_3, v_4 \ldots\}$ and edge set E = $\{e_1, e_2, e_3, e_4, e_5 \ldots\}$. The number of edges connected to a node is called the degree of that node or vertex (Newman, 2010).

In many real-life networks like for example on social media, you can always find a group of people (groups) that are well connected to each other, like people who like gardening and follow specific gardening pages or posts or experts. They are referred to as clusters or communities. Networks can be visualized using several programming languages using libraries like Python, C++, and R language. There are many free software editors which can also be used by a nonprogrammer to visualize networks like yEd graph editor. Using computers, we can simulate complex or cybernetic networks and simulate dynamical processes on these networks. Visualization of a network helps in understanding the structure of a network and elucidating network connectivity and communities in an intuitive way. Analysis of complicated graphs or networks using a variety of algorithms and techniques is called complex network analysis. Optimization of paths and properties of vertices using algorithms is called graph optimization (Barabasi, 2002).

12.4.2 Introduction to Complex Network Analysis

A subfield of network science called complex network analysis studies the modeling and analysis of complicated networks. These networks frequently exhibit complex behavior and have a lot of nodes (also known as vertices) and edges (also known as connections) (Newman, 2003).

Understanding a network's basic structure and how it affects the behavior of its nodes is one of the key aims of complex network analysis. Analysts do this by spotting patterns and trends in the network using a variety of methods, including centrality metrics, network motifs, and community discovery algorithms (Butts, 2006).

Based on their connections to other nodes, centrality measurements are used to determine which nodes in a network are the most significant. For instance, because it has more links to other nodes in the network, a node with a high degree of centrality can be regarded as being more significant (Reda Alhajj & Jon Rokne, 2014).

Network motifs are connectivity patterns that show up more frequently than would be predicted by chance in a network. These patterns can disclose crucial details about the way the network works and how certain nodes interact with one another (Barabasi & Albert, 1999).

To find groups of nodes within a network that is more closely connected to one another than to the rest of the network, community discovery algorithms are utilized. These communities can be utilized to comprehend the overall structure and operation of the network (Lancichinetti & Fortunato, 2009).

In conclusion, complex network analysis is an effective method for comprehending the dynamics and behavior of complex systems and has applications in a variety of disciplines, such as biology, sociology, and computer science.

12.4.3 Artificial Intelligence to Mitigate Cyberbullying

One potential use for AI in combatting cyberbullying is by implementing monitoring systems that flag suspicious behavior such as frequent unsolicited messages or posts. These algorithms could be trained to detect patterns associated with bullying tactics like harsh language or repetitive contact attempts (Milosevic et al., 2022). Another approach would involve using machine learning models to identify specific users who engage in abusive behavior through analysis of large amounts of data from sources such as chat logs or social media interactions. Once potential cyberbullies have been identified, they could receive automated warnings or notifications reminding them of proper online conduct standards (Rajamani & Iyer, 2023a). Additionally, AI technologies could aid in providing emotional support for victims of cyberbullying via text-based therapy systems or virtual reality exposure therapies designed to desensitize individuals to fearful situations like encountering threatening messages or images online (Sánchez-Medina et al., 2020).

12.4.4 Machine Learning Algorithms to Mitigate Cyberbullying

Machine learning algorithms have been used in several approaches to identify and mitigate cyberbullying.

12.4.4.1 Content Analysis and Moderation

This approach involves analyzing text data from social media, online forums, chat rooms, emails, etc., using natural language processing (NLP) techniques and machine learning algorithms like topic modeling, sentiment analysis, and classification models (Rajamani and Iyer 2023b). These methods aim at identifying harmful content by detecting profanity, hate speech, racist, sexist, or discriminatory language among others (Martínez-Valderrey et al., 2023).

By using natural language processing and computer vision techniques, AIs can automatically detect and remove harmful content from platforms such as social media sites, forums, or chat apps, before human moderators review them. This speeds up the process, enabling quick removal of offensive posts or messages (Gongane et al., 2022).

12.4.4.2 Behavior Analysis

Another approach involves tracking users' behaviors, activities, and interactions across multiple online channels and sessions by building user profiles over time. By leveraging supervised learning techniques like decision trees, random forest classifiers, support vector machines (SVM), artificial neural networks (ANN), etc., researchers develop features, such as frequency of posting, number of followers/friends, type of messages sent/received, participation patterns in online communities, etc., serve as predictors for cyberbullying detection. Some works combine both content and behavior analyses to achieve better results (Rajamani & Iyer, 2023a).

12.4.4.3 Collaborative Filtering

Collaborative filtering-based systems analyze previous instances of identified cyberbullying cases; they recommend actions to other members of their community after comparing them against previous instances of cyberbullying hate text. Machine learning techniques can assist researchers and experts who develop interventions or educational materials aimed at reducing cyberbullying. These initiatives often involve identifying common risk factors, creating awareness campaigns, or training people in safer online practices.

12.4.4.4 Automatic Monitoring

With machine learning algorithms, platforms can track patterns of behavior among users. If someone frequently engages in harassing activities (e.g., sending abusive messages), they may receive a warning or have their account suspended.

12.4.4.5 Personalized Filtering

Some systems use machine learning models to analyze user preferences and behavior, filtering out unwanted or upsetting interactions. For example, Facebook allows individuals to hide certain keywords or topics they do not want to see in their news feed.

12.4.4.6 Sentiment Analysis

By analyzing the tone and context of messages or posts, machines can identify potentially hurtful language or behaviors before they cause harm. People responsible for these actions might then be approached by a counselor or offered resources to prevent future incidents (Milosevic et al., 2022).

Incorporating artificial intelligence into existing efforts against cyberbullying could make a positive impact. It is important to recognize potential risks associated with relying heavily on technology or automated decision-making processes (Neelakandan et al., 2022).

12.5 METHODOLOGY – GRAPH-OPTIMIZATION ALGORITHMS FOR ANOMALY DETECTION ON A NETWORK

For anomalous network activities, there are various kinds of graph-optimization techniques for detection as follows.

12.5.1 Shortest Path Algorithms

Algorithms that discover the shortest path between two nodes in a network are known as shortest path algorithms. Edgar Dijkstra's algorithm and A* search are two examples.

12.5.2 Minimum-Spanning Tree

The techniques known as minimum-spanning trees identify a subset of the edges in a graph such that all the vertices are connected, and the overall weight of the edges is kept to a minimum. Examples consist of the Kruskal and Prim algorithms.

12.5.3 Methods for Maximum Flow

These algorithms determine how much flow can be delivered from a source node to a sink node in a graph. Common examples are the Ford-Fulkerson algorithm and the Edmonds-Karp algorithm.

12.5.4 Network-Flow Algorithms

These methods locate a path through a network that satisfies a set of conditions, such as edge-capacity limitations. The simplex algorithm and the primal-dual algorithm are two such cases.

12.5.5 Algorithms for Finding Matches in Graphs

A matching in a graph is a subset of the edges where no two edges share an endpoint, namely: the Gale-Shapley algorithm and the Hungarian algorithm.

12.5.6 Classic "Traveling Salesman Problem" (TSP)

These methods identify the route that traverses every node in a network precisely once before retracing the steps to the origin. This paradigm determines the shortest path that stops at each node in the network, like a salesman who must tour all the customers but must use shortest possible path to save his time and gasoline/petrol. Two common examples are the nearest neighbor algorithm and the brute-force algorithm.

12.5.7 Algorithms for Finding Matches in Graphs

A matching in a graph is a subset of the edges where no two edges share an endpoint such as the Gale-Shapley algorithm and the Hungarian algorithm. There are other further graph-optimization strategies, including graph partitioning, graph coloring, and others.

There are several ways that complex network analysis can be utilized to find instances of cyberbullying in a network. The following are some detection paradigms using complex network analysis.

12.5.8 Community-Detection Algorithms

Since stalking act frequently involves a group of people cooperating, seeing communities inside a network can help spot possible nefarious activity. Communities inside a network can be found using algorithms like the Girvan-Newman algorithm and the Louvain approach. Girvan-Newman algorithm is the best-known method for this purpose which involves iteratively calculating the edge betweenness centrality of all the edges and then removes the edges with the highest value of centrality. This will increase the components and partition the graph (Lancichinetti & Fortunato, 2009).

12.5.9 Anomaly-Detection Algorithms

Cyberbullies frequently behave differently from other users in the network. Unusual network behavior that can point to fraudulent activities can be found using anomaly-detection techniques such as the isolation forest or the one-class support vector machine.

12.5.10 Link-Prediction Algorithms

Cyberbullies frequently use fictitious or deceptive links or names, inside a network to conceal their operations. You can utilize link-prediction algorithms to find connections in a network that might be cyberbullies, such as the Adamic-Adar index or the Jaccard coefficient.

12.5.11 Egocentricity or Centrality Measures of Nodes

A node's importance in a network is gauged by its degree centrality, which is dependent on the connections it has. High-degree centrality nodes are thought to be prominent or central nodes within the network. The most central nodes in a network can be found using centrality metrics such as degree centrality or betweenness centrality (Reda Alhajj & Jon Rokne, 2014).

It is worth noting that these are just a few examples of the ways in which network science algorithms can be used to detect nefarious activities. There are many other algorithms and approaches that can also be applied to this problem (Degenne & Forse, 1990).

12.6 PRACTICAL EXAMPLE OF DETECTING CYBERBULLYING USING NETWORK PARADIGM

Consider the scenario where we are social media network administrators, and we want to screen for personal accounts that may be involved in cyberbullying. First, we use community-detection algorithms to detect communities, which will essentially place the bullies and the victims in the same community. This happens because the stalker essentially tags or comments or harasses the victim and stays in close-network proximity to carry out nefarious activities. Second, we must determine degree centrality of accounts in the screened community, and we can then search for nodes with a particularly high-degree centrality.

12.6.1 Network Preprocessing

Preparation of network data for analysis if the first step is detecting cyberbullying using complex network analysis. Depending on the choice algorithm, we might need to clean up and prepare the data by deleting self-loops, eliminating nodes with low degree or less connectivity as they do not have much significance, or doing additional data preparation and cleaning (Rajamani & Iyer, 2022).

12.6.2 Community-Detection Algorithms

The principle of community-detection algorithms is to find nodes or groups of nodes, called communities, that do not fit in well with the rest of the network. This can be helpful for spotting cyberbullying, criminal activity, terrorists, hackers, fraudsters, cyberattacks, or other kinds of nefarious behavior within the network (Reda Alhajj & Jon Rokne, 2014).

Algorithms for community detection are used to locate communities or groupings within a network. They are frequently used to examine social networks, biological networks, and other networks in which the nodes stand in for people or other things and the edges signify the connections or relationships between them. Implementing the algorithm for community detection involves dividing the network into communities. Community-wise breaking-up the network can be done in a variety of ways, as follows.

12.6.2.1 Modularity-Maximization Algorithm

A graph-partitioning community-detection approach called modularity maximization can be used to bullying and stalking in a network. This is the process of finding the communities that maximize the percentage of intracommunity (links inside a given community) edges while minimizing the percentage of intercommunity edges (links between the communities). The network is split up into communities that increase the percentage of intracommunity edges while minimizing the percentage of intercommunity edges to achieve its desired results. Because nefarious networks frequently have a high degree of intercommunity connectivity and a low degree of intracommunity connectivity, this can be helpful for spotting such activities.

A graph's modularity can be increased using a variety of approaches. The Louvain algorithm, a heuristic algorithm that iteratively optimizes a graph's modularity score by shifting nodes between communities, is one popular technique. The Louvain algorithm begins with each node in its own community, combines communities iteratively based on the modularity score, and then starts over. The leading Eigenvector approach, the Infomap methodology, and the Map Equation are other examples of modularity maximization algorithms which can be used to detect communities.

It is crucial to remember that modularity maximization may not always work as a cyberbullying-detection strategy and can sometimes result in false positives or false negatives. As a result, it is crucial to verify any suspected fraudulent communities and to carefully consider the algorithm's limitations when interpreting the findings (Degenne & Forse, 1990).

12.6.2.2 An Example of Community-Detection Using Python 3.5's NetworkX Module

A method in the *NetworkX* package called "*nx.community. modularity_max. greedy_modularity_ communities(Graph)*" can be used to identify communities in a network that maximizes the modularity score. The modularity score is a measure of the density of connections within a community compared to the density of connections between communities. A high modularity score indicates that the communities in the graph are well-defined and distinct from each other. This function takes a graph as input and returns a list of sets, where each set represents a community in the graph. The function works by iteratively merging communities based on the modularity score, starting with each node in its own community. Imagine a community or network of crime depicted by Figure 12.1. You must import the *NetworkX* library and create a graph before you can use "*max.greedy_modularity_communities.*" The function can then be called with the graph as an argument (Hagberg et al., 2008) (Figure 12.2).

For instance, we could use this function to find communities in a graph using NetworkX.

The output of this program will be "*person: Suresh in community: a*," indicating that all the nodes or accounts "*suresh*" in the graph belong to the same community of bullies with our assigned label "*a*" (Hagberg et al., 2008).

You can also use the *community.label_propagation* function to find communities in a graph using label propagation. This function takes a graph as input and returns a dictionary, where the keys are the nodes in the graph and the values are the labels (communities) assigned to each node (Reda Alhajj & Jon Rokne, 2014).

This will output "*person: Rudra in community: b*" mapping each node or account ("*rudra*") to our label or community "*b*," indicating that all the nodes or accounts in the graph have been assigned to the same community (Reda Alhajj & Jon Rokne, 2014).

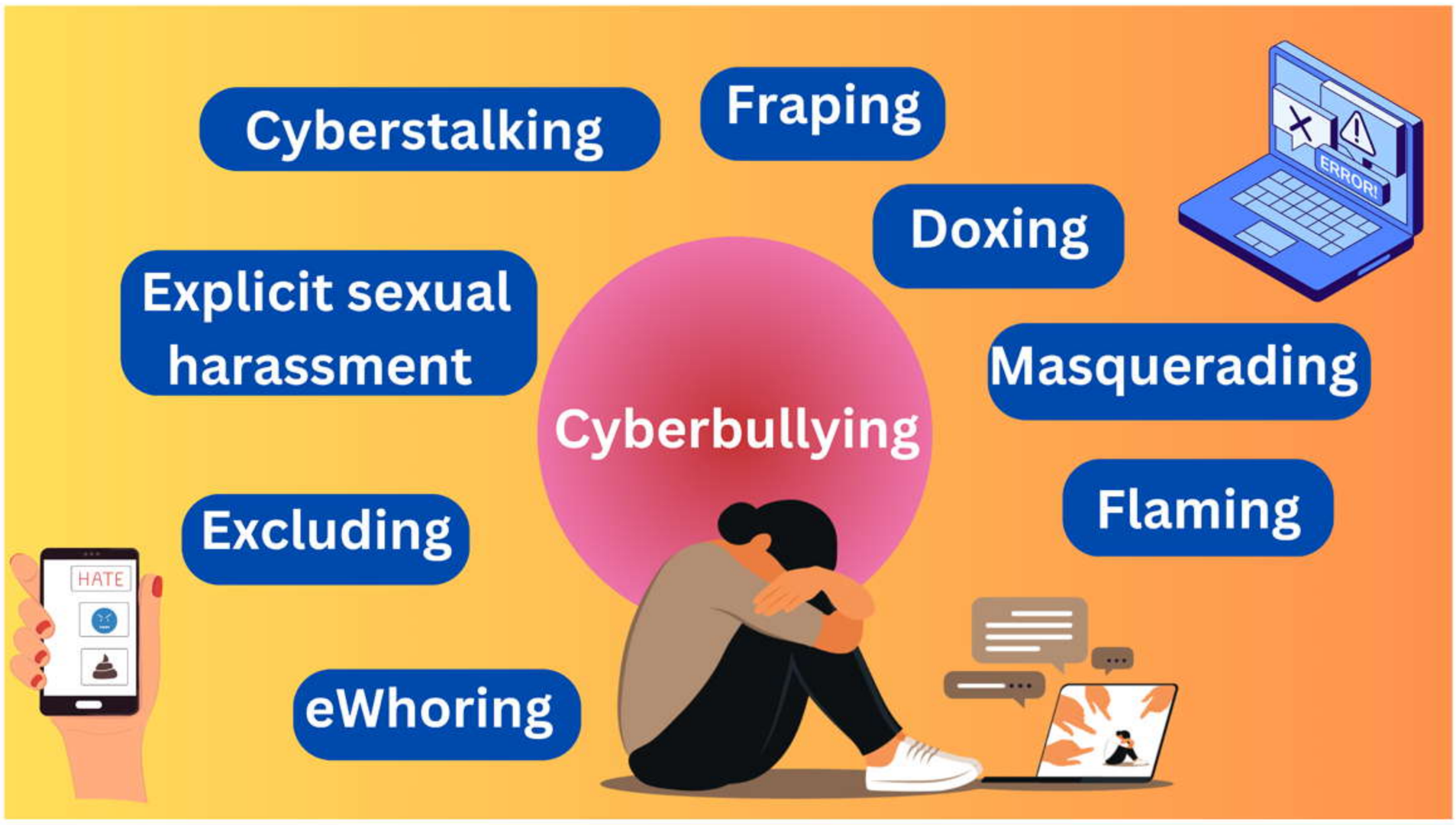

FIGURE 12.1 Spectrum of online behaviors that constitute cyberbullying and cause trauma to the victims; author's original illustration made using Canva Pro (Hinduja & Patchin, 2014; Aboujaoude & Savage, 2023).

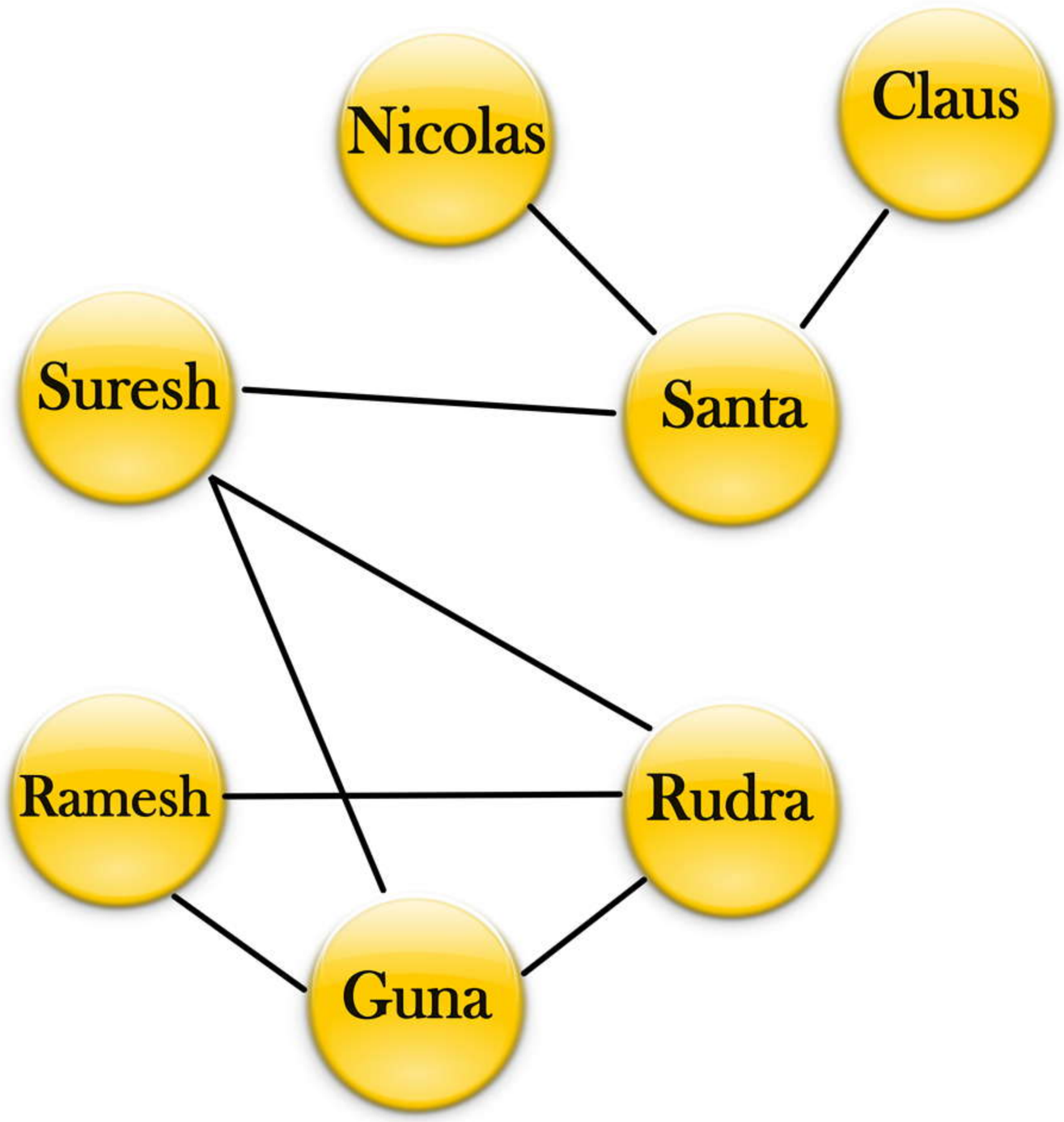

FIGURE 12.2 A simple example of seven individuals, who are segregated into two communities; we can create such a graph using NetworkX and delineate the communities using various complex analytical algorithms such as modularity maximization and label propagation. The working code for drawing this graph is also provided in the next section.

TABLE 12.1
Creating a Simple Network Graph Using NetworkX and Matplotlib Modules

```
#Install these modules in python 3.5 and above python -m pip install
#network, and python -m pip install matplotlib
#Import network, matplotlib modules
import networkx as nx
import matplotlib.pyplot as plt
# Create a graph
G = nx.Graph()
#Initilalize options for the graph plot
options = {'node_color': 'yellow','node_size':
 700,'alpha':0.9,'width': 1,
'edge_color':'red',}
# Add edges to the graph, create the community shown in figure 12.1
G.add_edges_from([('Santa', 'Claus'), ('Santa', 'Nicolas'), ('Suresh',
 'Santa'), ('Suresh', 'Guna'), ('Suresh', 'Rudra'), ('Ramesh',
 'Guna'), ('Ramesh', 'Rudra'),('Rudra', 'Guna'),])
nx.draw_circular(G, with_labels=True,**options) #font_weight='9')
```

TABLE 12.2
Simple Community Detection Using NetworkX Module greedy _modularity_ communities Function

```
import networkx as nx
# Create a graph
G = nx.Graph()
# Add edges to the graph, create the community shown in figure 12.1
# Add edges to the graph, create the community shown in figure 12.1
G.add_edges_from([('Santa', 'Claus'), ('Santa', 'Nicolas'), ('Suresh',
 'Santa'), ('Suresh', 'Guna'), ('Suresh', 'Rudra'), ('Ramesh',
 'Guna'), ('Ramesh', 'Rudra'),('Rudra', 'Guna'),])
nx.draw_circular(G, with_labels=True,**options) #font_weight='9')
# the number of edges incident to Santa is 3 Claus, Nicolas, Suresh
print(G.degree['Santa'])
# Find communities in the graph using the greedy modularity
 maximization algorithm
communities = nx.community.modularity_max.
 greedy_modularity_communities(G)
#Chr value of lower case "a" which is our assigned label for first
 community.
#This can be any label, but this code does automatic assignment.
#So next label is community is "b" then "c","d","e","f".. so on for
 any size
i=97
for persons in communities:
    print(f'====Community {chr(i)} By modularity maximization
 algorithm ====')
    for person in persons:
        print(f' person: {person} in community:   {chr(i)}')
    i+=1
```

12.6.2.3 Hierarchical Clustering

Periodically separating the communities with the highest intercommunity edge density, the network is divided into a hierarchy of increasingly fine-grained communities is a process called hierarchical clustering. By treating the communities as network compressions, this probabilistic approach aims to determine the network's minimal description length.

12.6.2.4 Louvain's Method

The Louvain method is a quick, greedy optimization procedure that includes incrementally enhancing the network's modularity.

12.6.2.5 Label-Propagation Algorithm

A semisupervised machine-learning approach called label propagation spreads a limited set of labeled data points' labels across the remaining data points in the data set. Label propagation is based on the community membership of nearby nodes; this

TABLE 12.3
Simple Community Detection Using NetworkX Asynchronous Label _ propagation Algorithm

```
import networkx as nx
# Create a graph
G = nx.Graph()
# Add edges to the graph, create the community shown in figure 12.1
# Add edges to the graph, create the community shown in figure 12.1
G.add_edges_from([('Santa', 'Claus'), ('Santa', 'Nicolas'), ('Suresh',
 'Santa'), ('Suresh', 'Guna'), ('Suresh', 'Rudra'), ('Ramesh',
 'Guna'), ('Ramesh', 'Rudra'),('Rudra', 'Guna'),])
nx.draw_circular(G, with_labels=True,**options) #font_weight='9')
# the number of edges incident to Santa is 3 Claus, Nicolas, Suresh
print(G.degree['Santa'])
# Find communities in the graph using the greedy modularity
 maximization algorithm
communities = nx.community.label_propagation.asyn_lpa_communities(G)
#Chr value of lower case "a" which is our assigned label for first
 community.
#This can be any label, but this code does automatic assignment.
#So next label is community is "b" then "c","d","e","f".. so on for
 any size
i=97
for persons in communities:
    print(f'====Community {chr(i)} By Asynchronous label propogation
 algorithm (async_lpa) ====')
    for person in persons:
        print(f' person: {person} in community:   {chr(i)}')
    i+=1
```

straightforward, effective technique spreads labels or community membership information throughout the network. It operates by initially giving each node in the graph a distinct label, which is then iteratively updated based on the labels of the nodes around it. When there is a small amount of labeled data available but a huge amount of unlabeled data, this straightforward and effective approach can be utilized. A weighted average, where the weights are determined by how similar the data points are to one another, can be used to do this. Till the labels of the data points converge or attain an acceptable level of accuracy, keep iterating. For a variety of tasks, including classification, clustering, and regression, label propagation can be utilized. It is predicated on the notion that close data points' labels are probably going to be similar.

This involves the following steps: 1. Pick a sizable collection of unlabeled data points and a small collection of labeled data points. 2. Initialize the unlabeled data points' labels to match those of the labeled data points to which they are most comparable. 3. Update each node's label to reflect the label that is most frequently used by its neighbors by iterating across the graph's nodes. 4. Keep iterating, until the labels of the nodes converge or attain an acceptable level of accuracy (Everett, 1985).

12.6.2.6 Stochastic Block Model Method

This probabilistic model proposes that the network is constructed by connecting nodes more frequently inside communities than across communities once nodes are randomly assigned to communities.

12.6.2.7 Spectral Clustering

Spectral clustering is a mathematical technique that includes locating the eigenvectors of the graph's Laplacian matrix and using them to group the network's nodes.

There are other additional community-detection techniques suggested in the literature, each with distinct advantages and disadvantages (Al-Harigy et al. 2022). The specific properties of the network and the investigator's study objectives frequently influence the community-detection algorithm that is chosen.

12.6.3 Egocentricity-Detection Algorithms Using Python 3.5's NetworkX Module

After isolating the communities in a network, we examine the network to check if any nodes or clusters of nodes or communities do not seem to fit in with the rest of the network. These nodes could be revealing signs of nefarious behavior.

12.6.3.1 Degree Centrality

Degree centrality can be used to pinpoint nodes that may be implicated in staking in the context of cyberbullying detection. A network's central nodes can be used to identify probable cyberbullies activity because cyberbullies frequently play a central role in a network. Due to their greater number of connections to other nodes in the network, these nodes may be more inclined to engage in nefarious activities. It is important to keep in mind that degree centrality is merely one indicator of a node's importance and may not necessarily be the most useful indicator for spotting fraud. In this situation, other metrics such as betweenness centrality or eigenvector centrality may also be helpful. To effectively identify cyberbullying activity, it is also crucial to consider additional elements, such as the type of connections between nodes (Reda Alhajj & Jon Rokne, 2014).

12.6.3.2 Radial Measures of Centrality

Radial measures of centrality are measures of a node's centrality by examining routes that begin from a node and span outward toward other vertices in a radial fashion. These are degree, closeness, and eigenvector centrality (Borgatti & Everett, 1993). Degree of a node, explained in the introduction section, is the simplest radial measure. Closeness of a node is the sum of the shortest path of a given node to all remaining nodes on a network. This measure does not increase with size of the network making distinction between the nodes a difficult prospect. Eigenvector centrality of a node is the measures of the extent to which a node is connected to other well-connected nodes. This is computed by finding the principal eigenvector of the adjacency matrix of a graph. There are many computationally efficient algorithms for large sparse matrices. Eigenvector centrality remains stable for large networks and hence a usable measure of centrality in case of large networks (Figure 12.3).

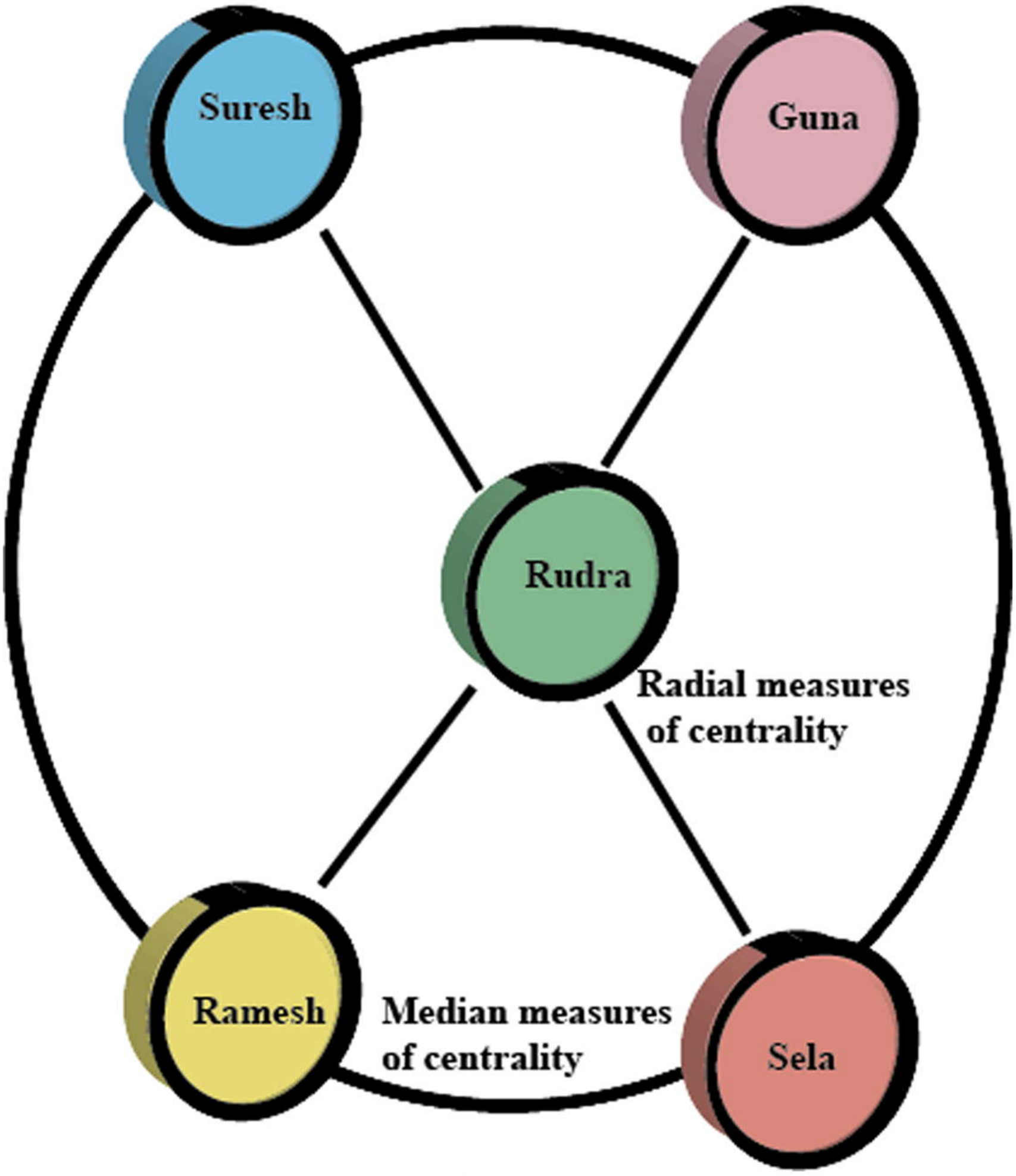

FIGURE 12.3 Radial measures of centrality and median measures of centrality are two measures of centrality of a node on a network. These are measure relative to a given node "Rudra" in this sample. Betweenness measures the connectivity of node to its neighbors and radial measures, degree, closeness, and eigenvector centrality of the radial distance to other nodes.

12.6.3.3 Median Measures of Centrality

Median measures of centrality are measures of a node's centrality by its longitudinal connectedness with other nodes (Borgatti & Everett, 1993). The most used medial measure is betweenness. Betweenness is number of times a vertex is found on the shortest route that connects any two other vertices. This can be computed using Ulrik Brandes algorithm. Cohesion is the extent of connectedness of whole network as opposed to a node. Cohesion matrix is the measure of cohesion. The adjacency matrix of a graph is the measure of cohesion in the simplest form. Connectedness and compactness are two more measures of cohesion of a network (Reda Alhajj & Jon Rokne, 2014).

12.6.3.4 Betweenness Centrality

The percentage of all shortest paths that pass through a node is thus considered to represent its betweenness centrality. The term "betweenness" in network analysis refers to a measurement of a node's significance (or vertex) in a network based on its capacity to link other nodes. Betweenness centrality counts the instances in which

a node spans the shortest distance between two other nodes. A node with a high betweenness centrality is frequently referred to as a key connector or hub since it has a significant impact on how other nodes in the network communicate (Longobardi et al. 2021). To determine betweenness centrality, we first list every shortest path in the network between any two nodes. Then we count how many times each node appears on the shortest pathways for each node.

To understand the function that nodes play in the communication and information flow inside a network, such as gatekeepers or major influencers, betweenness centrality is frequently employed to identify significant nodes in a network. To construct effective communication and transportation networks, it is also used to locate network bottlenecks or weaknesses.

It may be feasible to find patterns of nefarious behavior that are hidden when examining isolated transactions or nodes by identifying nodes with high betweenness centrality. Due to the high betweenness centrality of the criminal networks, it may be simpler to trace the flow of resources or information through the network and spot any irregularities in situations where the crime involves the manipulation of resources or information moving through the network (Barabasi, 2002).

12.6.3.5 An Example of Centrality Detection Using Python 3.5's NetworkX Module

A method in the *NetworkX* package called "*nx.eigenvector_centrality*" can be used to calculate eigenvector centrality of a node or account in a network. The following code creates a path graph of alphabets from A to P, then proceeds to calculate the eigenvector centrality of each node, and plots the values in a bar graph (Hagberg et al., 2008).

The output of the code is an image which is depicted in the figure; it can be observed from the plot that the nodes 'G,' 'H,' and 'I' have highest eigenvector centrality as these lie at the center of the circular path of the graph and inferred to have maximum reach to all the nodes.

12.6.4 Continue Investigation and Network Surveillance

It is vital to remember that these algorithms may result in false positives or false negatives because they are not perfect. As a result, it is crucial to confirm any abnormalities found and to carefully consider the algorithm's limits when interpreting the outcomes. These methods are not fool-proof methods as they are based on stochastic methods. There can be many instances of false-positive detections using the previously outlined steps. False-positive detections can entail compiling more information, conducting further research, or speaking with subject matter experts. Further, many cyberbullying instances may also go undetected using these methods (or false-negatives), which maybe be curtailed by repeating steps 1, 2, and 3. Thus, continued surveillance of network and optimization of our choice algorithms based on given network is essentially day-to-day activity of a network administrator in detecting and weeding out cyberbullying (Vasudev, 2006).

TABLE 12.4
Eigenvector Centrality Detection, Graphing Centrality Measures and Using *Python 3.5's NetworkX* Module

```
#Imports Networkx, string, and matplotlib modules. String is built-in
 Python module does NOT need installation
import networkx as nx
from matplotlib import pyplot as plt
import string
#initialize plot options
options = {'node_color': 'yellow','node_size':
 700,'alpha':0.9,'width': 1,  'edge_color':'red',}
# load A to P in a list
list_vertex=list(string.ascii_uppercase)[0:16]
#Initialize networkx Graph
G = nx. path_graph(list_vertex)
# compute eigenvector centrality of each node
centrality = nx.eigenvector_centrality(G)
#converting input dictionary values to a list
y = list(centrality.values())
x = list(centrality.keys())
fig = plt.figure("Degree of a random graph", figsize=(8, 8))
# Create a gridspec for adding subplots of different sizes
axgrid = fig.add_gridspec(5, 4)
ax0 = fig.add_subplot(axgrid[0:3, :])
nx.draw_shell(G, with_labels=True,**options) #font_weight='9')
ax0.set_title("Connected components of G")
ax0.set_axis_off()
ax1 = fig.add_subplot(axgrid[3:, :2])
degree_sequence = sorted((d for n, d in G.degree()), reverse=True)
dmax = max(degree_sequence)
ax1.plot(degree_sequence, "b-", marker="o")
ax1.set_title("Degree Rank Plot")
ax1.set_ylabel("Degree")
ax1.set_xlabel("Rank")
ax2 = fig.add_subplot(axgrid[3:, 2:])
ax2.bar(x,y)
#*np.unique(degree_sequence, return_counts=True))
ax2.set_title("Eigenvector Centrality")
ax2.set_xlabel("Vertex")
ax2.set_ylabel("Centrality")
fig.tight_layout()
plt.savefig("Centrality.png", dpi=300)
plt.show()
```

It should be noted that these are only a few instances of how network science algorithms might be applied to uncover cyberbullying. There are other additional methods and strategies that can be applied.

12.7 NETWORK MOTIFS TO HIDE CRIME

Network motifs are connectivity patterns that appear more frequently than would be predicted by chance inside a network. They have been employed in many disciplines, including biology, economics, and social networks, and can be used to pinpoint functional modules or paths within a network (Ranney et al. 2021). Network motifs have the potential to be employed in the context of fraud detection to find unusual patterns of activity or interactions within a network that might signify fraudulent behavior (Vasudev, 2006).

12.7.1 An Examples of Network Motifs to Hide Crime

A network motif known as a "feed-forward loop," for instance, consists of three nodes connected in a specific fashion, with the output of one node acting as the input for the following node. This kind of motif, which has been seen in biological and social networks, can be employed to boost signals or carry out computational operations. A feed-forward loop may be used to amplify or hide fraudulent transactions; therefore if one is seen in a financial network, it may be possible to utilize it to spot fraud (Reda Alhajj & Jon Rokne, 2014).

Other network patterns, such as "bistables," which are structures that may transition between two stable states, and "oscillators," which are structures that can produce periodic signals, may be helpful for detecting fraud.

12.7.2 Mechanisms of a Feed-Forward Network Motif

A feed-forward network motif consists of three nodes connected in a specific way. The "input node," the initial node, is where inputs from outside sources are received. The second node, sometimes known as the "output node," takes inputs from the first node and bases its output on those inputs. The third node, known as the "regulatory node," uses the inputs it gets from both the input node and the output node to control the information flow between the two nodes (Rajamani & Iyer, 2022). Figure 12.4 depicts the feed-forward loop motif.

According to this motif, the regulatory node receives its input from the regulatory node's output node and its output from the output node. The regulatory node modulates the information flow between the input and output nodes using the inputs it receives (Alsawalqa, 2021).

Networks of all kinds, such as social, biological, and economic ones, contain feed-forward loops. They have been seen in a wide range of devices and can be employed to boost signals or carry out computations. Feed-forward loops may be used to amplify or mask illegal transactions in the context of fraud detection, and they may also be used to spot fraudulent activities within a network (Gomez et al., 2022).

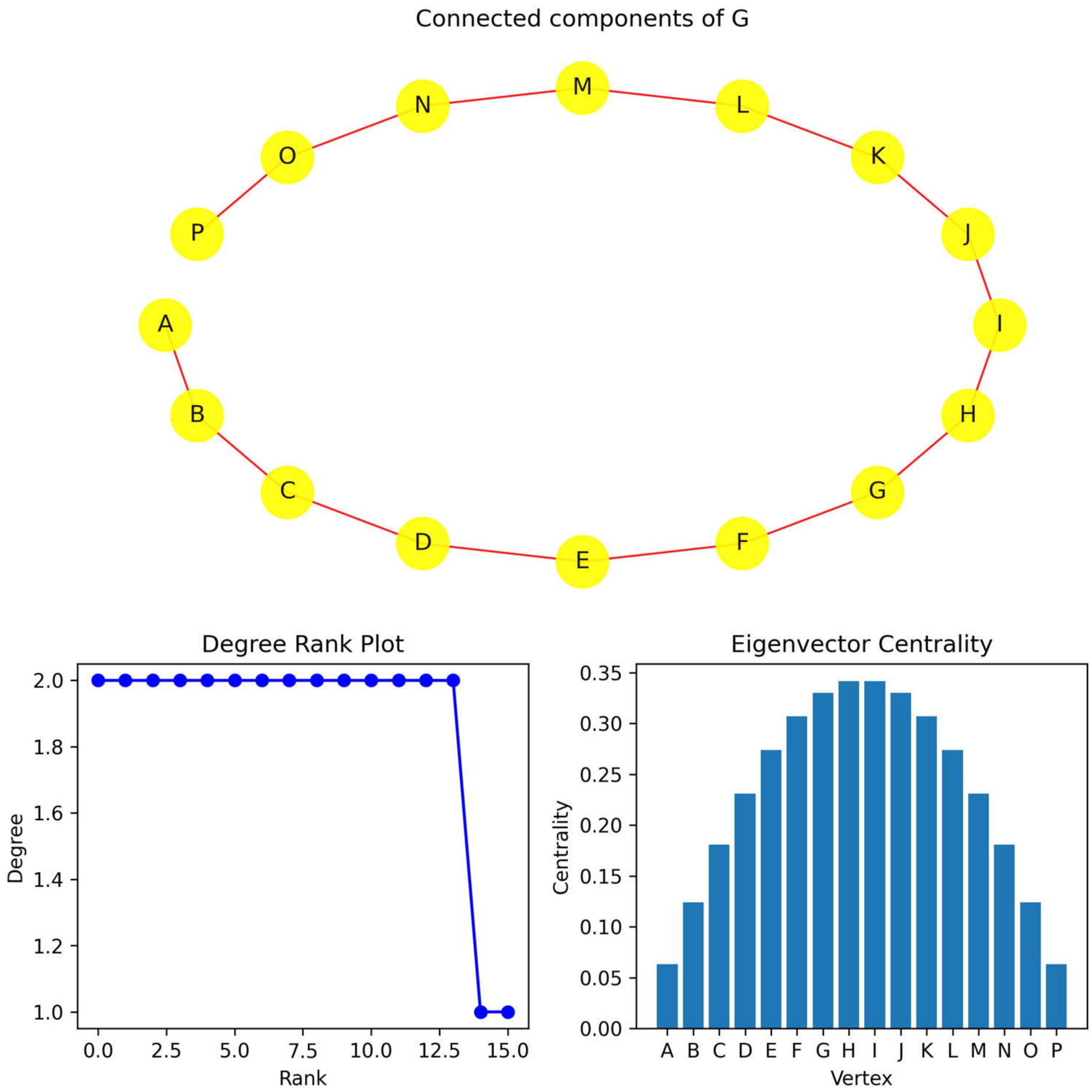

FIGURE 12.4 A simple example of path network from A to P ($N = 16$), shown above with measures plot of measures of centrality, namely, degree and eigenvector centrality. Plot of rank of node versus degree on left; it is to be noted that most nodes except "A" and "P" have degree of 2, and the bar plot of eigenvector centrality versus nodes, middle nodes "H" and "I," have maximum eigenvector centrality as they have access to maximum nodes being in the middle of the path graph.

12.7.3 Feed-Forward Network Motif for Crime and Evasion of Detection

By amplifying or hiding illegal transactions, a feed-forward network pattern may be used to hide criminal activities within a network. As an illustration, if a group of people were involved in a fraudulent operation, they would utilize a feed-forward loop to magnify the signals connected to their illegal transactions, making it harder for outsiders to identify the fraud (Everett, 1985) (Figure 12.5).

As an alternative, the feed-forward loop could be utilized to mask the fraudulent activity by generating a "smoke screen" of lawful transactions to hide the

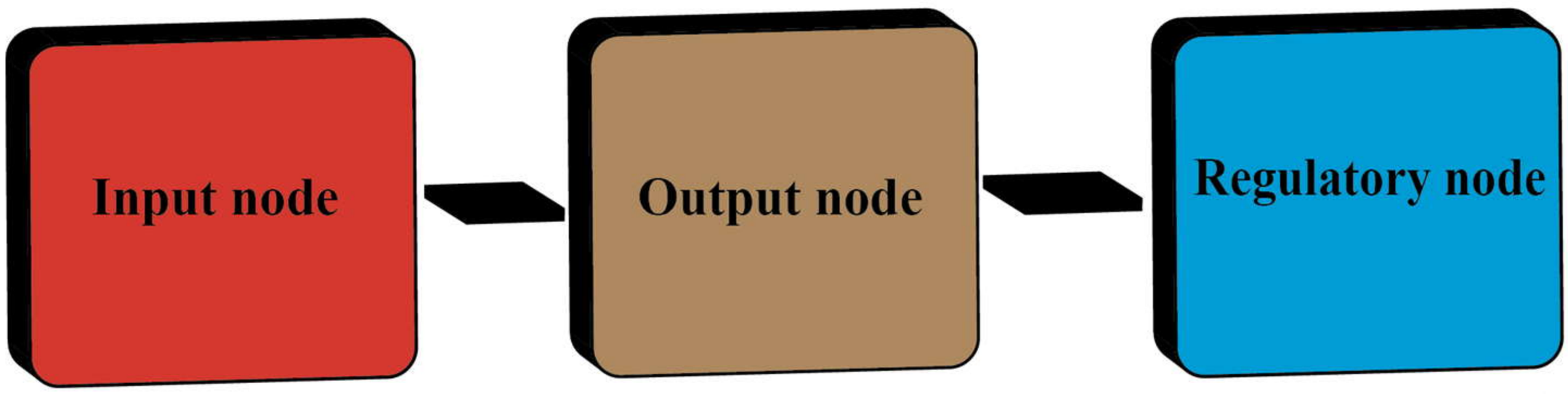

FIGURE 12.5 Network motifs can be tell-tale signs of nefarious activities and crime networks, a motif called feed-forward loop could be sign of fraud on a network. This picture illustrates the schema of such a network motif.

illegal activity. The regulatory node could be used to regulate the information flow between the two nodes, allowing the illicit transactions to be masked within the greater volume of legitimate transactions, for instance, if the input node of the feed-forward loop represents legitimate transactions and the output node represents illicit transactions. It is important to note that the potential employment of feed-forward loops or other network motifs to hide criminal conduct is completely conjectural, and there is no proof that such a plan has ever been successfully carried out. These kinds of motifs might be utilized to spot recurring patterns of conduct that might point to fraud (Lloret-Irles et al., 2022).

12.8 LIMITATIONS OF THIS REVIEW

This systematic review information and recommendations should be interpreted within a limited framework. Perceiving cyberbullying as a phenomenon is related to peer interaction and anonymity is an oversimplification. In contrast, the problem of cyberbullying arises due to a complex interaction of personal psychology, internet access, social media validation, social perception, family, and social media peer approval.

12.9 CONCLUSION

Cyberbullying is a modern menace and a misuse of technology to intimidate, harass, humiliate, and dehumanize others. As the technology of criminals evolves, so must the tactics and strategies to deal with such nefarious activities. In this compilation, a brief overview of cyberbullying is provided and followed by an account of steps to curb cyberbullying by network administrators, social media community administrators, teachers, and parents.

Complex analysis is the use of established and well-known network-analytical techniques to identify cyberbullying activities (Ngo et al. 2021). This is accomplished by establishing communities in the complex network and computing several centrality measures of offending node or account. To illustrate the actual process of complex network analysis, a few NetworkX working program samples are also included. These are based on simplified networks for the ease of comprehension. This is followed by continuous network surveillance to identify future culprits.

REFERENCES

Aboujaoude, E., & Savage, M. W. (2023). Cyberbullying: Next-generation research. *World Psychiatry : Official Journal of the World Psychiatric Association (WPA)*, *22*(1), 45–46. https://doi.org/10.1002/wps.21040

Ademiluyi, A., Li, C., & Park, A. (2022). Implications and preventions of cyberbullying and social exclusion in social media: Systematic review. *JMIR Formative Research*, *6*(1), e30286. https://doi.org/10.2196/30286

Alfakeh, S. A., Alghamdi, A. A., Kouzaba, K. A., Altaifi, M. I., Abu-Alamah, S. D., & Salamah, M. M. (2021). Parents' perception of cyberbullying of their children in Saudi Arabia. *Journal of Family & Community Medicine*, *28*(2), 117–124. https://doi.org/10.4103/jfcm.JFCM_516_20

Al-Harigy, L. M., Al-Nuaim, H. A., Moradpoor, N., & Tan, Z. (2022). Building towards Automated cyberbullying detection: A comparative analysis. *Computational Intelligence and Neuroscience*, *2022*, 4794227. https://doi.org/10.1155/2022/4794227

Alhajj, R. & Rokne, J. (2014). *Encyclopedia of Social Network Analysis and Mining* (1st ed.). Springer. doi:10.1007/978-1-4614-6170-8

Alsawalqa, R. O. (2021). Cyberbullying, social stigma, and self-esteem: The impact of COVID-19 on students from East and Southeast Asia at the University of Jordan. *Heliyon*, *7*(4), e06711. https://doi.org/10.1016/j.heliyon.2021.e06711

Armitage, R. (2021). Bullying in children: Impact on child health. *BMJ Paediatrics Open*, *5*(1), e000939. https://doi.org/10.1136/bmjpo-2020-000939

Barabasi, A. L. (2002). *Linked: The new science of networks*. Perseus Books Group.

Barabasi, A. L. & Albert, R. (1999). Emergence of scaling in random networks. *Science*, *286*, 509–512.

Barlett, C. P. (2023). Cyberbullying as a learned behavior: Theoretical and applied implications. *Children (Basel, Switzerland)*, *10*(2). https://doi.org/10.3390/children10020325

Bitar, Z., Elias, M.-B., Malaeb, D., Hallit, S., & Obeid, S. (2023). Is cyberbullying perpetration associated with anxiety, depression and suicidal ideation among lebanese adolescents? Results from a cross-sectional study. *BMC Psychology*, *11*(1), 53. https://doi.org/10.1186/s40359-023-01091-9

Borgatti, S. P. & Everett, M. G. (1993). Two algorithms for computing regular equivalence. *Social Networks*, *15*, 361–376.

Butts, C. T. (2006). Exact bounds for degree centralization. *Social Networks*, *28*, 283–296.

Camacho, A., Runions, K., Ortega-Ruiz, R., & Romera, E. M. (2023). Bullying and Cyberbullying perpetration and victimization: Prospective within-person associations. *Journal of Youth and Adolescence*, *52*(2), 406–418. https://doi.org/10.1007/s10964-022-01704-3

Everett, M. (1985). Role similarity and complexity in social. *Social Networks*, *7*, 353–359.

Fazeen, M, Dantu, R, & Guturu, P. (2011). Identification of leaders, lurkers, associates and spammers in a social network: Context-dependent and context-independent approaches. *Social Networks*, *1*(3), 241–254.

Floros, G., & Mylona, I. (2022). Association of cyberbullying and internet use disorder. *Current Addiction Reports*, *9*(4), 575–588. https://doi.org/10.1007/s40429-022-00440-9

Gabrielli, S., Rizzi, S., Carbone, S., & Piras, E. M. (2021). School interventions for bullying-cyberbullying prevention in adolescents: Insights from the UPRIGHT and CREEP projects. *International Journal of Environmental Research and Public Health*, *18*(21). https://doi.org/10.3390/ijerph182111697

Gomez, C. E., Sztainberg, M. O., & Trana, R. E. (2022). Curating cyberbullying datasets: A human-AI collaborative approach. *International Journal of Bullying Prevention : An Official Publication of the International Bullying Prevention Association*, *4*(1), 35–46. https://doi.org/10.1007/s42380-021-00114-6

Gongane, V. U., Munot, M. V., & Anuse, A. D. (2022). Detection and moderation of detrimental content on social media platforms: Current status and future directions. *Social Network Analysis and Mining*, *12*(1), 129. https://doi.org/10.1007/s13278-022-00951-3

Hagberg, A. A., Schult, D. A., & Swart, P. J. (2008). Exploring Network Structure, Dynamics, and Function using NetworkX. In G. Varoquaux, T. Vaught, & J. Millman (Eds.), *Proceedings of the 7th Python in Science Conference* (pp. 11–15).

Henares-Montiel, J., Benítez-Hidalgo, V., Ruiz-Pérez, I., Pastor-Moreno, G., & Rodríguez-Barranco, M. (2022). Cyberbullying and associated factors in member countries of the european union: A systematic review and meta-analysis of studies with representative population samples. *International Journal of Environmental Research and Public Health*, *19*(12). https://doi.org/10.3390/ijerph19127364

Hinduja, S., & Patchin, J. W. (2014). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Corwin press.

Hirschi, T. (1969). *Causes of delinquency*. University of California Press.

Huang, J., Zhong, Z., Zhang, H., & Li, L. (2021). Cyberbullying in social media and online games among chinese college students and its associated factors. *International Journal of Environmental Research and Public Health*, *18*(9). https://doi.org/10.3390/ijerph18094819

Kim, Y. J., Qian, L., & Aslam, M. S. (2021). Cyberbullying among traditional and complementary medicine practitioners in the workplace: Protocol for a cross-sectional descriptive study. *JMIR Research Protocols*, *10*(8), e29582. https://doi.org/10.2196/29582

Lancichinetti, A & Fortunato, S. (2009). Community detection algorithms: A comparative analysis. *Physical Review E*, *80*(5), 056117.

Lloret-Irles, D., Cabrera-Perona, V., Tirado-González, S., & Segura-Heras, J. V. (2022). Cyberbullying: Common predictors to cyber-victimisation and bystanding. *International Journal of Environmental Research and Public Health*, *19*(23). https://doi.org/10.3390/ijerph192315750

Longobardi, C., Thornberg, R., & Morese, R. (2021). Editorial: Cyberbullying and Mental Health: An Interdisciplinary Perspective. *Frontiers in Psychology*, *12*, 827106. https://doi.org/10.3389/fpsyg.2021.827106

Martínez-Valderrey, V., Gil-Mediavilla, M., Villasana-Terradillos, M., & Alguacil-Sánchez, S. (2023). Editorial: Bullying, cyberbullying, and dating violence: State of the art, evaluation instruments, and prevention and intervention proposals. *Frontiers in Psychology*, *14*, 1119976. https://doi.org/10.3389/fpsyg.2023.1119976

Marvin, Krohn. (1986). The web of conformity: A network approach to the explanation of delinquent behavior. *Social Problems*, *33*(6), S81–S93. Marvin, Krohn, Massey, J. L., & Zielinski, M. (1988). Role overlap, network multiplexity, and adolescent deviant behavior. *Social Psychology Quarterly*, *51*(4), 346–356.

Milosevic, T., Van Royen, K., & Davis, B. (2022). Artificial intelligence to address cyberbullying, harassment and abuse: New directions in the midst of complexity. *International Journal of Bullying Prevention : An Official Publication of the International Bullying Prevention Association*, *4*(1), 1–5. https://doi.org/10.1007/s42380-022-00117-x

Neelakandan, S., Sridevi, M., Chandrasekaran, S., Murugeswari, K., Pundir, A. K. S., Sridevi, R., & Lingaiah, T. B. (2022). Deep learning approaches for cyberbullying detection and classification on social media. *Computational Intelligence and Neuroscience*, *2022*, 2163458. https://doi.org/10.1155/2022/2163458

Newman, M. (2010). *Networks: An introduction*. Oxford University press.

Newman, M. E. J. (2003). The structure and function of complex networks. *SIAM Reviews*, *45*(2), 167–256.

Ngo, A. T., Tran, A. Q., Tran, B. X., Nguyen, L. H., Hoang, M. T., Nguyen, T. H. T., Doan, L. P., Vu, G. T., Nguyen, T. H., Do, H. T., Latkin, C. A., Ho, R. C. M., & Ho, C. S. H. (2021). Cyberbullying among school adolescents in an urban setting of a developing country: Experience, coping strategies, and mediating effects of different support on psychological well-being. *Frontiers in Psychology*, *12*, 661919. https://doi.org/10.3389/fpsyg.2021.661919

Rajamani, S. K., & Iyer, R. (2022). Development of an android mobile phone application for finding closed-loop, analytical solutions to dense linear, algebraic equations for the purpose of mathematical modelling in healthcare and neuroscience research. *NeuroQuantology*, 20, 4959–4973. https://doi.org/10.6084/m9.figshare.c.6156024.v1

Rajamani, S. K., & Iyer, R. S. (2023a). A Scoping Review of Current Developments in the Field of Machine Learning and Artificial Intelligence. In D. Samantha (Ed.), *Designing and developing innovative mobile applications* (pp. 138–164). IGI Global. https://doi.org/10.4018/978-1-6684-8582-8.ch009

Rajamani, S. K., & Iyer, R. S. (2023b). Machine Learning Based Mobile Applications Using Python and ScikitLearn. In D. Samanta (Ed.), *Designing and developing innovative mobile applications* (pp. 282–306). IGI Global. https://doi.org/10.4018/978-1-6684-8582-8.ch016

Ranney, M. L., Pittman, S. K., Moseley, I., Morgan, K. E., Riese, A., Ybarra, M., Cunningham, R., & Rosen, R. (2021). Cyberbullying prevention for adolescents: Iterative qualitative methods for mobile intervention design. *JMIR Formative Research*, *5*(8), e25900. https://doi.org/10.2196/25900

Sampasa-Kanyinga, H., Lalande, K., & Colman, I. (2018). Cyberbullying victimisation and internalising and externalising problems among adolescents: The moderating role of parent-child relationship and child's sex. *Epidemiology and Psychiatric Sciences*, *29*, e8. https://doi.org/10.1017/S2045796018000653

Sánchez-Medina, A. J., Galván-Sánchez, I., & Fernández-Monroy, M. (2020). Applying artificial intelligence to explore sexual cyberbullying behaviour. *Heliyon*, *6*(1), e03218. https://doi.org/10.1016/j.heliyon.2020.e03218

Schodt, K. B., Quiroz, S. I., Wheeler, B., Hall, D. L., & Silva, Y. N. (2021). Cyberbullying and mental health in adults: The moderating role of social media use and gender. *Frontiers in Psychiatry*, *12*, 674298. https://doi.org/10.3389/fpsyt.2021.674298

Shin, S. Y., & Choi, Y.-J. (2021). Comparison of cyberbullying before and after the COVID-19 pandemic in Korea. *International Journal of Environmental Research and Public Health*, *18*(19). https://doi.org/10.3390/ijerph181910085

Sutherland, E., Cressey, D. R., & Luckenbill, D. F. (1992). *Principles of criminology* (11th ed.). General Hall.

Tozzo, P., Cuman, O., Moratto, E., & Caenazzo, L. (2022). Family and educational strategies for cyberbullying prevention: A systematic review. *International Journal of Environmental Research and Public Health*, *19*(16). https://doi.org/10.3390/ijerph191610452

UmaMaheswaran, S. K., Deivasigamani, S., Joshi, K., Verma, D., Rajamani, S. K., & Ross, D. S. (2022). Computational Intelligence Approach to Improve The Classification Accuracy of Brain Tumor Detection. In *2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART)*, pp. 1192–1196. https://doi.org/10.1109/SMART55829.2022.10047792

Vasudev, C.(2006). *Graph theory with application*. New Age International Publication House.

Vogels, E. A., & Atske, S. (2022, December 15). Teens and Cyberbullying 2022. *Pew Research Center: Internet, Science & Tech*. https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/

Wright, M. F., & Wachs, S. (2023). Cyberbullying involvement and depression among elementary school, middle school, high school, and university students: The role of social support and gender. *International Journal of Environmental Research and Public Health*, *20*(4). https://doi.org/10.3390/ijerph20042835

Zhao, L., & Yu, J. (2021). A meta-analytic review of moral disengagement and cyberbullying. *Frontiers in Psychology*, *12*, 681299. https://doi.org/10.3389/fpsyg.2021.681299

Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures. *Frontiers in Public Health*, *9*, 634909. https://doi.org/10.3389/fpubh.2021.634909