RESEARCH ARTICLE

SAMRIDDHI Volume 14, Issue 4, 2022 Print ISSN: 2229-7111 Online ISSN: 2454-5767

An Approach to Prevent Neighborhood Attack over Social Media

Jitendra Patel*, Ravi K. S. Pippal

Department of Computer Science, Ram Krishna Dharmarth Foundation University, Bhopal, Madhya Pradesh, India

Abstract

Social media sites contain the personal information of the users, which entice the attackers The attacker uses several types of attacks on the social networking site to obtain sensitive information from the users. As different types of passive and active attacks are carried out on social media sites, user privacy may be compromised; to avoid this, the network operator releases data anonymously. Data from social media users is gathered and stored by social media operators for distribution to various third-party consumers. Because the fetched data frequently contains sensitive information, the network operator makes the entire graph available in anonymized and sanitized forms. It does not, however, provide a complete guarantee of user privacy. This research provided a way for anonymizing social network graphs using a neighborhood adjacency matrix-based anonymization process. This anonymization procedure could be utilized to defend against the social network graph's neighborhood attack. By adding fake edges to the social network graph, the suggested anonymization procedure increases the number of isomorphic neighborhood networks. As a result, a user's unique neighborhood network cannot be used to re-identify them in a social network graph.

Keywords: Social Media, Social Media Mining, Graph anonymization, Neighbourhood Attack, Graph-based Attack, Adjacency matrix.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2022); DOI: 10.18090/samriddhi.v14i04.10

Introduction

The practice of representing, evaluating, and extracting banned and suspicious patterns from social media data is known as social media mining. Basic concepts and algorithms for working with large amounts of social media data were introduced in social media mining. It covers topics such as computer science, data mining, machine learning, social network analysis, network science, sociology, ethnography, statistics, optimization, and arithmetic. It includes the instruments for formally representing, measuring, modeling, and mining meaningful patterns from vast amounts of social media data.[1]

Social media mining aims to discover new and useful knowledge from social network data. The data contains user's sensitive information, and it needs to be anonymized before publishing or given to data mining researchers to preserve social media users' privacy.[2]

The user's sensitive information is contained in the data published on social media sites. These data can be sent to a third party anonymously via an API for research and data analysis purposes. Because the data is in an anonymized format, attackers cannot re-identify an individual. However, if the victim has the same sequence as the attacker and the attacker has some previous knowledge of the victim, the attacker can re-identify the victim using structural-based assaults. The primary goal of this study is to offer an anonymized format for social networking data that is resistant to structural attacks.

The neighborhood attack on social networks was the topic of this paper. Third-party customers such as data analysts, epidemiologists, sociologists, and criminologists were given access to anonymized social networking data by social networking services. If an attacker obtains social network data, he or she will undertake various de-anonymization assaults on it.

To undertake de-anonymization attacks over social networks, an adversary gathers some baseline knowledge of social networks, which can be obtained by crawling or well-known web browser history stealing attacks, or by actively participating in social network sites.[3]

Corresponding Author: Jitendra Patel, Department of Computer Science, Ram Krishna Dharmarth Foundation University, Bhopal, Madhya Pradesh, India. e-mail: jitendra.jp12@gmail.com

How to cite this article: Patel J, Pippal RKS. (2022). An Approach to Prevent Neighborhood Attack over Social Media. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology,* 14(4), 60-66.

Source of support: Nil

Conflict of interest: None

An opponent acquires information about the victim's neighbor nodes, including their relationships, and uses this information as background knowledge in a neighborhood assault. Adversary used this knowledge and created a sub graph between the victim and its neighbors. After modeling the sub graph of the targeted node, the attacker searches anonymized social networks for this sub graph, and if it matches, the targeted node is successfully detected.[4,5]

- In a neighborhood attack scenario, the social network data is taken as naively anonymized and the social network graph doesn't contain any fake vertices and edges. Given an anonymized social network such that
- Anonymized social network is k-anonymous.
- Each vertex in the original social network is anonymized and anonymized social network does not contain any fake vertex.
- Every edge in the original social network is retained in anonymized social network.
- Anonymized social network can be used to answer aggregate network queries as accurately as possible.[6-9]

Social Media

Users can chat with their friends or relatives or find people who share their interests or concerns about politics, economics, music, or sports on social media.[6] The use of social media technologies, for example, can reveal information about a user's thoughts, feelings, goals, habits, and qualities. Marketing companies can use social media to promote their products and get more popularity among individuals who use the information on the social site. Social media provides benefits such as social connection, knowledge, and entertainment.

Social Connectivity

Social media emphasizes better connectivity by providing instant messaging services allowing real-time text transmission over the internet. For instance, people use social media to meet old friends, maintain relationships and even connect to new friends, which strengthens the overall connectivity between Social media users may build different type of communities and group to discuss or share information and get a different kind of views of other people. Many new updates have introduced by different social media sites like video call, conference chat, etc. that will directly benefits the connectivity. Social engagement is helpful in collective social activities likes helping person to improve interpersonal relationship, avoid being in isolated environment, and so on.

Information Accomplishment

Social media allow users to share information about them, political view, economics, music or sports. On social media, users may generate content, upload images, audio, videos and share with others. Users also share political views, latest technology, and upcoming movies or events information with their friends and get the opinion about that post. Generally people join the communities or group of users who have the same interest or problems (like; sport, science, social issues etc). Users can also contribute material that is already available on social media, such as information or content that is publicly available to the public. With the rise in popularity of social media, many websites now allow users to share their published articles, photographs, or videos on social media, allowing them to attract a wider audience. Marketing firms utilize social media to publicized new product details to gauge customer interest.

Advertising

With the rise in popularity of social media, marketing firms are utilizing it as a platform for product promotion. Marketing organizations can use social media to publish advertisements on their websites or develop a page for their product advertisements.[10-14] Social media users connect with one another and share information available on the platform. Marketing organizations take advantage of this by posting advertisements for new products on social media, which are then shared by people who are interested in them. Because of the benefits of sharing information, the new product's advertisement can reach a larger number of individuals in a shorter amount of time. Many marketing firms are also using social media to get input from consumers, allowing them to assess their product's popularity, customer needs, and concerns.

Attacks on Social Media

On the online social network, there is a lot of user information content. If someone wants to learn more about someone's life, the greatest way to do so is through social media. People on social media store their personal and private information on their profiles, which they can share with their friends who also use social media services. Because most people put their genuine information in their social media profiles, and that information may be extremely valuable to others, attackers are drawn to people's personal and private information. As a result of the genuine information available on social networking sites, these sites have become targets for attackers looking to obtain real information about social media users. Attackers utilize several types of social media attacks to gain access to user profiles or steal information from users on social networking sites. There are two types of social media attacks: aggressive and passive.

Active Attacks

In social media, active attacks are performed on the storage system. The attacker, by launching various types of attack on real time social networking sites, tries to steal information or access social media users. Attackers send malicious code, messages, bots, and hyperlinks to the users. User's mistakenly open malicious contents and get redirected to some malicious website. Also the malicious code gets spread

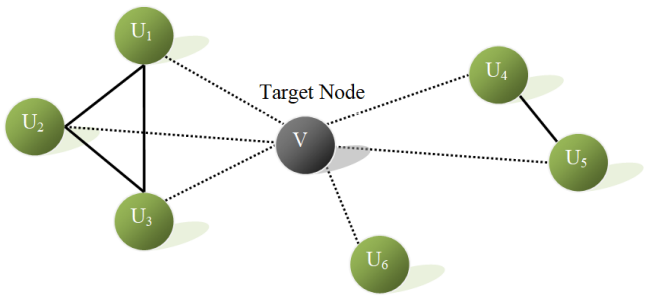

Figure 1: Neighborhood Graph over the Vertices V

in the user account that sends user sensitive information directly to the attacker.

Passive Attacks

Passive attacks on social network data are carried out by attackers. Researchers can analyze the hazards and challenges that social media users face by obtaining data from social networking sites. For third-party consumers, social networking companies have produced a sanitized version of anonymized social network data, which is available on social networking sites. Attackers obtain data from social media sites and run a de-anonymization assault on them to gain information about social media users. Passive attacks are difficult to detect, and the amount of user information that has been compromised is also a concern.

Related Work

Recently, neighborhood anonymization of the social network restricts the adversary with background knowledge of neighborhood structure to prevent structure-based attacks.[8-10] This paper presents the anonymization of social network data and preserves user privacy against neighborhood attacks.[11,12] The neighborhood attack based on a user and its neighbor's information identifies the isomorphic structure.[13-15] If two or more neighborhood networks are isomorphic in the social network graph, then the adversary cannot place a unique vertex neighborhood sub-network.[16,17] The proposed methodology increases the isomorphic neighborhood network in the social network graph by adding established imitation relationship edges.[18]

Neighborhood Attack over Social Networks

Suppose an adversary with advance knowledge of a targeted node's neighborhood can successfully identify a node in anonymized social networks and the neighborhood information of the identified node exactly matches the targeted node of the original social networks node. In that case, the adversary is said to have re-identified the target node (as shown in Figure 1).[6]

Building Background Knowledge

For a neighborhood attack, the adversary gathers information about the neighbors of the targeted node and their relationships, then builds a neighborhood network of the targeted node, which must be re-identified in an anonymized social network graph. Using a web-history stealing attack or actively participating in social networking sites, the adversary acquires information from targeted node neighbors.[7] Once the adversary has obtained knowledge about the targeted node's neighbors and their relationships, the adversary forms a sub graph based on the data gathered. The neighborhood attack is predicated on the idea that if an attacker gathers information about the victims' node's neighbors and their relationships, they can re-identify the victim's node from an anonymized social network.[15,16]

Suppose if an attacker knows that A has five friends, three of V's friends {u1,u2,u3} are friends with each other, {u4,u5} are connected and the last node is only the friend of V, Figure 2 represents the 1-neighborhood network of vertex V. An attacker can use this graph to identify a since 1-neighborhood graph is unique to each social network node. The information of vertex V's friends and the relationship between them is the background knowledge of the attacker, based on background knowledge attacker make a 1-neighborhood network of vertex V and use this graph to identify vertex V in published social network.

Extracting 1-Neighborhood Networks of Vertices

The vertex neighborhood network has all nodes and relationship between them; those have 1-distance or a direct link from the selected nodes in the network graph. 1-distance neighborhood network also known as 1.5-degree ego-network.

For extracting 1-neighborhood network of all vertices in the social network graph, the steps are described below:

- Build a social network graph from social network data. In this social network graph, a vertex may be connected with a single vertex or with multiple vertices.
- Now check the degree of each vertex in the social network graph and create vertices degree list in ascending order. Degree of a vertex is decided by a vertex is connecting with how many other vertices. If a vertex has connected with n other vertices in the social network graph then vertex has n degree.
- Once all vertices degree list is created in ascending order, select the first minimum degree node and find all the neighbors node of this vertex.
- Repeat the same process again with increasing vertex degree to extract all vertices 1-neighborhood network from the social network graph.
- When all vertices 1-neighborhood network are extracted then save them in ascending order list as vertices are arranged in degree sequence.

All vertices of 1-neighborhood networks are extracted and arranged in ascending order sequence. Now create the adjacency matrix for each neighborhood network and create the adjacency matrix for the adversary neighborhood

network that is created based on adversary background knowledge.

Adjacency Matrices of Neighborhood Networks

A basic labeled graph's adjacency matrix, also known as the connection matrix, is a matrix with rows and columns labeled by graph vertices, and a 1 or 0 at position (v i, v j) depending on whether v i and v j are adjacent or not. The adjacency matrix for a simple graph with no self-loops must have 0's or dots (.) on the diagonal. The adjacency matrix for an undirected graph is symmetric.

Figure 3 depicts the adjacency matrices of a sample node's neighborhood network. It illustrates the neighborhood network of vertex H and has four vertices: D, H, F, and G. A dot (-) represents diagonal values and no link value, while 1 represents an edge between two vertices. The adjacency matrices of these neighborhood networks are constructed after extracting the neighborhood networks of all vertices. The adversary neighborhood network's adjacency matrix is also generated using enemy background knowledge. Compare the adjacency matrices of the opponent neighborhood network with those of the vertices neighborhood network on the social network.

Algorithm [Stepwise explanation of performing NBH attack]

Step 1 Start

Step 2 Select the un-anonymized social network graph G (V, E) from the database, where $V = \{v_1, v_2, v_3 \ldots \ldots v_n\}$ is set of n vertices and $E = e_{ij} = (v_i, v_j) \mid vi,vj \in V, i \neq j$ is the set of edges between the n vertices of graph G. The degree of a node is decided by number of edges connected to with it. The set of degree $D = \{d_1, d_2, d_3 \ldots \ldots d_k\}$ is the available degrees in G.

Step 3 Extract adjacency matrix of each node from the un-anonymized social network graph G(V,E).

Step 4 Extract the neighborhood networks $N(v_i)$ from G. Here, $N(v_i)$ is the set of neighborhood networks $N(v_i) = \{N(v_1), N(v_2), N(v_3) \ldots \ldots N(v_s)$ in the graph G.

Step 5 Compare the adjacency matrix of neighborhood with the prior background knowledge of the target vertices.

Step 6 Resulted outcome of step 5 performs the Neighborhood attack.

Step 7 Stop

Comparison of Adjacency Matrices

This section explains the procedure of comparing adjacency matrices of created neighborhood network.

For comparing the adjacency matrix of two neighborhood networks, the steps are explained below:

- Select the list of all vertices neighborhood network and create adjacency matrices list for all of them.
- Now remove the head vertex from each neighborhood network adjacency matrix and create a new list for these adjacency matrices. Same as do for the adversary neighborhood network adjacency matrix, remove the head node (targeted node) from the adjacency matrix.
- The concept is behind the removing head node from the adjacency matrix because the targeted node location is unknown in the social network and the adversary used only neighbor nodes information. Therefore, after removing the head node from the adjacency matrix of the neighborhood network, the comparison may be possible between adjacency matrix of the social network and the adjacency matrix of adversary neighborhood network.
- After completing step 2, start a comparison of the adversary neighborhood network adjacency matrix with the social network adjacency matrices of the neighborhood network.

Vertex Re-identification

Vertex re-identification in a social network is the last stage of neighborhood attack scenario. For vertex re-identification comes after comparing the adversary adjacency matrix with the social network neighborhoods adjacency matrices. The details of vertex re-identifications are presented in the following steps:

- Select the adversary adjacency matrix without head vertex (targeted node), that is created based on background knowledge.
- Select the list of neighborhood networks adjacency matrices that are created after removing the head vertices in the social network
- Now, from the list select the first adjacency matrix and compare with the adversary adjacency matrix.
- Repeat the 3rd step for all the adjacency matrices for the social network neighborhood network until all the adjacency matrices are not compared.
- Once the comparison of adjacency matrices are completed then the result of matching adjacency matrix are displayed.
- This resultant adjacency matrix shows the neighbors of targeted vertex from the social network and result shows the neighborhood network adjacency matrix is associated with which vertex.
- Now the targeted vertex id is disclosed, with this vertex-id adversary can find the location of targeted node from the social network and all the information related to targeted node are disclosed to the adversary.
- In some exceptional cases, the result has more than 1 adjacency matrix of the neighborhood networks. It means if the targeted node and another node in a social network have the same neighbors associated with them then the result can show the more than 1head vertex for the result adjacency matrix.
- In an exceptional case, if p-number of vertices has similar neighborhood nodes then the adversary adjacency matrix matched with p-number of vertices and the result shows the p-number of vertices id. It means the adversary cannot find the targeted node more than 1/p probability.

Table 1: Parameters of Un-Anonymized Social Network Graph

Dataset	*#Tweets*	*#Vertices*	*#Edges*	*#Average Degree*
Twitter Dataset	100	315	435	3
	200	554	1085	4
	1000	2313	4110	4
Gnutella Dataset	501	501	710	3
	1001	1001	2068	4
	5001	5001	15798	6

Table 2: Parameters of Anonymized Social Network Graph

Dataset	*#Tweets*	*#Vertices*	*#Dummy Edges*	*#Total Edges*	*#Average Degree*
Twitter Dataset	100	315	101	536	4
	200	554	251	1336	6
	1000	2313	2513	6623	5
Gnutella Dataset	501	501	189	899	4
	1001	1001	958	3026	5
	5001	5001	4568	20366	8

Table 3: Evaluation of Anonymized Social Network Graph

	Tweet	RRAD	RRAE	Noise
Twitter Dataset	100	0.33	0.23	7.5
	200	0.50	0.23	4.4
	1000	0.25	0.61	1.3
Gnutella Dataset	501	0.33	0.27	4.9
	1001	0.25	0.46	2.3
	5001	0.33	0.29	0.2

Experimental Setup

In the social big data network anonymization, all the experiments conducted on a system running the Ubuntu 16.04 operating system, with a 2.3 GHz Core(TM) i3 CPU, 3.0 GB RAM and a 320 GB hard drive with open-source software Neo4j (version 3.3.5) and R (version 3.3.0). The program is implemented in R programming language. This paper illustrates the comparative analysis of social network graph anonymization on different sets of two different datasets, i.e., Real time Twitter dataset, and Gnutella Peer to Peer Network Dataset.

Real Time Twitter Dataset

Three set of real time data is extracted/crawled from the twitter. Firstly, 100 tweets is crawled, the network has 315 vertices and 435 edges. The data is collected from the followers of modi. Each node represent the followers and each edges represent a connection between a pair of hosts. Secondly, 1000 tweets has been selected, the network has 2313 nodes and 4110 edges. Thirdly, 10000 tweets is extracted, the network has 20350 vertex and 43500 edges.

Gnutella Peer to Peer Network Dataset

The Gnutella peer to peer network dataset represents a directed graph where the edge represents a connection between a pair of Gnutella hosts. It has 22687 nodes and 54705 edges.

Result Evaluation

The anonymization process tampers the originality by pouring some noise over the network, i.e., adding or removing the edges in published data. However, the level of anonymization depended upon the degree of noise added to the networks. The analysis is carried out on common parameters includes a number of nodes, the number of actual edges, the number of dummy edges and an average degree of the graph. In this paper, social network anonymization experiments were performed on two datasets: real-time Twitter and Gnutella peer-to-peer network datasets, as shown in Table 1.

The graphical description of anonymized social network graph, i.e., several vertices, the minimal number of dummy edges required to be added, the total number of resultant edges and an average degree, are shown in Table 2. The change in network information before anonymization and anonymization is visible after comparing Table 1 and 2. The number of vertices has remained unchanged. Whereas after incorporating the dummy edge, network density is increased, that reflects both in the total number of edge count and average degree.

Evaluation of the NUMA anonymization approach is carried out by using the following evaluation metrics (as shown in Table 3):

- **Anonymization Reflection of Average Degree (γ^{ad}):** γ^{ad} is the reflection of change in average degree before and after the anonymization through numa, as shown in equation 4.

$$\gamma^{ad} = \frac{\sum_{i=1}^{n} d(v_i) \in G' - \sum_{i=1}^{n} d(v_i) \in G}{\sum_{i=1}^{n} d(v_i) \in G} \quad (4)$$

.Where, G and G′ represent the graph before and after the anonymization.

- **Anonymization Reflection of Edge (γe):** γe is the reflection of the changed in total number of edge after anonymization,as shown in equation 5.

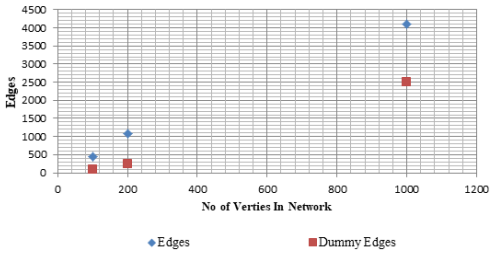

Figure 2: Reflection of Edges after Anonymization over Twitter Dataset

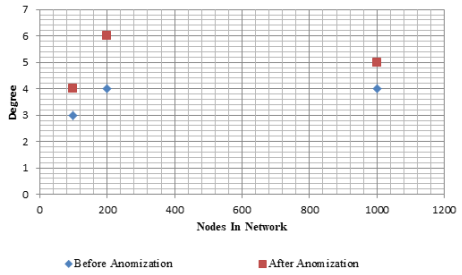

Figure 3: Reflection of Degree after Anonymization over Twitter Dataset

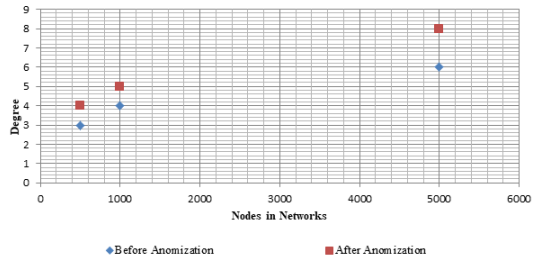

Figure 4: Reflection of Degree After Anonymization over Gnutella Dataset

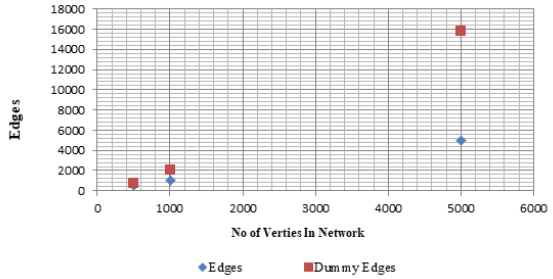

Figure 5: Reflection of Edge After Anonymization over Gnutella Dataset

$$\gamma^e = \frac{\sum_{i=1}^{n} e_i \in G' - \sum_{i=1}^{n} e_i \in G}{\sum_{i=1}^{n} e_i \in G} \quad (5)$$

Noise Level(α^l): Noise in network may be created due to change in network parameter i.e. number of vertices, edge and average degree. α^l is measured as the total reflection in network information after anonymization as shown in equation 6.

$$\alpha^l = \frac{\gamma^v + \gamma^e + \gamma^{ad}}{|v| + |e| + |ad|} \quad (6)$$

The average degree of graph before and after anonymization is shown in Figure 2 and the relative ratio of average degree is shown in Figure 3. The relative ratio of average degree over Twitter dataset is measured between 1.65 to 1.75. and the relative ratio of average degree in Gnutella peer to peer network is measured between 1.3 to 1.75. The changes of a few edges or vertices using adjacency based anonymization still have a small effect on the average degree.

Edge Change of graph before and after anonymization is shown in Figure 4 and Relative ratio of edge change is shown in Figure 5. The relative ratio of edge change over Twitter dataset is measured between 0.05 to 0.2. and the relative ratio of edge change in Gnutella peer to peer network is measured between 0.3 to 0.85. In big social networks, this adjacency matrix-based anonymization changes a small portion of vertices and edges without significantly affecting the neighborhood.

Conclusion

Social media has become an integral component of people's daily lives. For chatting and sharing, social media provides an easy way to connect with family and friends. People use social media to reconnect with old friends, maintain relationships, and even make new acquaintances, all of which helps to increase general connection among social media users. Users' personal information is stored on social media platforms, luring attackers in. To obtain the user's sensitive information, the attacker uses many types of attacks on the social media site. As a result of several types of passive and aggressive attacks on social networking platforms, users' privacy may be compromised. To avoid such a scenario, the network operator makes the data anonymous. Fake edges and vertices have recently been added to anonymization algorithms for preserving social network graph data. Inserting dummy vertices and edges raises the noise level, resulting in information loss. The number of dummy edges and vertex's added is directly proportional to the degree of information loss. In the anonymization of social networks, information loss is still an issue. Using dummy vertices and edges in social network data can alter the graph's uniqueness and increase the noise level. If there is excessive noise in anonymous social network data, researchers and data analysts may make an incorrect conclusion.

Reference

[1] Abawajy, J.H., Ninggal, M.I.H., Herawan, T.: Privacy preserving social net- work data publication. IEEE Communications Surveys Tutorials 18(3), 1974–1997 (2016). https://doi.org/10.1109/COMST.2016.2533668

[2] Jamil, A., Asif, K., Ghulam, Z., Nazir, M.K., Mudassar Alam, S., Ashraf, R.: Mpmpa: A mitigation and prevention model for social engineering based phishing attacks on facebook. In: 2018 IEEE International Conference on Big Data (Big Data). pp. 5040–5048 (2018).

[3] Ji, S., Li, W., Gong, N.Z., Mittal, P., Beyah, R.: Seed-based de-anonymizability quantification of social networks. IEEE Transactions on Information Forensics and Security 11(7), 1398–1411 (2016).

[4] Ji, S., Li, W., Srivatsa, M., Beyah, R.: Structural data de-anonymization: Theory and practice. IEEE/ACM Transactions on Networking 24(6), 3523–3536 (2016).

[5] Ji, S., Mittal, P., Beyah, R.: Graph data anonymization, de-anonymization attacks, and de-anonymizability quantification: A survey. IEEE Communications Surveys Tutorials 19(2), 1305–1326 (2017).

[6] Kergl, D. Enhancing network security by software vulnerability detection us- ing social media analysis extended abstract. In:

2015 IEEE International Conference on Data Mining Workshop (ICDMW). pp. 1532–1533 (2015).
[7] Liu, G., Wang, C., Peng, K., Huang, H., Li, Y., Cheng, W.: Socinf: Mem- bership inference attacks on social media health data with machine learning. IEEE Transactions on Computational Social Systems 6(5), 907–921 (2019).
[8] Ninggal, M.I.H., Abawajy, J.: Attack vector analysis and privacy-preserving social network data publishing. In: 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. pp. 847–852 (2011).
[9] Orabi, M., Mouheb, D., Al Aghbari, Z., Kamel, I.: Detection of bots in social me- dia: A systematic review. Information Processing and Management 57(4), 102250 (2020).
[10] Patil, N.A., Manekar, A.S.: A novel approach to prevent personal data on a social network using graph theory. In: 2015 International Conference on Computing Communication Control and Automation. pp. 186–189 (2015).
[11] Rekha, H.S., Prakash, C., Kavitha, G.: Understanding trust and privacy of big data in social networks - a brief review. In: 2014 3rd International Conference on Eco-friendly Computing and Communication Systems. pp. 138–143 (2014)
[12] Reza, K.J., Islam, M.Z., Estivill-Castro, V.: Social media users' privacy against malicious data miners. In: 2017 12th International Conference on Intelligent Systems and Knowledge Engineering (ISKE). pp. 1–8 (2017).
[13] Sharma, V.D., Yadav, S.K., Yadav, S.K., Singh, K.N., Sharma, S.: An effective approach to protect social media account from spam mail – a machine learning approach. Materials Today: Proceedings (2021).
[14] Sushama, C., Sunil Kumar, M., Neelima, P.: Privacy and secu- rity issues in the future: A social media. Materials Today: Proceedings (2021).
[15] Tian, W., Mao, J., Jiang, J., He, Z., Zhou, Z., Liu, J.: Deeply understanding structure-based social network de-anonymization. Procedia Computer Science 129, 52–58 (2018).
[16] Wang, B., Jia, J., Zhang, L., Gong, N.Z.: Structure-based sybil detec- tion in social networks via local rule-based propagation. IEEE Trans- actions on Network Science and Engineering 6(3), 523–537 (2019).
[17] Yang, D., Qu, B., Cudr´e-Mauroux, P.: Privacy-preserving social media data publishing for personalized ranking-based recommendation. IEEE Transactions on Knowledge and Data Engineering 31(3), 507–520 (2019).
[18] Zhang, J., Sun, J., Zhang, R., Zhang, Y., Hu, X.: Privacy-preserving social media data outsourcing. In: IEEE INFOCOM 2018-IEEE Conference on Computer Communications. pp. 1106–1114 (2018).