Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 2, February-2016

NETWORK SECURITY ON CENTRALIZED AND DISTRIBUTED SOCIAL NETWORKS BY INCREMENT CLUSTERING

Mr.Mrunalkumar Khairnar[1],Ms.Dipali Hadiyel[2], Mr.Sunny Thakur[3]

Information Technology, Sigma Institute of Technology, Vadodara, India[1 2 3]

Mr.Romil Patel[4]

Assistant Professor, IT, Sigma Institute Of Technology, Vadodara, India[4]

Abstract: - *In the past few years different social networks sites grow rapidly and they holds public and private information about their users. The privacy-preservation in social networks is major problem in now-a-days. The network data is divided between several data holders. The aim is to find the anonymized users make the cluster of every user and make anonymized view of the network without any of the users information near links among nodes that are arrange by other data users .In past centralized setting and anonymization algorithm is based on sequential clustering (Sq).Our algorithms considerably better than the SaNGreeA algorithm which is implemented using incremental clustering which is the leading algorithm for achieving anonymity in networks by means of clustering and provide security using checksum algorithm. We then devise secure distributed forms of the algorithms.*

Keywords: - *Social Networking, Sequential Clustering, Incremental clustering, Security.*

A. *I. INTRODUCTION*

The network is defines as a set of entities and the relations between the different users. A social network that provides the information for different entities to the users and connect them related to their relation, which may be relations of transaction. In the basic method, networks are displayed by the different graphs, where the nodes of the graph correspond to the values and the structural information represent relations between them [1].The social networks may be more difficult than the network. For example, a financial transaction network [12], the graph would be directed .If the interaction contains more than two players for example a social network that describes the users in social clubs then the network would create graph, where demographic information which we get from different type of interaction which are in form of labels and nodes in graph such as age, gender, location, or Jobs which could enrich and shed light on the structure of the network [1][13]. However, the data in such social networks cannot be released as is, since it might contain perceptive information.

II. EXISTING SYSTEM

In the existing system security issue is major part. Existing system uses sequential clustering to move, to delete and to add the players. A native anonymization of the network [12][1][13], in the sense of removing identifying attributes like names,ages,id,address or social security numbers from the data, is insufficient.

Existing system has 3 major category:-

- In this k-anonymity is differenced by adding or deleting the edges.
- Add noise and switching the data
- Use alternative graph method and cluster nodes into super node.

Limitation of existing system:-

- Its work only in centralized system in distributed manner this system not work properly.
- Security cannot be maintained
- Easily collect information from social graph
- Not reliable and performance.

III. PROPOSED SYSTEM

In this project our main aim is to present the extended method for Shield security of Centralized and Distributed Social Networks by incremental Clustering with improved dependency and performance:

- To represent shield data in anonymizing users
- To represent the new framework and methods.
- To represent high reliable system performances related to algorithm.
- Provide less time consumption
- To find competitive analysis of existing and proposed algorithm in order to claim the efficiency and time consumption

We presented incremental clustering algorithms for anonymizing social networks. Better utility is achieved by the proposed algorithms. The network data is divided between several data holders. The main point is to protect the structural information of the network where all the player have information about the nodes who are interconnected. In distributed scenario, each of the players needs to secure the node identity which are under their control from the other player. Hence, it is more difficult than Scenario in two manners:

1. proper secure computation of the descriptive information loss
2. The players must hide from other players the allocation of their nodes to clusters. So we use incremental clustering algorithm for as in network to adapt all nodes.

IV. SYSTEM IMPLEMATION

System flow:-

In this flow first select datasets, using datasets make graph of related nodes. Make the number of cluster and then partition of cluster. Move last partition nodes into the existing cluster and compare the sequential cluster and incremental cluster and then check secure computation sum for secure communication. Comparison between of both study

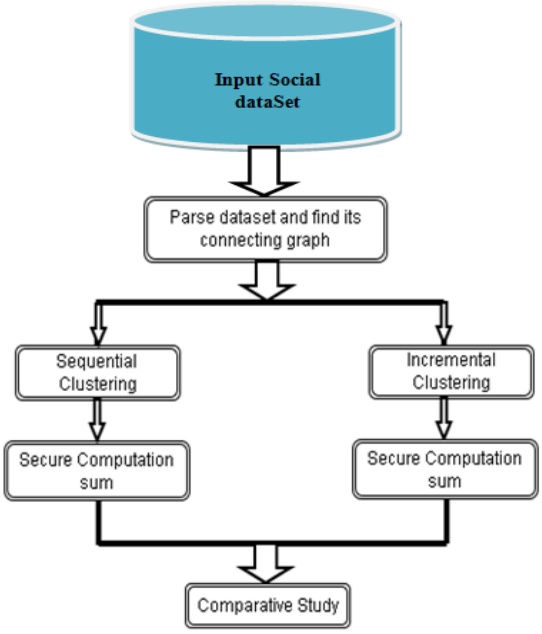

Fig. System Flow

A. *K-means Algorithm:-*

1. Plot K points into the space represented by the objects that are being clustered. These points represent predefined group centroids.
2. Determine each object to the group that has the nearest centroid.
3. When all objects have been submitted, recalculate the positions of the K centroids.
4. Repeat Steps 2 and 3 until the centroids no longer transfer. This creates a separation of the objects into groups from which the metric to be minimized can be calculated.

B. *Initial Partition Algorithm:-*

Input: A social network nodes, an integer k

Output: cluster of size ≥ k
Process:
Step 1. Choose a random partition of cluster of vertices
Step 2. Let cluster which is belong to current vertices.
Step 3. For each cluster compute different information loss if vertices move from one cluster to another cluster.
Step 4.If one cluster is singleton, move vertices from one cluster to another cluster and delete the first cluster.
Step 5.Else, if information loss is less than zero then move vertices from one cluster to another.
Step 6.If cluster size is greater than K split each of them randomly into two equally sized clusters
Step 7.If at least one node move during the last loop, go to step 2 to 6.
Step 8.while exists cluster size smaller than k, select one of them and unify it with the cluster which is closet
Step 9: Resulting cluster as output.

III.CONCLUSION AND FUTURE WORKS

Proposed system is running on real and sample data set which improves the performance and reliability of the system. We represented incremental clustering algorithms for secure social networks and anonymization view. Descriptive information loss and the players must hide from their allocation of their nodes which are to be clustered from the other player is the main problem in the existing system. So we use incremental clustering algorithm for security and reduce time complexity. As the privacy protection apply we can block the users/attacker for some time of span who are trying to hack the data.

ACKNOWLEDGMENT

We would like to extend our gratitude to our respected teacher – Mr.Romil Patel, for his constant support and for imparting us with the knowledge and helping us throughout the paper.

REFERENCES

1. Tamir Tassa and Dror J. Cohen "Anonymization of Centralized and Distributed Social Networks by Sequential Clustering" IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 2, February 2013
2. G. Aggarwal, T. Feder, K. Kenthapadi, R. Motwani, R. Panigrahy, D. Thomas, and A. Zhu, "Anonymizing Tables," Proc. 10th Int'l Conf Database Theory (ICDT), vol. 3363, pp. 246-258, 2005.
3. Baraba´si and R. Albert, "Emergence of Scaling in Random Networks," Science, vol. 286, pp. 509-512, 1999.
4. J. Benaloh, "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret," Proc. Advances in Cryptology (Crypto), pp. 251-260, 1986.
5. F. Bonchi, A. Gionis, and T. Tassa, "Identity Obfuscation in Graphs Through the Information Theoretic Lens," Proc. IEEE 27th Int'l Conf. Data Eng. (ICDE), pp. 924-935, 2011.
6. Campan and T.M. Truta, "Data and Structural k-Anonymity in Social Networks," Proc. Second ACM SIGKDD Int'l Workshop Privacy, Security, and Trust in KDD (PinKDD), pp. 33-54, 2008.
7. W. Jiang and C. Clifton, "A Secure Distributed Framework for Achieving k-Anonymity," The Int'l J. Very Large Data Bases, vol. 15, pp. 316-333, 2006.
8. M. Kantarcioglu and C. Clifton, "Privacy-Preserving Distributed Mining of Association Rules on Horizontally Partitioned Data," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 9, pp. 1026-1037, Sept. 200410] S. Kirkpatrick, D.G. Jr, and M.P. Vecchi, "Optimization by Simmulated Annealing," Science, vol. 220, no. 4598, pp. 671-680, 1983.
9. K. Liu and E. Terzi, "Towards Identity Anonymization on Graphs," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD), pp. 93-106, 2008.
10. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "-Diversity: Privacy Beyond k-Anonymity," ACM Trans. Knowledge Discovery and Data, vol. 1, no. 1, article 3, 2007.
11. M.E. Nergiz and C. Clifton, "Thoughts on k-Anonymization," Proc. Int'l Conf. Data Eng. (ICDE), p. 96, 2006.
12. P.Mohana Lakshmi,P.Balaji,P.Nirupma "Sequential Clustering Algorithms for Anonymizing Social Networks".
13. S.Bhagat,G.Coremode,B.Krishnamurthy and D. Srivasta "Class based graph annoymization for social network data"
14. Hongxin Hu, Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, and Jan Jorgensen" Multiparty Access Control for Online Social Networks: Model And Mechanisms"