Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/2665
DOI URL: http://dx.doi.org/10.21474/IJAR01/2665
ISSN NO. 2320-5407

RESEARCH ARTICLE

PRIVACY PRESERVING IN SOCIAL NETWORK

Harshit Varshney and Nital Adikane.
MIT College of Engineering Department of Information Technology, India.

Manuscript Info

Manuscript History

Received: 31 October 2016
Final Accepted: 30 November 2016
Published: December 2016

Key words:-
Cloud computing, social networks, privacy probability in distinguishability.

Abstract

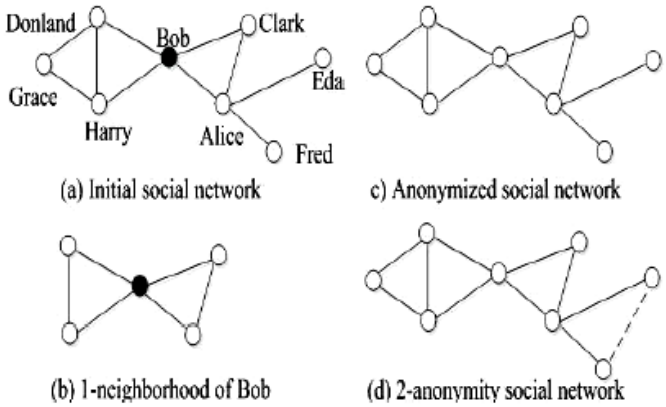
In the real world, a 3rd party companies will publish social networks, e.g., a cloud service supplier , for commerce intellect. An vital point is privacy protecting when declare social system of connection data. The paper shows a rare type of security problem,this termed surroundings violation. We suppose that an raider ability about the intensity of an ambition one-hop bystander, in accession to get community chart, the neighbour relationship target the one-hop bystander the aim and the relationship among these bystanders. Using this information, an attacker may find out the target from a *k*-anonymous social network with likelihood higher than 1/*k* where any node's 1-community chart is isomorphic with *k – 1* other node's chart. To protect the 1*-neighbourhood attack, privacy property key is defined, probability in distinguishability, for an large social network, and Introduce a heuristic in distinguishable group anonymization (HIGA) scheme to produce an anonymous social network with this privacy property. The practical study shows that the anonymous social networks can also be used to answer aggregate queries with high accuracy.

Introduction:-

As social network have been growing rapidly, to recognize their structure, advertising publicity, and data mining. In few years information technology is expected to rebuild the emerging computing paradigm as a cloud computing. Cloud services, are available in a pay-as-you-go manner, 24/7 at a low price. The important merits of cloud computing, e.g., flexibility and scalability, to outsource a portion of their data to a cloud environment more and more organizations that host social network data but main issue is preserving privacy when publishing social network data.

Social network helps to build social relationships between social actors. The relationships between social actors is usually private, and directly outsourcing the social networks to a cloud might result in unacceptable announcement.e,g,circulate social network information that depict a group of social actors related by passionate networks or shared drug injections may concession the privacy of the social actor involved.

Corresponding Author:- Harshit Varshney.
Address:- MIT College of Engineering Department of Information Technology, India.



neighbour attacks in a social network

A new approach is to anonymize the identity of the social actors before outsourcing. In any case , an attacker that has some knowledge about a target's neighborhood, specially a one-hop neighborhood, can still re-discover the target with high confidence. This attack, is termed as 1-neighborhood attack, is proposed by Zhou et al. [7].

Assume a social network of "co-authors", as shown in Fig. 1(a), where an edge that links two authors denotes that they initially cooperated on a paper and a node denotes an author. In the neighborhood attack, an attacker, who knows Bob's one-hop neighbors and the connections between them, i.e., Bob's 1-neighborhood graph, as shown in Fig. 1(b), can re-identify Bob from an anonymzed graph, Fig. 1(c), where all user identities are removed.

This is because Bob's 1-neighborhood graph is identical. To alleviate this attack, Zhou et al. defined a k-anonymity social network, where an attacker, with the idea of any target's 1-neighborhood graph, cannot re-identify the target with confidence more than 1/k. Their basic goal is to add noise edges to make any node's 1-neighborhood graph isomorphic with at least $k - 1$ other nodes' graphs. Given k isomorphic 1- neighborhood graphs, now all have a probability of 1/k to the target. For example, in Fig 1(d) we add an edge between Eda and Fred and then it becomes a 2 anonymity social network.

In this paper, we identify a new type of privacy attack, termed 1*-neighborhood attack, where an attacker is considered to know the degrees of the target's one-hop neighbors, in addition to the structure of the 1-neighborhood graph. We can well call this type of background knowledge the 1*-neighborhood graph.

This assumption is sensible , since once the attacker identify the target's one-hop neighbors, he will try to collect more data about the one-hop neighbors, rather than only collecting the connection data between them. With this assumption, the attacker may re-identify the target from a k-anonymity social network with a probability more than 1/k.

To illustrate, let us consider that the attacker knows the degrees of Bob's one-hop neighbors, Alice, Clark, Donland, and Harry, say 4, 2, 3, 3, respectively. In Fig. 1-(d), the degrees of Alice's one-hop neighbors, Bob, Clark, Eda, and Fred, are 4, 2, 2, 2, respectively [7] only adds edges to make 1-neighborhood graphs isomorphic, Alice can be removed from the target candidate group, and the probability to re-identify Bob is 1.To make the degrees of the k isomorphic graphs same we need to deal with 1*neighborhood attack and it need the addition of more edges .

To generate an anonymized social network, we propose a heuristic indistinguishable group anonymization (HIGA) scheme. Our basic idea consists of four key steps:

Grouping:-
we group nodes whose 1*-neighborhood graphs satisfy certain metrics, and provide a splitting and combining mechanism to make each group size at least equal to k.

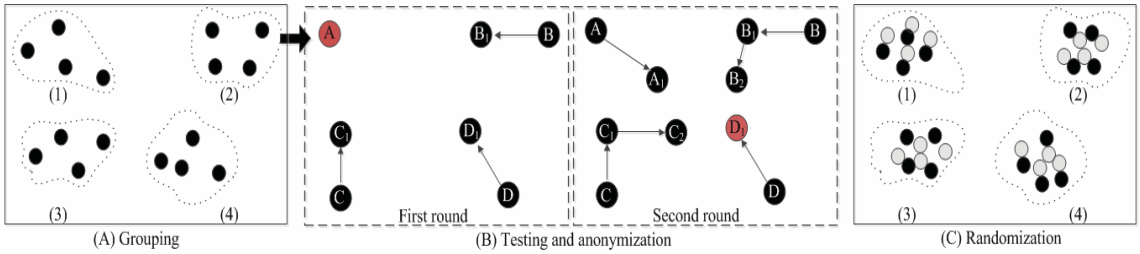
Testing:-
we use random walk (RW) [8], [9] to examine whether the 1-neighborhood graphs of any pair of nodes match or not.

Anonymization:-
we propose a heuristic anonymization algorithm to make any node's 1-neighborhood graph approximately match those of other nodes in a group, by either adding or removing edges [10], [11]

Randomization:-
We randomly modify the graph structure with a certain probability to ensure each 1*-neighborhood graph has a few probability of being different from the original one.

Preliminaries:-
System Model:-
We consider a system which consists of a publisher, a cloud service provider, an attacker, and users. The publisher,such as Twitter or Facebook , outsources a social network to a cloud. In proposed system, a social network is modeled as an undirected graph where V (G) is a set of nodes, and E(G) is a set of edges. The attacker may has few background knowledge about the target and he tries to re-identify the target by analyzing the social network. To preserve the privacy of the social actors in the network from the attacker, the publisher anonymizes G to G_ = (V (G_),E(G_)) before outsourcing. As in [7], we assume that each node in G exists in G_, and no fake nodes are added in G_ to preserve the structure of the social network. As previous work [10], [11], we allow edges {(u, v)} ∈ E(G) to be removed from E(G_). The cloud service provider, such as Google or Flipkart handles the cloud infrastructures, which take the bandwidth, storage space, and CPU power of many cloud servers to provide 24/7 services. We assume that the cloud infrastructures are the most reliable and the most powerful than personal computers. The users can perform data analysis on the outsourced social networks with more convenience. The users are assumed to be more interested in aggregate queries on the social networks; we are particularly interested in aggregate queries in this paper.

Attack Model:-
In this paper, we assume that the attacker is interested in the privacy of social actors. Before an attack, the attacker needs to collect background knowledge about the target victim. We assume that an attacker may have background knowledge about the 1*-neighborhood graphs of some targets. Informally, a



Analogue of the HIGA scheme.

target's 1*-neighborhood graph consists of both the 1-neighborhood graph of the target and the degrees of the target's one-hop neighbors. Following the work in for each node u ∈ V (G), the related 1-neighborhood graph, denoted as Gu, is defined as follows:

Neighborhood Graph. Gu = (Vu,Eu), where Vu denotes a set of nodes {v|(u, v) ∈ E(G) ∨ (v = u)}, and Eu denotes a set of edges {(w, v)|(w, v) ∈ E(G) ∧ {w, v} ∈ Vu}. For each node u ∈ V (G), the related 1*-neighborhood graph, denoted as G∗
u, is defined as follows:
1*-Neighborhood Graph. G∗
u = (Gu,Du), where Gu is the 1-neighborhood graph of node u, and Du is a sequence of degrees of u's one-hop neighbors.
For example, it may be easy to know that Fred has 100 neighbors,but hard to know the detailed information (ID, name, or age)about these 100 neighbors.

Heuristic indistinguishable group anonymization:-

A. Grouping We group nodes by using the following metric Number of one-hop neighbors,out-degree sequence, in-degree sequence, total number of edges and betweenness. We consider only these matrics Although other metrics, e.g., closeness centrality and local clustering coefficient, also can be used for grouping.

In-degree sequence. Iv = {|Eu+|}u∈ Vv , where Eu+={(u,w)|w ∈ Vv}, and |Eu+| is the number of edges in Eu+

Out-degree sequence.

Ov = {|E_u^-|}u∈ V_v , where E_u^- ={(u,w)|w ∉ Vv}, and | E_u^- | is the number of edges in E_u^-.

Betweenness. Bv = |V_v^*|/|V_v^+|, where V_v^* = {(u,w)|u, v ∈ V_v ∧ (u,w) ∉ Ev}, and V_v^+= {(u,w)|u, v ∈ V_v}.

B. Testing:-

Here we analyze each pair of nodes u and v by computing the steady states of their 1-neighborhood graphs We determine the approximate matching of Gu and Gv by performing bipartite graph. Inspired by the work in [12], we use random-walk-based approximate matching as the building block of our HIGA scheme. The random walk (RW) [8] is known as a useful tool

to obtain the steady state distribution for a graph referred to as the topological signatures, which provide the foundation for the approximate matching

Conclusion:-

In this paper To prevent the 1*-neighbourhood attack, privacy preserved property key is defined, probability in distinguishability, for an expand social network. We assume that an raider ability about the intensity of an ambition one-hop bystander, in accession to get community chart, the neighbour relationship target the one-hop bystander the aim and the relationship among these bystanders To generate such time of property for preserving the privacy in social network for anonym zing. Here we gave a new scheme called heuristics indistinguishable group anonymization (HIGA). The intensity of an ambition one-hop bystander, in accession to get community chart, the neighbour relationship target the one-hop bystander the aim and the relationship among these bystanders.

References:-

1. L. Getoor and C. Diehl, “Link mining: A survey,” ACM SIGKDD Explorations Newsletter, 2005.
2. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica et al., “A view of cloud computing,” Communications of the ACM, 2010.
3. G. Wang, Q. Liu, and J. Wu, “Hierarchical attribute-based encryption for fine-grained access control in cloud storage services,” in Proceedings of ACM CCS, 2010.
4. J. Gao, J. Yu, R. Jin, J. Zhou, T. Wang, and D. Yang, “Neighborhoodprivacy protected shortest distance computing in cloud,” in Proc. of ACM COMAD, 2011.
5. B. Zhou, J. Pei, and W. Luk, “A brief survey on anonymization techniques for privacy preserving publishing of social network data,”ACM SIGKDD Explorations Newsletter, 2008.
6. J. Potterat, L. Phillips-Plummer, S. Muth, R. Rothenberg, D.Woodhouse, T. Maldonado-Long, H. Zimmerman, and J. Muth, “Risk network structure in the early epidemic phase of HIV transmission in Colorado springs,” Sexually Transmitted Infections, 2002.
7. B. Zhou and J. Pei, “Preserving privacy in social networks against neighborhood attacks,” in Proc. of IEEE ICDE, 2008.
8. L. Page, S. Brin, R. Motwani, and T. Winograd, “The PageRank citation ranking: Bringing order to the web,” Stanford InfoLab, Tech. Rep., 1999.
9. M. Diligenti, M. Gori, and M. Maggini, “A unified probabilistic framework for web page scoring systems,” IEEE Transactions on Knowledge and Data Engineering, 2004.
10. M. Hay, C. Li, G. Miklau, and D. Jensen, “Accurate estimation of the degree distribution of private networks,” in Proc. of IEEE ICDM, 2009.
11. M. Gori, M. Maggini, and L. Sarti, “Exact and approximate graph matching using random walks,” IEEE Transactions on Pattern Analysis and Machine Intelligence, 2005.
12. K. Liu and E. Terzi, “Towards identity anonymization on graphs,” in Proc. of ACM SIGMOD, 2008.