ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 11, November 2016

A Research on Sanitization Technique against Personal Information Inference Attack on Social Network

Vaman Bankar[1] ,Prof. Miss. Khusbhu Sawant[2] ,Prof. Kuntal Barua[3]
PG Scholar, Dept.Of Computer Science & Engg., JDCT,Indore, M.P., India[1]
Professor, Dept.Of Computer Science & Engg., JDCT,Indore, M.P., India[2]
HOD, Dept.Of Computer Science & Engg., JDCT,Indore, M.P., India[3]

ABSTRACT-. Online social networking has become one amongst the foremost fashionable activities on the online. on-line social networks like Facebook ar more and more utilised by many of us. OSNs enable users to regulate and customise what personal data is on the market to alternative users. These networks enable users to publish details regarding themselves and to attach to their friends. a number of the knowledge unconcealed within these networks is supposed to be personal. A privacy breach happens once sensitive data regarding the user the knowledge that a private desires to stay from public is disclosed to AN mortal. however it's attainable to use learning algorithms on discharged knowledge to predict personal data. personal data outpouring might be a very important issue in some cases. Here the goal is simulate the logical thinking attacks victimization discharged social networking knowledge to predict personal data. In the planned system desired use {of knowledge|of knowledge|of information} ANd individual privacy presents an chance for privacy conserving social network data mining. Here within the system there ar 2 attainable sanitation techniques that might be employed in varied things for preventing logical thinking attack, those techniques ar removing details, removing link data from that dataset these techniques ar used for preventing logical thinking attack.

KEYWORDS- Online social networking, Private information leakage, privacy preserving social network, inference attack.

I. INTRODUCTION

Social networks area unit thought of as on-line applications that let the users to attach by method of assorted link varieties. supported the provided details, these networks let individuals to list details concerning themselves that area unit applicable to the basics of the network. Some website may be a common use of social network, so individual users list their most popular activities, movies and books. Conversely an expert network like LinkedIn, users specify details that area unit suited to their skilled life. These sites gather in depth personal info and so social network application suppliers have a rare probability of direct usage of this info that might be helpful to advertisers for marketing. For preventing logical thinking attack projected system is employed and it improves the classification accuracy of system by exploitation Naive bays classification.

II. LITERATURE SURVEY

Third Party Extension Attack

The human daily need as communication and socialization is the part of ever increasing use of social networking services. Social networks are a very useful and powerful communications tool that also has ability to share large volumes of information. However there are certain ways to exploitation of the user's personal information, it

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 11, November 2016

can have harmful consequences on user privacy. In order to address users privacy concerns a number of social media and social network web sites, such as Facebook, Orkut and Flickr, allow their participants to set the privacy level of their online profiles and to disclose either some or none of the attributes in their profiles[1]. While some users make use of these features, others are more open to sharing personal information. Some people feel comfortable displaying personal attributes such as age, political affiliation, gender, marital status, relationship status or location, while others do not. In addition most social- media users utilize the social networking services provided by forming friendship links and affiliating with groups of interest[13],[6]. While a persons profile may remain private, the friendship links and group affiliations are often visible to the public. Unfortunately these friendships and affiliations leak information, in fact as show they can leak a surprisingly large amount of information. The problem consider is sensitive attribute inference in social networks, inferring the private information of users given a social network in which some profiles and all links and group memberships are public[4],[5].

Gross et al. Examine specific usage instances at Carnegie Mellon. Note potential attacks, such as node reidentification of classification data, that helpful for accessible data on Facebook as social network site could assist with [11]. and further use that while privacy controls can exist on the users profile side of the social networking site like face- book, many individuals can not take advantage of this tool. This finding coincides need the amount of data that able to crawl using a very simple java crawler on a Facebook network. However need to extend on work by experimentally examining the accuracy of some types of the category reidentification that propose before and after sanitization[10].

K.Lui et al. Consider Social networks, online communities, peer-to-peer file sharing and telecommunication systems can be modeled as complex graphs. These graphs are of significant importance in various application domains such as marketing, psychology, epidemiology and homeland security[8].

In [10], Ahmadinejad et al study inference attacks that can be launched via the extension Application Programming Interface (API) of Facebook, Taxonomy of such attacks is devised and a risk metric is proposed to help subscribers of the third party applications refine their privacy expectations.

In [3], Heatherly et al have worked on Launching inference attacks using social net- working data to predict private information.

E.Zheleva et al.Consider the set of records with the same anonymized attributes forms an equivalence class. Since k-anonymity was first introduced, various methods for k- anonymizing data have been developed in the research community [4],[7].

Hay et al.and Liu and Terzi consider different ways of anonymizing facebook sites networks. However the work focuses on inferring details attributes from nodes as user in the network, not individually identifying individuals [4].

D.J. Watts et al. Collective Dynamics of Small World Networks for the experimentation of Inference attack because the sheer size SNS does not allowed for Dataset[21].

Different Classifier Approach

He et al. consider ways for inferring private information via friendship links by creating a user network from the links inside a facebook network. While the data crawl a real social network, Live Journal, use hypothetical attributes to analyze learning algorithm[4].

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 11, November 2016

J. Yedidia et al. compare various methods of link based classification including loopy belief propagation, mean field relaxation labeling, and iterative classification. However their comparisons do not consider the ways to preserve link based classification. Belief propagation as a means of classification is presented in [11].

Zheleva and Getoor propose several methods of social graph anonymization, focusing mainly on the idea that by anonymizing both the nodes in the group and the link structure, that one thereby anonymizes the graph as a whole. However, the meth- ods all focus on anonymity in the structure itself. For example through the use of k-anonymity or t-closeness, depending on the quasi identifiers which are chosen, much of the uniqueness in the data may be lost. Through the method of anonymity preservation,maintain the full uniqueness in each node, which allows more information in the data postrelease[9].

A. Friedman et al.Prposes Several classification and Sanitation techniques for Data Mining with Differential Privacy[17].

J. He et al. the authors conduct distributed data mining in a peer-to-peer net- work to end usage data about the network itself. However, the situation mentioned in this system is different from 7 scenario; in research the assumption is that the data is distributed fully across the system with each site having only minuscule knowledge of the entirety.The system is take overall social networks data and divided among several data warehouses where perform classification[4].

C. van et al. New Models in Probabilistic Information Retrieval are purposed for calculating the classification accuracy intended purpose to increase the classification accuracy for judging the Inference attack chances[20].

C. Clifton, Using Sample Size to Limit Exposure to Data Mining of SNS users because the Social sites are large network and the access of this dataset not allowed for all user so testing on only sample size dataset[18].

Sensitive attribute Removal

J. He et al.authors consider perturbing network data in order to preserve privacy. While their method considers graph structure, it ignores any extra details or traits that a node inside the social network may possess.

Note that authorized subjects are in terms of user relationships rather than by listing specific instances (i.e., person ids). However, in that work policy propagation is not possible, since no hierarchies are over resources, relationships and actions [10].

Raymond Heatherly et al. examine the user profile information instead hiding personal detail publish all detail but at the time of data release pass sanitize data set means remove some sensitive attribute and pass it to third party for some advertise purpose[1].

K. Tumer et al. Bayes Error Rate Estimation Using Classifier Ensembles, Different ensembles affect on the classifier accuracy [19].

L. Sweeney et al. A Model for Protecting Privacy by using the annonymization techniques of graph of social networking site's users profile data as node and link only [22].

III. PROBLEM DEFINITION

• Privacy to person that thinks about with the integrity of the people body, means that stop the trespasser entry in personal knowledge.

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 11, November 2016

• Privacy of non-public behavior,This relates to totally different aspects of behaviour like sexual preferences, political activities and spiritual thoughts each privately and public places.

• Here the effectiveness of each native and relative classification accuracy square measure reduces by victimization the sanitation strategies and it's terribly useful for preventing personal data attack on social network.

• Privacy of non-public communication just in case of people has Associate in Nursing interest to be able to communicate among alternative|one another} through totally different media while not being monitored or intercepted by other persons or organizations.

• Privacy of non-public knowledge, people claim that knowledge regarding themselves mustn't be out there to alternative people or organizations while not their consent and though the info is processed by a third-party, the individual should be able to have sizeable degree of management over it knowledge and its use.

• Here it has been planned to style a system that explore the impact of doable knowledge sanitation approaches on preventing such non-public data outflow, whereas permitting the recipient of the change knowledge to try to to illation on non-sensitive details.

• Desired use of knowledge Associate in Nursingd individual privacy presents an chance for privacy conserving social network, That is that the discovery {of information of knowledge} and relationships from social network data while not violating privacy.

IV. IMPLEMENTATION STRATEGY

1. AES Algorithm

AES is an symmetric block cipher. AES works by repeating the same steps multiple times. AES is a secret key encryption algorithm. AES operates on a fixed number of bytes. AES and most encryption algorithms are reversible. The AES algorithm operates on fixed number of bytes, that makes it simpler to implement. The key is divided into individual sub keys, a sub key for each operation round is considered. This process is known as KEY EXPANSION. AES is an iterated block cipher, that is the same operations are performed many times on fixed number of bytes. These operations can be divided into the following main functions:

1. Sub Bytes-This is a non-linear substitution step where each byte can be re- placed with another byte according to data in lookup table.
2. Shift Rows-This is a transposition step where each row of the state is shifted circularly for a certain number of steps.
3. Mix Columns-This is a mixing operation which operates on the columns, combining the bytes in each column.
4. Add Round Key-Each byte of the state is combined with the round key using bitwise xor Rounds.

2. Mathematical Modelling

Network classification

Network classification Collective inference is a method of classifying social network data using a combination of node details and connecting links in the social graph. Each of these classifiers consists of three components: a relational classifier, a local classifier, and a collective inference algorithm. Local Classifier: Local classifiers are a type of learning method that is applied in the initial step of collective inference. It is a classification technique that examines details of a node and constructs a classification scheme based on the details that it finds there. The naive classifier

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 11, November 2016

builds a model based on the details of nodes in the training set. Then applies this model to nodes in the testing set to classify them. Relational Classifiers: The relational classifier is a separate type of learning algorithm that looks at the link structure of the graph and uses the labels of nodes in the training set to develop a model which it uses to classify the nodes in the test set.

Specifically in [14] Macskassy and Provost examine four relational classifiers:

Class-distribution relational neighbour (cdRN), weighted-vote relational neighbour (wvRN),network- only Bayes classifier (nBC), and network-only link-based classification (nLB). The cdRN classifier begins by determining a reference vector for each class. That is for each class, cdRN,Cx develops a vector RVx which is a description of what a node that is of type Cx tends to connect to Specifically, RVx(a) is an average value for how often a node of class Cx has a link to a node of class Ca. To classify node ni, the algorithm builds a class vector, CVi, where CVi(a) is count of how often ni has a link to a node of class Ca. The class probabilities are calculated by comparing CVi to RVx as shown in eq.(5)for all classes Cx.Then BC classifier uses Bayes theorem to classify based only on the link structure of a node. That is it defines

$$P(C_x^i|\mathcal{N}_i) = \frac{P(\mathcal{N}_i|C_x^i) \times P(C_x^i)}{P(\mathcal{N}_i)} = \prod_{n_j \in \mathcal{N}_i} \frac{P(C_a^j|C_x^i) \times P(C_x^i)}{P(n_j)}, \quad \text{.....Eq(5)}$$

where Ni are the neighbors of ni, and then uses these probabilities to classify ni.ThenLB classifier collects the labels of the neighboring nodes and by means of logistic regression, uses these vectors to build a model.In the wvRN relational classifier, to clas- sify a node ni each of its neighbors, nj, is given a weight. The probability of n i being in class Cx is the weighted mean of the class probabilities of nis neighbors as calculated in eq.(6). That is

$$P(C_x^i|\mathcal{N}_i) = \frac{1}{Z} \sum_{n_j \in \mathcal{N}_i} [w_{i,j} \times P(C_x^j)], \quad \text{.....Eq(6)}$$

Collective Inference Methods: Unfortunately there are issues with each of the methods described above. Local classifiers consider only the details of the node it is classifying. Conversely relational classifiers consider only the link structure of a node. Specifically a major problem with relational classifiers is that while we may cleverly divide fully labeled test sets so that we ensure every node is connected to at least one node in the training set, real world data will may not satisfy this strict requirement. If this type of requirement is not met, then relational classification will unable to classify nodes which have no neighbors in the training set. The collective inference attempts to make up for these deficiencies by using both local and relational classifiers in a precise manner to attempt to increase the classification accuracy of nodes in the network and by using a local classifier in the first iteration, the collective inference ensures that every node will have an initial probabilistic classification will referred to as a prior and the algorithm then uses a relational classifier to reclassify nodes. At each of these steps i>2, the relational classifier uses the fully labeled graph from step i 1 to classify each node in the graph.

The collective inference method also controls the length of time the algorithm runs. In Some algorithms specify a number of iterations to run, while others are converge after a general length of time.

V. RESULTS ANALYSIS

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 11, November 2016

Results of Sanitized system of Facebook profile is formulated as follows, the performance analysis of system are discussed in detail.

1) Selection of Sample Data

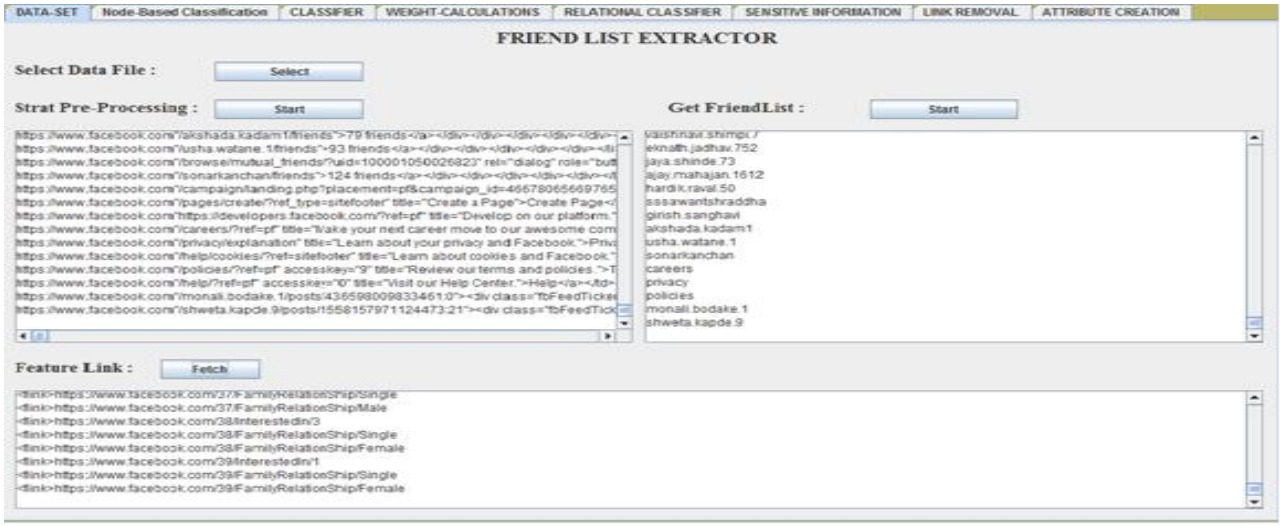


Fig.1 Selection of Sample Data

2) Feature vector generation and test node selection

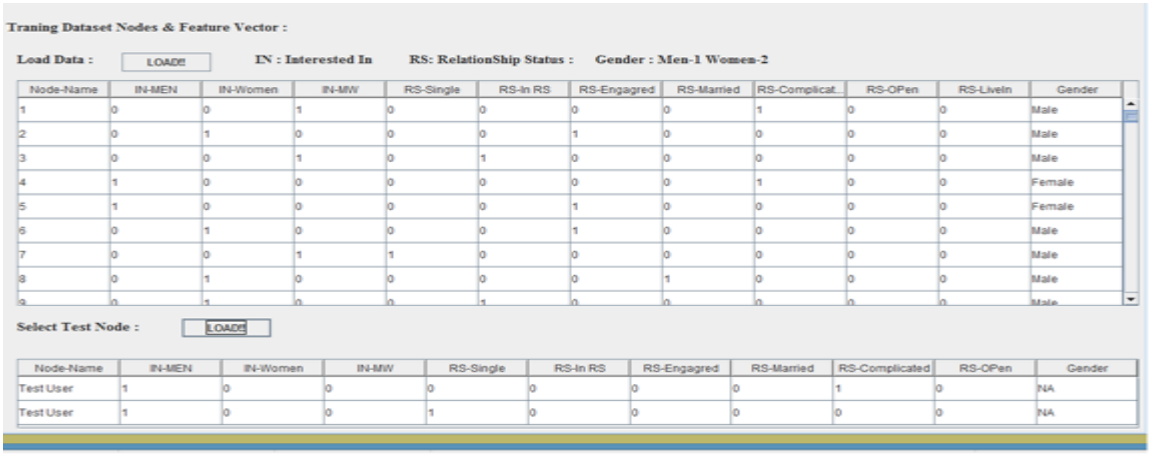
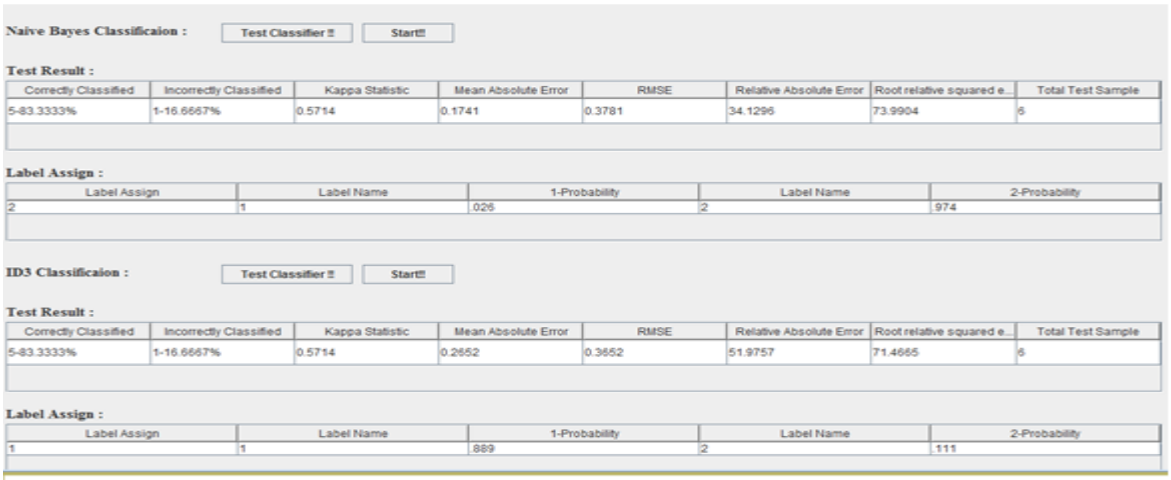


Fig.2 Feature vector and test node selection

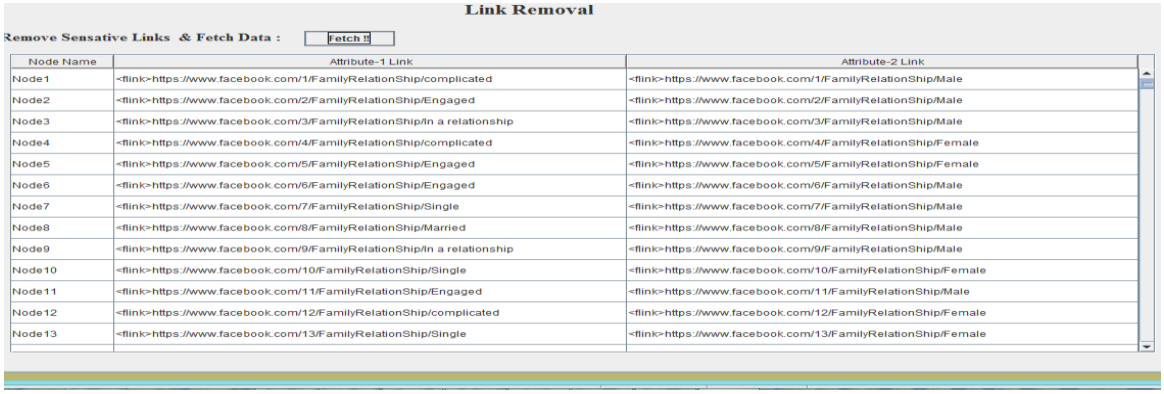
3) Classifier accuracy



ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 11, November 2016

Fig.3 Dataset Classifier

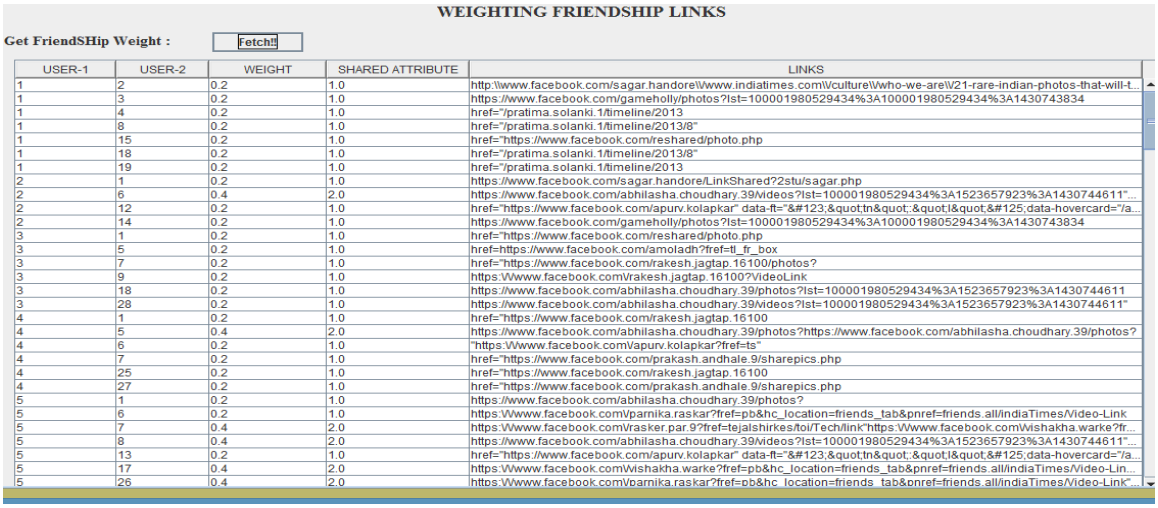
4) Sensitive Link removal model



Node Name	Attribute-1 Link	Attribute-2 Link
Node1	<flink>https://www.facebook.com/1/FamilyRelationShip/complicated	<flink>https://www.facebook.com/1/FamilyRelationShip/Male
Node2	<flink>https://www.facebook.com/2/FamilyRelationShip/Engaged	<flink>https://www.facebook.com/2/FamilyRelationShip/Male
Node3	<flink>https://www.facebook.com/3/FamilyRelationShip/In a relationship	<flink>https://www.facebook.com/3/FamilyRelationShip/Male
Node4	<flink>https://www.facebook.com/4/FamilyRelationShip/complicated	<flink>https://www.facebook.com/4/FamilyRelationShip/Female
Node5	<flink>https://www.facebook.com/5/FamilyRelationShip/Engaged	<flink>https://www.facebook.com/5/FamilyRelationShip/Female
Node6	<flink>https://www.facebook.com/6/FamilyRelationShip/Engaged	<flink>https://www.facebook.com/6/FamilyRelationShip/Male
Node7	<flink>https://www.facebook.com/7/FamilyRelationShip/Single	<flink>https://www.facebook.com/7/FamilyRelationShip/Male
Node8	<flink>https://www.facebook.com/8/FamilyRelationShip/Married	<flink>https://www.facebook.com/8/FamilyRelationShip/Male
Node9	<flink>https://www.facebook.com/9/FamilyRelationShip/In a relationship	<flink>https://www.facebook.com/9/FamilyRelationShip/Male
Node10	<flink>https://www.facebook.com/10/FamilyRelationShip/Single	<flink>https://www.facebook.com/10/FamilyRelationShip/Female
Node11	<flink>https://www.facebook.com/11/FamilyRelationShip/Engaged	<flink>https://www.facebook.com/11/FamilyRelationShip/Male
Node12	<flink>https://www.facebook.com/12/FamilyRelationShip/complicated	<flink>https://www.facebook.com/12/FamilyRelationShip/Female
Node13	<flink>https://www.facebook.com/13/FamilyRelationShip/Single	<flink>https://www.facebook.com/13/FamilyRelationShip/Female

Fig.4 Removal sensitive link

5)Weight calculation between users



USER-1	USER-2	WEIGHT	SHARED ATTRIBUTE	LINKS
1	2	0.2	1.0	http:\\www.facebook.com/sagar.handore\\www.indiatimes.com\\culture\\who-we-are\\21-rare-indian-photos-that-will-t...
1	3	0.2	1.0	https://www.facebook.com/gameholly/photos?lst=100001980529434%3A100001980529434%3A1430743834
1	4	0.2	1.0	href="/pratima.solanki.1/timeline/2013
1	8	0.2	1.0	href="/pratima.solanki.1/timeline/2013/8"
1	15	0.2	1.0	href="https://www.facebook.com/reshared/photo.php
1	18	0.2	1.0	href="/pratima.solanki.1/timeline/2013/8"
1	19	0.2	1.0	href="/pratima.solanki.1/timeline/2013
2	1	0.2	1.0	https://www.facebook.com/sagar.handore/LinkShared?2stu/sagar.php
2	6	0.4	2.0	https://www.facebook.com/abhilasha.choudhary.39/videos?lst=100001980529434%3A1523657923%3A1430744611"...
2	12	0.2	1.0	href="https://www.facebook.com/apurv.kolapkar" data-ft="{"tn":"I"}data-hovercard="/a...
2	14	0.2	1.0	https://www.facebook.com/gameholly/photos?lst=100001980529434%3A100001980529434%3A1430743834
3	1	0.2	1.0	href="https://www.facebook.com/reshared/photo.php
3	5	0.2	1.0	href=https://www.facebook.com/amoladh?fref=tl_fr_box
3	7	0.2	1.0	href="https://www.facebook.com/rakesh.jagtap.16100/photos?
3	9	0.2	1.0	https:\\www.facebook.com\rakesh.jagtap.16100?VideoLink
3	18	0.2	1.0	https://www.facebook.com/abhilasha.choudhary.39/photos?lst=100001980529434%3A1523657923%3A1430744611
3	28	0.2	1.0	https://www.facebook.com/abhilasha.choudhary.39/videos?lst=100001980529434%3A1523657923%3A1430744611"
4	1	0.2	1.0	href="https://www.facebook.com/rakesh.jagtap.16100
4	5	0.4	2.0	https://www.facebook.com/abhilasha.choudhary.39/photos?https://www.facebook.com/abhilasha.choudhary.39/photos?
4	6	0.2	1.0	"https:\\www.facebook.com\apurv.kolapkar?fref=ts"
4	7	0.2	1.0	href="https://www.facebook.com/prakash.andhale.9/sharepics.php
4	25	0.2	1.0	href="https://www.facebook.com/rakesh.jagtap.16100
4	27	0.2	1.0	href="https://www.facebook.com/prakash.andhale.9/sharepics.php
5	1	0.2	1.0	https://www.facebook.com/abhilasha.choudhary.39/photos?
5	6	0.2	1.0	https:\\www.facebook.com\parnika.raskar?fref=pb&hc_location=friends_tab&pnref=friends.all/indiaTimes/Video-Link
5	7	0.4	2.0	https:\\www.facebook.com\rasker.par.9?fref=tejalshirkes/toi/Tech/link"https:\\www.facebook.com\wishakha.warke?fr...
5	8	0.4	2.0	https://www.facebook.com/abhilasha.choudhary.39/videos?lst=100001980529434%3A1523657923%3A1430744611"...
5	13	0.2	1.0	href="https://www.facebook.com/apurv.kolapkar" data-ft="{"tn":"I"}data-hovercard="/a...
5	17	0.4	2.0	https:\\www.facebook.com\wishakha.warke?fref=pb&hc_location=friends_tab&pnref=friends.all/indiaTimes/Video-Lin...
5	26	0.4	2.0	https:\\www.facebook.com\parnika.raskar?fref=pb&hc_location=friends_tab&pnref=friends.all/indiaTimes/Video-Link"...

Fig.5 Weight Calculation between two users

Comparative Result Analysis

Here the result comparison of previous system accuracy with current system accuracy after removing of sensitive attribute as gender details. The table is contains the value of accuracy after removing attributes one by one of current and existing system. The graph 6.11 is show the comparison between previous and current system accuracy statestable contains the value of accuracy after removing details and link information from the dataset of existing system and also contains same data as details and link information from the dataset of current system. So the accuracy reduction is in large percentage in current system than previous one. So indirectly the data is more incorrect classify in this system on Gender attributes.

Approximately the 90 percent available nodes are heterosexual there are not details that are highly indicative of sexual orientation even minor changes affect the classification ac- curacy in unpredicted ways .Here get lowered classification accuracy after remove three attribute as Interest in field ,but for fourth details removal classification accuracy is in- creased.

VI. CONCLUSION

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 11, November 2016

Desired use of knowledge and individual privacy presents a chance for privacy-preserving social network data mining. that's the invention knowledge|of knowledge} and relationships from social network data while not violating privacy. Then devise 3 attainable cleaning techniques that might be used in varied things. The System is use for preventing illation attack on user profile information of social network. The projected system is exploitation each relationship links and details along provides higher certainty than details alone. Additionally implement the impact of removing details and links in preventing sensitive info leak. Here discovered things within which collective illation doesn't improve on employing a straightforward native classification technique to spot nodes. once mix the results from the collective illation implications with the individual results, begin to examine that removing Desired use {of information of knowledge of information} and individual privacy presents a chance for privacy-preserving social network data mining. that's the invention knowledge of knowledge} and relationships from social network data while not violating privacy. Then devise 3 attainable cleansing techniques that might be used in varied things. The System is use for preventing illation attack on user profile information of social network. The projected system is exploitation each friendly relationship links and details along provides higher certainty than details alone. additionally implement the impact of removing details and links in preventing sensitive info leak. Here discovered things within which collective illation doesn't improve on employing a straightforward native classification technique to spot nodes. once mix the results from the collective illation implications with the individual results, begin to examine that removing details and friendly relationship links along is that the best thanks to cut back classifier accuracy details and friendly relationship links along is that the best thanks to cut back classifier accuracy.

In system applying totally different classifier for reducing the accuracy of classification, the primary is Naive Bays classifier square measure supported link and detail info thus when removing sensitive attribute from the classified dataset its accuracy is reduces. Therefore the unharness dataset can't properly classify means that it useful for preventing the illation attack. Here show that every of those ways provides a live of privacy guarantee for users inside the network. The system will extended for cleansing of forestall personal info illation attack is by providing user profile info to third party in encrypted format for maintaining privacy for user profile information.

In future scope think about a lot of detail attributes for classification accuracy which will terribly helpful for accuracy reduces of classifier on totally different attribute removal.

REFERENCES

[1] **"Preventing Private Information Inference Attacks on Social Networks Ray- mond Heatherly, Murat Kantarcioglu, and Bhavani Thuraisingham," Fellow,IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 8 AUGUST 2013.**

[2] **Introduction to dataveillance and information privacy, and definitions of terms, Roger Clarkes Dataveillance and Information Privacy Pages, 1999.**

[3] **" J. Lindamood, R. Heatherly, M. Kantarcioglu, and B. Thuraising- ham, Inferring Private Information Using Social Network Data, Proc.18th Intl Conf. World Wide Web (WWW), 2009.**

[4] **" E. Zheleva and L. Getoor, Preserving the Privacy of Sensitive Relationships in Graph Data, Proc.First ACM SIGKDD Intl Conf. Privacy, Security, and Trust in KDD, pp. 153-171, 2008.**

[5] **J. He, W. Chu, and V. Liu, Inferring Privacy Information from Social Networks, Proc. Intelligence and Security Informatics, 2006.**

[6] **K.M. Heussner, Gaydar n Facebook: Can Your Friends Reveal Sex- ual Orientation ABC News, http://abcnews.go. com/Technology/gaydar-facebook- friends/storyid=8633224. UZ939UqheOs, Sept. 2009.**

[7] M. Hay, G. Miklau, D. Jensen, P. Weis, and S. Srivastava, Anonymizing Social Networks,Technical Report 07-19, Univ. of Massachusetts Amherst, 2007.

[8] K. Liu and E. Terzi, Towards Identity Anonymization on Graphs, Proc. ACM SIG- MOD Intl Conf. Management of Data (SIGMOD 08), pp. 93-106, 2008.

[9] E.Zheleva and L. Getoor, Preserving the Privacy of Sensitive Relationships in Graph Data, Proc.First ACM SIGKDD Intl Conf. Privacy, Security, and Trust in KDD, pp. 153-171, 2008.

[10] R. Gross, A. Acquisti, and J.H. Heinz, Information Revelation and Privacy in Online Social Networks, Proc.ACM Workshop Privacy in the Electronic Soc. (WPES 05), pp. 71-80, http://dx.doi.org/10.1145/1102199.1102214, 2005.

[11] J. Yedidia, W. Freeman, and Y. Weiss. Exploring Artifiial Intelligence in the New Millennium. Science Technology Books, 2003.

[12] Ahmadinejad, SeyedHossein, and Philip WL Fong. "On the feasibility of inference attacks by third-party etensions to social network systems." Proceedings of the 8thACM SIGSAC symposium on Information, computer and communications se- curity. ACM, 2013.

[13] S.A. Macskassy and F. Provost, Classification in Networked Data: A Toolkit and a Univariate Case Study,J. Machine Learning Research, vol. 8, pp. 935-983, 2007.

[14] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubrama- niam, L- Diversity: Privacy Beyond K-Anonymity,ACM Trans. Knowledge Discovery from Data, vol. 1, no. 1, p. 3, 2007.

[15] [15] C. Dwork, Differential Privacy, Automata, Languages and Programming, M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, eds., vol. 4052, pp. 1-12, Springer, 2006.