



International Journal of Engineering, Business and Enterprise Applications (IJEBA)

www.iasir.net

Prevent conclusion Attack by Removal of Sensitive Attribute from social Network Information

Jyoti Mhaske B.

Department of Computer Engineering, MET, BKC Adgaon, Nashik,
Savitribai Phule Pune University, Maharashtra, India.

Abstract: Online social sites have become one of the most frequent activities on the Internet. Online social sites such as Facebook are mostly access by many people for various uses. OSNs allow users to control and customize what personal information is available to other users. Such networks allow users to publish their details about themselves and to connect their friends. Some of the information revealed inside these networks is meant to be sensitive. A privacy break occurs when sensitive information about the user the information that an individual wants to keep from public is disclosed to an adversary. So it is possible to use some learning methods on released data to predict sensitive information as private information. Sensitive information leakage could be an important issue in some cases. Here the goal of system is simulate the conclusion attacks using released social networking sites data to predict sensitive attribute information. In the proposed system use of data and individual privacy presents an chance for privacy preserving social network data mining. Here in the system some sensitive data removal techniques are like anonymization of data and perturbation that could be used in different situations for preventing conclusion attack, such techniques are removing details of user profile, adding some new attribute information and manipulate some fields in the user profile these techniques are proposed for preventing conclusion attack.

Keywords: SNS, FB dataset, NB, ID3, Social network, classifier

I. Introduction

Social networking used to connect and share information with friends. People use social sites services for different reasons to join network with new contacts, reconnect with formal friends, maintain current relationships, build or promote a business or project, participate in discussions about a certain topic, or just have fun meeting and interacting with other users and it will generate very useful information by such discussions and meeting of facebook users . Social Network site and Twitter website have a broad range of users. LinkedIn has positioned itself as a professional networking site profiles include resume information and groups are created to share questions and ideas with group members in similar fields. Unlike traditional personal homepages people in these societies publish not only their personal attributes, but also their relationships with friends. It may cause the privacy violation in social networks. Information privacy is needed for users. Existing techniques are used to prevent direct disclosure of sensitive personal information. Here focus on social network data Social classification and inferring the individuals' private information. More private information is inferred by applying collective classification algorithm.

The system enhance how the online social network data could be used to find sensitive attribute from individual private trait that a user is not wish to disclose (e.g. gender identification, sexual orientation and religion related data). For example in an office people connect to each other because of similar occupations ,similar business and other profession. Therefore it is possible that one may be able to guess someone's attribute from the attributes of his/her friends. In such cases, privacy is indirectly exposed by their social relations rather than from the owner attribute or status. This is called personal information leakage from conclusion attack. [1]

The Purpose of this work is it has been proposed to design a system that show the effect of possible data sanitization approaches on hiding or preventing such sensitive information leakage, while allowing the recipient of the sanitized data to do conclusion on non-private details.

Motivation of the Proposed Approach

Providing specific use of data and individual profile privacy presents an opportunity for privacy preserving social network sites. That is the discovery of information and relationships from social site data without violating privacy .But the problem of sanitizing a user profile of social network to prevent conclusion of social sites data and then examines the effectiveness of those approaches on a user profile data set.

In order to protect privacy, sanitize both details and the underlying link structure of the graph. That is deleting some information from a users profile and remove some links between friends. In many situations the data needs to be published and shared with others. Social networks are online applications that allow their users to connect

by means of various linktypes. As part of their professional network because of users specify details which are related to their professional life. These sites gather extensive personal information, social network application providers have a rare opportunity direct use of this information could be useful to advertisers for direct marketing. In such situation need to prevent conclusion attack by using sanitization technique, sanitize the data set before release to third party.

II. RELATED WORK

Zheleva and Getoor in [9] 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 methods 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 post release.

J. He et al [4] 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.

R. Gross et al [10] 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.

Gross et al.[10] examine specific usage instances at Carnegie Mellon. Note potential attacks, such as node reidentification or stalking, that easily accessible data on Facebook could follow with. and further note that while privacy controls may exist on the users profile end of the social networking site, many individual profiles do not take advantage of this system. This finding coincides very well with the amount of data that able to crawl using a very simple HTML crawler on a Facebook network. However, need to extend on work by experimentally examining the accuracy of some types of the demographic reidentification and classification that propose before and after sanitization.

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

Hay et al.[4] consider various methods for anonymizing social networks data. However, the work focuses on inferring details attribute of nodes in the network, not individually identifying individuals as single profile attribute instead of this it infer the more than one attribute .

He et al. [4] consider methods to infer sensitive or private information via friendship links by creating a network by using Bayesian classifier from the links inside a social network. While the data crawl a real social network, LiveJournal, use hypothetical attributes to analyze learning algorithm [4].

Raymond Heatherly, et al[1] the work is based on the user profile information of social network instead hiding personal detail publish all detail but at the time of data release sanitize that data set means remove some sensitive attribute. Before handover that data set to third party for some advertise purpose it should converted into some encrypted format and release it to third party.

III. OVERVIEW OF OUR APPROACH

The system architecture of sanitization method of user profile information is show the detailed work flow of system is as shown in figure 1, how could be gather information of users profile. In that it is important to note that for any detail type, the expected response can either be single or multivalued, and that a user has the option of listing no detail values for any given detail. For example, consider user profile data as home town and activities detail type. A user can only have one home town, but can list multiple activities (for instance, soccer, reading, video games). However, a user also has the option of listing no detail values for these. For example the detail value of video games for the detail type activities will be listed as (activities, video games), to distinguish it from other details that may have the same detail value, such as (groups, video games). Further even if a user lists multiple activities, data can store each independently in a detail with the corresponding detail name. That is a user who enters jogging and swimming as his favorite activities will have the corresponding details favorite activity, jogging and favorite activity, swimming.

The Naive Bays classifier classify the user profile data into specified classes by using Nave Bayes classifier, Naive Bayes classifier improves the accuracy of classification. Classification is occurs on the basis of node and detail information of user profile data.

Details of user profile can be manipulated in some ways: As adding details to nodes of social network, modifying existing details by some modification and removing details from nodes. However here details or link information modification can be categorize by classifier into two categories: perturbation for adding something and anonymization for removing some at- tributes. Adding and modifying details can both be considered methods of perturbation-that is introducing various types of "noise" into D to decrease classification accuracies. Removing node however it can be considered an anonymization method. After removal of sensitive information it provide

the sanitized dataset for further encryption technique which convert the sanitize dataset into encrypted format for privacy concern.

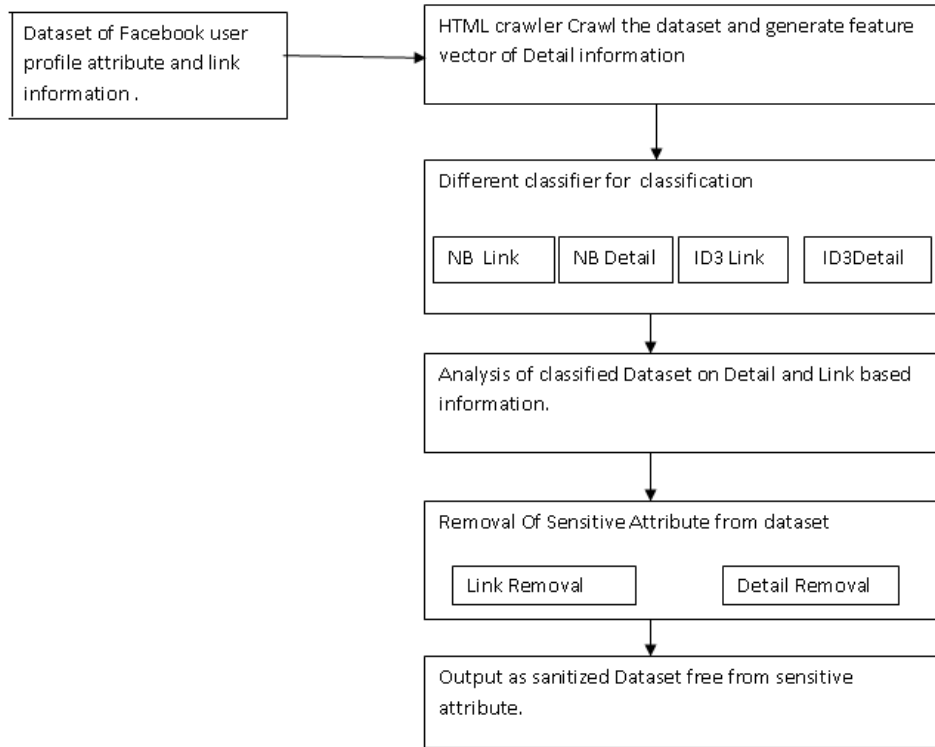


Fig. 1. System architecture of sanitization of user profile data

Naive Bays classifier is used to classify the large number user profile data according to detail and link information of user profile information. Initially friends often share common attributes (e.g. hobbies and professions). Thus, it is possible to predict someone's attributes by looking at the category of friends as their common attributes whatever he/she has. In the real world people are connected with each other via all types of relations, and a personal attribute may only be sensitive to certain types of relations like gender, and sexual orientation. For example, in order to predict someone's age, it is more appropriate to consider the ages of his/her classmates or officemates. Therefore to infer people's privacy from social relations, one must be able to filter out other types of relations between two connected people on social sites.

To solve this problem here find out the privacy conclusion in homogeneous societies where individuals are connected by a single type of social relations as heterosexual and homosexual and the impact of every person on his/her friends is the same. Homogenous societies reflect small closely related groups (such as offices, classes or clubs), where people are connected by a relatively pure kind of relationship. Real social networks can be always as the combinations of many homogeneous societies.

Determining an individual's political affiliation, gender identification, sexual orientation are an exercise in graph classification. Given a user node n_i with m details of user profile and p potential classification labels ($C_1; \dots; C_p, C_x$) the probability of n_i comes in class C_x , is given by the equation.[1]

$$\operatorname{argmax}_{1 \leq x \leq p} \frac{P(C_x^i) * P(D_1^1 | C_x^i) * \dots * P(D_1^m | C_x^i)}{P(D_1^1, \dots, D_1^m)} \quad (1)$$

To perform conclusion use Bayesian networks to show the causal relation in social networks. Specifically, if want to conclude the value of attribute A for a person (referred to as query node X), first construct a Bayesian network from some social network, and then analyse the Bayesian network to achieve the probability that X has attribute A .

However, that $P(D_1^1; \dots, D_1^m)$ is equivalent for all values of C_{xi} . That is, because the probability of seeing any particular detail without consideration of any particular class x is equivalent for all x . Thus, here need only compare to determine a new class label for n_i . [1]

$$\operatorname{argmax}_{1 \leq x \leq p} [P(C_x^i) * P(D_1^1 | C_x^i) * P(D_1^m | C_x^i)] \quad (2)$$

A. Maintaining the Integrity of the Specifications

ID3 is a simple decision tree erudition algorithm developed by Ross Quinlan (1983) [4]. The basic idea of ID3 algorithm is to create a decision tree of given set, by using top-down greedy search to check each attribute at every tree node. To select the most useful attribute using classification technique, here present a metric information gain and to catch an optimal way to classify an erudite set. The information gain metric is such a function that we can use for efficient balanced splitting. In direction to define information gain exactly, we need to deliberate entropy. First, let's assume that the resulting decision tree classifies instance into two classes without loss of simplification and we would call them P (positive) and N (negative). Given set S, containing these positive and negative targets, the entropy of S related to this Boolean classification is:

$$\text{Entropy}(S) = -P(\text{positive}) \log_2 P(\text{positive}) - P(\text{negative}) \log_2 P(\text{negative}) \quad (3)$$

P (positive): proportion of positive examples in S P (negative): proportion of negative examples in S

B. Link Classification

Collective inference is a method of classifying social network data using a mixture of node details and connecting links in the social graph. The classifiers consists of three components: a local classifier, a relational classifier, and a collective inference algorithm.

C. Local classifier

Local classifiers is a learning method that is applied in the initial step of collective inference. Naive bayes algorithm is used as a local classifier. This classifier construct a model based on the details of nodes in the training set, apply this model to nodes.

D. Relational classifier

The relational classifier is a separate method of learning algorithm that consider the link structure of the graph, and uses the labels of nodes of user profile in the training set to build a model which it uses to classify the nodes in the test set.. Four relational classifiers: class-distribution relational neighbor (cdRN), weighted-vote relational neighbor (wvRN), network-only Bayes classifier (nBC), and network-only link-based classification (nLB).

E. Hiding Private Information

To be able to formalize a privacy definition with user profile dataset, Here need to address two issues with respect to an conclusion attack. First, need to have some understanding of the potential prior information (i.e., background knowledge) the adversary can use to launch an conclusion attack. For example, if an adversary already knows all the hidden and unhidden private information related to the social network, it will be useless to try to protect against such an adversary. Second, need to analyze the potential success of conclusion attack given the adversary's background information. For example, if the adversary has only the disclosed social network data, what is the best classifier he can build to predict sexual orientation?

F. Manipulating Details

Details attribute of profile can be manipulated by three ways: adding details to user nodes, modifying existing details attribute and removing details from nodes attribute. Here details can classify these three methods into two categories: perturbation for adding manipulation details and anonymization means deleting some details. Adding and modifying details can both be considered methods of perturbation that is, introducing various types of "noise" into Details attribute to decrease classification accuracies.

G. Choosing Details

Now choose which details to remove. The choice is guided by the following definition is used for finding high probability details to remove which improve classification accuracy. Definition: Given G and a nonzero set of sensitive details I, determine the set of details $D' \subseteq D$, where $G' = (V, E, D - D')$ has the most reduction in classification accuracy for some set of classifiers C on the sensitive attributes I for the given number of removals m.

Assume a person, n_i , has the class value C_2 out of the set of classes C, and this person has public details D_i . [1]

$$\text{argmax}_{1 \leq x \leq p} [P(C_y^i) * P(D_i^1 | C_y^i) * P(D_i^m | C_y^i)] \quad (4)$$

This allows to find the single detail that is the most highly indicative of a class and remove it.

H. Manipulating link information

The other option for anonymizing social networks is altering links. Unlike details, there are only two methods of altering the link structure: adding or removing links. Assume that there are two possible classes for a node, and the true class is C_1 . Remove the links that increase the likelihood of the node being in class C_1 . Here consider that the define a node to be in class C_2 if $\beta(i)$ is positive. [1]

$$\beta(i) = P(C_2, N_i) - P(C_1, N_i) \quad (5)$$

$\beta(i)$ as the new value for above equation if the friendship link remove $F_{i,j}$. here need to compute $\beta_j(i)$ as

$\beta(i)$ and Z are constants for all $\beta_j(i)$ the best choice for i that maximizes $\beta(i)$ becomes one that maximizes [1]

$$M_i = (p(p(C_2|F_{i,j}) - p(C_1|F_{i,j})) * W_{i,j}) \quad (6)$$

IV. IMPLEMENTATION STRATEGY

A. Dataset

Input for system is Users profile information of social network and Network consisting of only nodes and edges Detail values of nodes i.e user profile details are provided as input to this Naive bays classification. The facebook dataset is extract by log in to user accounts and download their profiles as .html files. Now apply html parser to that parses HTML files and collects attribute values of user profiles and store the results in database.

B. Result analysis

System Output is the data of user profile information those data is in well classified manner. Those data are ready to release to the third party for their advertising purpose .The user profile data set is without sensitive attribute means the release data set is does not contain sensitive attribute so conclusion attacks are prohibited. The effect of removing details and links in preventing sensitive information leakage.

C. Result of classifier accuracy

Bayesian classification provides practical learning algorithms and prior knowledge and observed data can be combined. It provides a useful perspective for understanding and evaluating many learning algorithms. And also calculates explicit probabilities for hypothesis and it is robust to noise in input data. Bayesian reasoning is particularly suited when the dimension-ality of the inputs is high. It is applied to decision making and inferential statistics that deals with probability inference, used to predict future events. It requires a small amount of training data to estimate the parameters is the advantage. After giving the facebook dataset from crawler to the classifier as Naive Bays classifier and ID3 classifier that classifier calculate the classification accuracy before any alteration to the dataset. This classification accuracy metric changes is showing the efficiency of this system.

ID3 Algorithm is good at dealing with categorical attributes. When dealing with the multiple attributes in the decision tree, then the split point for the decision tree is going to be computed using the measure from information theory called Information Gain, which is known as an attribute selection method for the ID3 algorithm. Here calculate the accuracy by different algorithms of classification and first calculate the accuracy of correct classified dataset by both algorithm is about 83% accuracy of correct classification of dataset. The classifier accuracy are reduces after removing the sensitive attribute its about 53%. This classification on the basis of gender ,relationship status and friendship link information of the facebook profile data.

sensitive attribute details Here the dataset is collected from facebook users profile the information about their basic contact information. This information contains the attribute as Interest in field as interest in men ,women and both and marital status of the user as is that person is married ,single, in relationship ,engaged, and last detail about their gender information as male or female. The following table is contain the information about the details of 11 users profile of facebook. In table "0" means the value of that detail is Null, "1" means value is positive of that details. Gender "1" indicate Male and "2" indicate female.

Load Data :	LOAD!!	IN : Interested In		RS: RelationShip Status :		Gender : Men-1 Women-2				
Node-Name	IN-MEN	IN-Women	IN-MW	RS-Single	RS-In RS	RS-Engagred	RS-Married	RS-Complicated	RS-OPen	Gender
1	1	0	0	1	0	0	0	0	0	2
2	0	1	0	1	0	0	0	0	0	1
3	0	1	0	0	0	0	1	0	0	1
4	0	0	1	1	0	0	0	0	0	1
5	0	1	0	1	0	0	0	0	0	1
6	0	0	1	1	0	0	0	0	0	2
7	1	0	0	1	0	0	0	0	0	2
8	0	1	0	1	0	0	0	0	0	1
9	1	0	0	0	0	0	0	1	0	2

Fig. 2. Vector generation of Dataset

Here test some user data by classifier in the two cases first case check the correctness of classified dataset before any changes occurs to dataset ,and In second case check the correctness after removal of some attribute from dataset. The accuracy of different classifier shown in following figure.

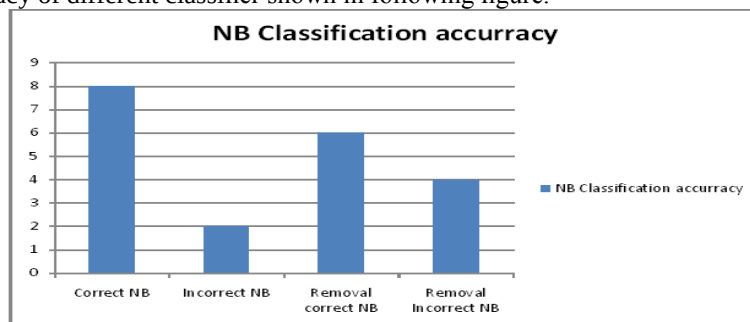


Fig.3 Naïve Bays Classifier Accuracy

In above first graph show the Naive Bays classifier accuracy after remove the some sensitive attribute or deleting some sensitive link information from dataset. Graph contains the correct classified accuracy 83 %before any manipulation on dataset ,after removal sensitive attribute the accuracy is reduce upto 53%. In above second graph show the ID3 classifier accuracy after remove the some sensitive attribute or deleting some sensitive link information from dataset. Graph contains the correct classified accuracy 80 %before any manipulation on dataset ,after removal sensitive attribute the accuracy is reduce upto 40%.So it is very helpful for preventing inference attack on dataset.

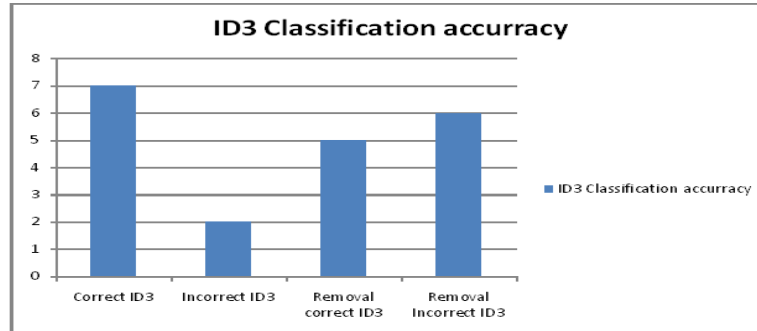


Fig. 4. ID3 Classifier Accuracy

V. CONCLUSION AND FUTURE WORK

The System is use for preventing conclusion attack on user profile data of social network. The proposed system is using both friendship links and details together gives better predictability than details alone. In addition implement the effect of removing details and links in preventing sensitive information leakage. Here show that each of these methods provides a measure of privacy guarantee for users within the network, but can also be used by third parties for classification on non-sensitive attributes. In future the system can extended for prevent private information conclusion attack is by providing user profile information to third party in encrypted format for maintaining privacy for user profile data.

REFERENCES

- [1] "Preventing Private Information Inference Attacks on Social Networks Raymond Heatherly, Murat Kantarcioglu, and Bhavani Thuraisingham," Fellow, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 8 AUGUST 2013.
- [2] J. Lindamood, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, Inferring Private Information Using Social Network Data, Proc.18th Intl Conf. World Wide Web (WWW), 2009.
- [3] 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
- [4] J. He, W. Chu, and V. Liu, Inferring Privacy Information from Social Networks, Proc. Intelligence and Security Informatics, 2006.
- [5] K.M. Heussner, Gaydar n Facebook: Can Your Friends Reveal Sexual Orientation ABC News, <http://abcnews.go.com/Technology/gaydar-facebook-friends/story?id=8633224>. UZ939UqheOs, Sept. 2009.
- [6] M. Hay, G. Miklau, D. Jensen, P. Weis, and S. Srivastava, Anonymizing Social Networks, Technical Report 07-19, Univ. of Massachusetts Amherst, 2007.
- [7] K. Liu and E. Terzi, Towards Identity Anonymization on Graphs, Proc. ACM SIGMOD Intl Conf. Management of Data (SIGMOD 08), pp. 93- 106,2008.
- [8] J. He, W. Chu, and V. Liu, Inferring Privacy Information from Social Networks, Proc. Intelligence and Security Informatics, 2006.
- [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 Artificial Intelligence in the New Millennium. Science Technology Books, 2003.
- [12] N. Talukder, M. Ouzzani, A.K. Elmagarmid, H. Elmeleegy, and M. Yakout, Privometer: Privacy Protection in Social Networks, Proc. IEEE 26th Intl Conf. Data Eng. Workshops (ICDE 10), pp. 266- 269, 2010.
- [13] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramanian, L-Diversity: Privacy Beyond K-Anonymity, ACM Trans. Knowledge Discovery from Data, vol. 1, no. 1, p. 3, 2007.
- [14] 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.
- [15] A. Friedman and A. Schuster, Data Mining with Differential Privacy, Proc. 16th ACM SIGKDD Intl Conf. Knowledge Discovery and Data Mining, pp. 493-502, 2010.
- [16] C. Clifton, Using Sample Size to Limit Exposure to Data Mining, J. Computer Security, vol. 8, pp. 281-307, <http://portal.acm.org/citation.cfm?id=371090.371092>, Dec. 2000.
- [17] K. Tumer and J. Ghosh, Bayes Error Rate Estimation Using Classifier Ensembles, Intl J. Smart Eng. System Design, vol. 5, no. 2, pp. 95-110, 2003.
- [18] C. van Rijsbergen, S. Robertson, and M. Porter, New Models in Probabilistic Information Retrieval, Technical Report 5587, British Library, 1980.
- [19] D.J. Watts and S.H. Strogatz, Collective Dynamics of Small-World Networks, Nature, vol. 393, no. 6684, pp. 440-442, June 1998.
- [20] L. Sweeney, k-Anonymity: A Model for Protecting Privacy, Intl J. Uncertainty, Fuzziness and Knowledge-based Systems, pp. 557-570, 2002.

Acknowledgments

Very much thankful to all authors; those are mentioned in the references and all the respected peoples who helped for designing and development of system work.