A privacy-preserving model to control social interaction behaviors in social network site

Sanaz Kavianpour
Ali Tamimi
Bharanidharan Shanmugam

A privacy-preserving model to control social interaction behaviors in social network sites

Sanaz Kavianpour[a,1], Ali Tamimi[b], Bharanidharan Shanmugam[c]

[a]*Abertay University, Dundee, Scotland, UK*

[b]*Washington State University, Pullman, WA, USA*

[c]*Charles Darwin University, Darwin, Australia*

Abstract

Social Network Sites (SNSs) served as an invaluable platform to transfer information across a large number of users. SNSs also disseminate users data to third-parties to provide more interesting services for users as well as gaining profits. Users grant access to third-parties to use their services, although they do not necessarily protect users' data privacy. Controlling social network data diffusion among users and third-parties is difficult due to the vast amount of data. Hence, undesirable users' data diffusion to unauthorized parties in SNSs may endanger users' privacy. This paper highlights the privacy breaches on SNSs and emphasizes the most significant privacy issues to users. The goals of this paper are to i) propose a privacy-preserving model for social interactions among users and third-parties; ii) enhance users' privacy by providing access to the data for appropriate third-parties. These advocate to not compromising the advantages of SNSs information sharing functionalities.

Keywords

Anonymization; Classification; Privacy; Social interaction behaviors; Social network sites

1. Introduction

Social network sites (SNSs) have become a significant and inevitable part of online social interactions for more than half a billion users worldwide [1]. SNSs are virtual spaces that allow users to initiate modern interactions. Their popularity is due to the opportunity they give to the users to create unlimited profiles and to share personal information, to forge new relationships using online dating capabilities and to have fun using the countless option of online activities. Furthermore, some organizations used SNSs to establish a community for professional or business collaborations to share knowledge among their employees and to update the organizations current events or ongoing programs [2][3].

The number of SNSs' users play a prominent role in ensuring their success [4]. Hence, SNSs providers should offer interesting features and facilities to attract more users. To fulfill this fundamental requirement, SNSs provide a platform for third-party developers to run their applications and provide services such as gaming and fortune telling for the users. Third-Party Applications (TPAs) require accessing the users' profile data to provide the numerous services available. The users' profiles embody a vast source of personal information such as

[1] Corresponding author email addresses:
sa.kavianpour@gmail.com
s.kavianpour@abertay.ac.uk

identification information, demographic and other sensitive data [5]. Unsolicited exposure of the personal information may lead to a breach of privacy matters [6].

Users' data are assembled and maintained by the social network service providers under a single administrative domain [7]. Although SNSs have privacy setting options to protect users' data privacy, there are not adequate to preserve users' privacy as they are confusing and not transparent enough for all users, especially naive users. For instance, 88% of Facebook users have a general comprehension of the messages which appear in the dialogs to ask permissions [8]. The potential sensitivity of users data and the lack of existing privacy setting techniques makes privacy an explicit issue [9]. Hence, privacy is a significant key element for SNSs to protect users' data from unauthorized parties as protecting users' data is one of the biggest challenges in SNSs.

This section introduces the paper while the following Section 2, describes the problem statement. Related works are explained in Section 3. Section 4, presents the proposed privacy-preserving model in details. The experimental results are discussed in Section 5. The paper concludes with a discussion of directions for future work in Section 6.

2. Problem statement

The ubiquitous usage of SNSs enhances the growth of the amount and sensitivity of users' data that is accumulated and disseminated in SNSs [10]. This data is a significant target for TPAs. The vast information exchange to TPAs may pose risks to SNSs' users. First, a TPA can be malicious and gather a high volume of user data further than the required usage. It was stated that 91% of TPAs on SNSs have accessed to data which they do not require for operation [11]. Second, SNSs policies can be violated by TPAs developers to control user data. SNSs have a set of rules that are termed as developer policies which should abide. These rules prevent developers from abusing personal information or disseminating it to other parties. Reported incidents illustrated that TPAs violated these policies [12].

Users are mostly unaware of the information storage and utilization by TPAs [13][14]. They tend to use and trust these TPAs by sharing their personal information in good faith. Accessibility to users' private data is not an issue of TPAs. The substantial issue is in the way of users' data usage as TPAs can store, exchange and abuse their accesses [15]. SNSs platforms employ user consent permission systems that limit their control over TPAs because of the coarse-grain granularity of permissions. These systems are in contrast with the principle of minimal privileges which should be granted to TPAs to fulfill their task [16]. Although permissions are required to run the application, they are not clear how and when they are used.

All interactions between TPAs and users in SNSs is encapsulated by Application Programming Interface (API). This API designed without an access control mechanism which is a significant technical issue. Although many previous types of research have been done on SNSs access control between users in the platforms, the access control of TPAs in SNSs are still inadequate. Hence, this research intends to propose a privacy-preserving model which enhance privacy within social interaction behaviors. Social interaction behaviors denote the interactions among TPAs and SNSs users in this research. It is intended that the proposed model preserves users' privacy and mitigates information leakage without users interference.

3. Related work

Privacy disclosure arises when social network data published by other parties such as researchers and advertisements [17]. Proposing and developing privacy-preserving models to overcome privacy issues in regards to users' data are significant in the SNSs researches [18][19]. Blosser and Zhan [20] presented protocols to create and interact with privacy-preserving collaborative social networks. Their scheme integrates small networks while retaining the data purity for the owners. Campan et al. [21] introduced a greedy approach (SANGREEA) to optimize utility employing the attribute and structural information simultaneously. Guha et al. [22] proposed a mechanism entitled NOYB that provides fine-grained control for users' privacy employing encryption to provide privacy and only authorized users were able to decode and decrypt the result. It applies on the Facebook, and the results describe that it is practical, feasible, and no cooperation is required from online services. Fong et al. [23] designed an access control model which formalizes and generalizes the Facebook privacy protection mechanism. Zhu et al. [24] proposed a collaborative framework for access control in social networks using innovative key management.

Shakimov et al. [25] employed a Virtual Individual Server (VIS) running in a paid compute utility to preserve location privacy. Masoumzadeh and Joshi [26] proposed new methods, which enhance edge-perturbing anonymization based on the structural roles and edge betweenness in social network theory. To prevent many security concerns regarding online personal disclosure, Fire et al. [27] developed the social privacy protector software that entails three protection layers for enhancing Facebook users' privacy via implementation of diverse methods. It identifies a user's friends who might pose a threat and limit their access to the user's personal information in the first layer. In the second layer, Facebook's basic privacy settings according to various types of social network usage profiles are deployed. The third layer alerts the users about the number of installed applications that have access to their Facebook private information. Its evaluation on 74 Facebook users shows that it is effective in limiting 392 friends access to users' personal information.

Heathely et al. [28] examined and illustrated the effect of removing details and links in preventing sensitive information leakage. Cheng et al. [29] proposed an access control framework, which provided control over TPAs access to users' data and activities in SNSs while sustaining the TPAs functionality. This approach provided access for TPAs with regards to user-specified policies without any transmission of data to TPAs. Although this model provided better controllability for users to preserve their privacy, it was not able to remove privacy issues completely. Furthermore, it kept away users' private information from external TPAs completely, which can affect TPAs functionality. Sun et al. [30] proposed a privacy-preserving method for sharing data in social networks. This method provides effective revocation to hinder a contact's access to the private data once the contact is removed from the social group and can be used as a plug-in for Facebook.

Privacy-preserving models usually apply tasks including masking, modifying and generalizing on the original data to protect privacy while sustaining data utility. There are various models for preserving the privacy of micro-data that have been used for social network data as well [31]. Anonymity is the best privacy protection technique with the least effect on data quality [32]. The focus of anonymity is on two principles [33]. First, to design better anonymity methods which preserve privacy as well as retaining practical data utility. Second, to develop more efficient anonymity algorithms that can fulfill the requirements. Various anonymization techniques comprise generalization, suppression, anatomization, permutation and perturbation [34]. Generalization is the most used technique. The most employed models which provide well outcomes in anonymization are *k*-anonymity [35], *l*-diversity [36] and *t*-closeness [37]. The *k*-

anonymity, *l*-diversity and integrated approach of *k*-anonymity *l*-diversity have been used to preserve users' data privacy while publishing it online by several researchers as follows.

Campan et al. [38] employed the community detection algorithm based on modularity quality function by which the community structure of the original networks was preserved. Tassa and Cohen [39] used the sequential clustering algorithms and centralized setting for anonymizing SNSs. In weighted social networks, *k*-anonymity applied by Skarkala et al. [40] that was effective against attacks when an adversary has information about the network.

Yuan et al. [41] proposed a *k*-degree *l*-diversity anonymity model that considers the protection of structural information and sensitive attributes of users. This model employed both *l*-diversity and recursive (*c, l*) - diversity. The noise node-adding algorithm was designed to construct a new graph from the original graph with the least distortion on graph properties. The experimental results of the model illustrated that the developed noise node adding algorithms outperforms other algorithms used in previous work according to edge editing. Although the algorithm was effective, it caused perturbation in the graph. Moreover, in a distributed environment, this model cannot preserve privacy as an attacker can exploit users' data via the combination of the published data by various publishers. Chakraborty et al. [42] found out some shortcomings in *k*-degree-*l*-diversity anonymity model proposed by [41]. Hence, they provided an enhanced algorithm to overcome those weaknesses. The proposed algorithm generates the anonymized graph with a minimum number of noise nodes while maintaining the structural property of the original graph and preserving the anonymized graph data efficiency.

There are various models which were proposed for privacy-preserving data publishing to mitigate information disclosure and protect users' privacy. Although these privacy models are enforced, an attacker may still extract one's private information when data publishers or groups disclose sensitive attributes. Hence, this motivates researchers to propose and develop new models to provide more secure models with a better utility of released data. Next section presents a new privacy-preserving model in details.

4. Proposed model

A new privacy-preserving model is proposed for social interactions among SNSs users and third-parties. The components of the model consist of the classification algorithm, the anonymization algorithm, and the anonymized database. All these components located in the anonymity service which needs to be embedded in the SNSs server to play an intermediate role between the users and third-parties to control social interactions. Fig. 1 depicts the schema of the model.

The operation process of the proposed model involves two main steps. Once a third-party sends a request for the users' data, the request will be passed to anonymity service. In the first step, the classification algorithm classifies the third-party according to its attributes values to assign it to an accurate pre-defined class and to detect malicious and non-malicious interactions. In the second step, when the third-party assigned to its accurate class, anonymization algorithm provides access to an anonymized database based on its class authority. Therefore, the requested data will return to third-party based on its class authority.

4.1. Data collection

We developed an application to extract users profile data from Facebook which used as input data for the anonymization algorithm. The developed application is written in C# and provided web messages for users to send a message from the online web. After Facebook approval, the

application extracted users' data by their consent.Our voluntary participants were friends and friends of friends who run the application to fulfill the requirements of data for the experiment. The data collected from 1500 users profile data from August to November 2016.

4.2. Implementation details (algorithms skeleton)

This section illustrates the main components of the proposed model in details.

4.2.1. Classification algorithm

The first component of the model is the classification algorithm. The applied classification algorithm roots in decision tree learning [43] and it is an optimized implementation of the C4.5

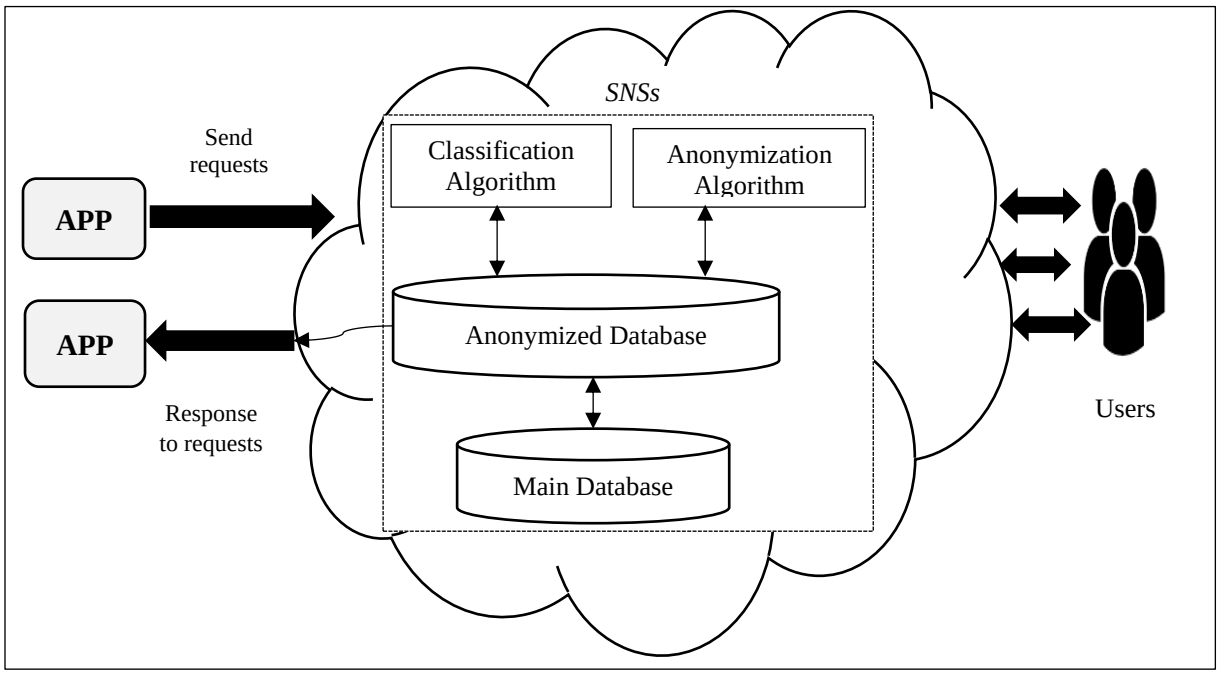

Fig.1. Proposed privacy-preserving model.

algorithm. Decision tree creates a model with rules that are human-readable and interpretable. The classification algorithm has two phases as model construction and use of the model.

- ***Model construction.*** Third-parties commonly interact with SNSs users through applications. All TPAs have some features that are available on their description pages. Thus, preliminary, the classification algorithm searched for TPA features automatically by crawling the generic application page for each application identifier, fetched available information and perceived the URL redirection behavior. Among all features, application category, rating, required permission set, external link: to post ratio and website reputation score (WOT) are selected as they often assist more in detecting malicious applications [44]. These features are independent variables and are shown in Fig.2 by the values details. The gathered information which makes the training dataset is used for model construction and defines a set of pre-defined classes. Class and access are pre-determined as dependent variables. Five different classes are defined and labeled in the algorithm for TPAs based on the access levels as i) Class A: Full access; ii) Class B: High Access; iii) Class C: Moderate Access; iv) Class D: Low Access; and v) Class E: Rejected (No Access) [45].

Hence, the model is constructed based on the information gathered from the training dataset with the pre-determined classes. The most significant independent variable (feature) needs to be identified to be assigned as the root node and then split other independent variables accordingly. Algorithm 1 presents the classification.

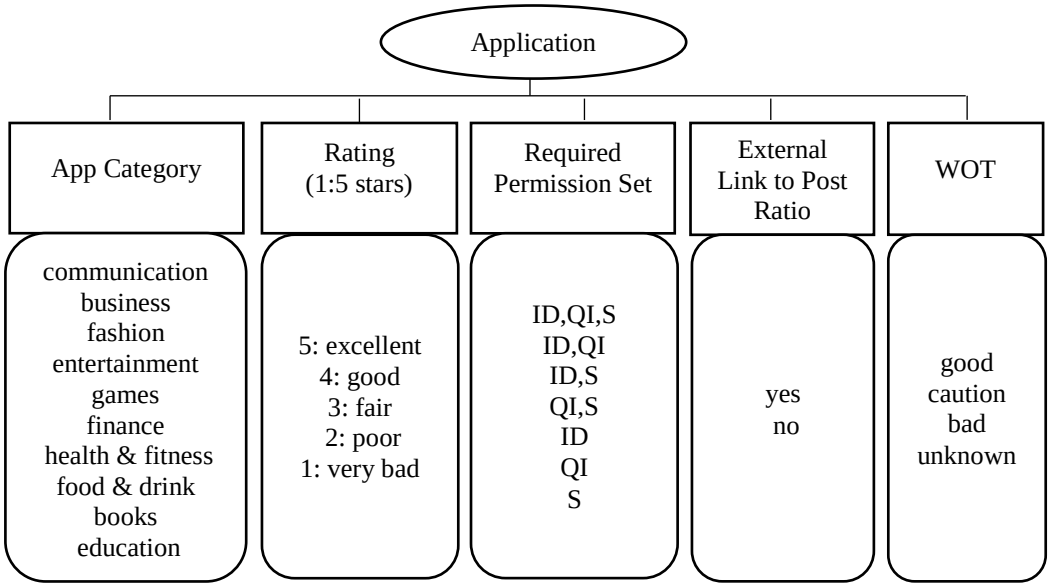

Fig. 2. Application features and values.

- ***Use of the model.*** The constructed model is used to classify an unknown sample from the test set. The classification algorithm classifies data in regards to the features in the training dataset to predict unknown samples. It analyses and compares TPA features with the training set. Then, will assign TPA class authority (class label) and will grant access to the requested users' data accordingly. Table 1 depicts a sample of a training dataset for the constructed decision tree and its classification rules portrayed in Fig.3.

Table1 Sample of a training dataset.

App Category	Rating	Required Permission Set	External Link to Post Ratio	WOT	Access	Class
business	4	ID,QI	no	good	high	B
communication	5	QI,S	no	good	high	B
games	2	QI	yes	unknown	rejected	E
business	4	QI,S	yes	caution	moderate	C
business	2	QI	no	caution	low	D
entertainment	2	QI	yes	bad	low	D
business	4	QI,S	no	good	high	B
games	4	ID,QI,S	no	caution	moderate	C
communication	2	QI	yes	bad	low	D
fashion	2	ID,QI	yes	unknown	rejected	E

Constructed Model (Decision Tree)	Classification Rules

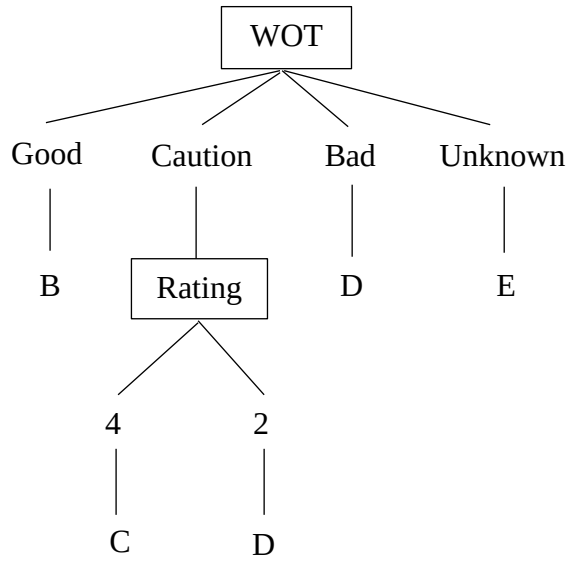	**if** *WOT== "Good"* **then**
	Return B
	if *WOT=="Bad"* **then**
	Return D
	if *WOT== "Unknown"* **then**
	Return E
	if *WOT== "Caution"* **then**
	if *Rating*== 4 **then**
	Return C
	if *Rating*= =2 **then**
	Return D

Fig. 3. Decision tree and its classification rules.

Algorithm 1 Classification Algorithm

```
1: c ← Class-of (first-instance)
2: same-class ← True
3: for each instance in training-set do
4:       if (Class-of (instance) ≠ c) then
5:           same-class ← False
6:           break
7:       else
8:            RETURN c
9: if  (same-class) then
10:      A ← Choose-best-attribute(training-set)    • select the attribute which
       is more powerful in classification
11:      T ← Generate-Tree(training-set, A)     • generate tree of training set
       based on value of A
12:      Trace(T )     •   Trace is a recursive function which is explained below
13:
14: - - - - - - - - - - - - - - - - - - - -Trace Function- - - - - - - - - - - - - - - - - - -
15: procedure Trace(T )
16:      B← Branches(T )   • Branches function return the branches of root of
       Tree in an Array
17:       for each b in B do
18:            if (Branches(b) == null) then
19:                 RETURN b
20:            else
21:                 RETURN Trace(b)
```

4.2.2. Anonymization algorithm

The second component of the model is the anonymization algorithm. According to the graph theory, the social network can be a graph G (N, E, A). N is a set of vertices (nodes) that represents the users in the network and E is a set of edges (links) that represents the relationships between users [46]. A is a set of attributes (A= ID, QI, S) for each node in the graph consist of Identifiers (ID), Quasi-identifiers (QI) and Sensitive (S) attributes [47]. The proposed anonymization algorithm roots in two most popular concepts, known as *k*-anonymity and *l*-diversity. This algorithm provides three different access levels of anonymization, namely high access, moderate access, and low access; each level is considered for a specific third-party class as shown in Table 2.

Table 2 Access levels.

Level	Attribute	TPA Class
1: high access	$ID = \{ID_1, ID_2,..., ID_n\}$ $QI = \{QI_1, QI_2,..., QI_n\}$ $S= \{S_1, S_2,..., S_n\}$	B
2: moderate access	$QI = \{QI_1, QI_2 ,..., QI_n\}$ $S= \{S_1, S_2,..., S_n\}$	C
3: low access	$QI = \{QI_1, QI_2,..., QI_n\}$	D

The algorithm searches in the dataset to find the most similar users in regards to quasi-identifiers to assign them to the same group. The goal of clustering is to diminish the amount of generalization that is required to be done on data to provide anonymity and consequently, reduce the amount of data distortion. Generalization should have a constraint as vast generalization will alleviate the data value and effectiveness.

l-diversity algorithm substitutes a sensitive attribute with *l* well-represented sensitive values to provide diversity in the sensitive attributes. In this case, the entropy of the data set should be at least log (1). The last part of anonymization algorithm evaluates the privacy score in sharing the disclosed data in the context of sensitive information. In this algorithm, all ID and S attributes are considered as sensitive profile items. A third-party request will be checked for any sensitive information. Level 1 is considered for third-parties from class B which are eligible for high access to users' data upon requests. A third-party from class B can request for all three types of attributes of ID, QI, and S as there is no elimination of attributes at this level. The anonymization algorithm calculates the percentage of privacy leakage of a request ($P_{(plr_i)}$) and compares the result with the percentage of privacy leakage in level 1($P_{(pll_i)}$) [48]. If it is less than the percentage of privacy leakage in level 1, the anonymization algorithm will grant access to the third-party to level 1. Otherwise, it will send the request to level 2 which is anonymized. The percentage of privacy leakage ($P_{(pl)}$) is calculated in the following Equation.

$$P_{(pl)} = \frac{\alpha}{\beta} * 100$$

α is the sensitivity of i the sensitive profile item and β is the total sensitivity of all the n items.

Level 2 is for third-parties from class C, which is authorized for moderate access to users data. A third-party from class C can request for just two types of attributes QI and S as identifiers are removed at this level to diminish the access to users data. Similar to level 1, the anonymization algorithm calculates the $(P_{(plr_i)})$ and compares it with the percentage of privacy leakage in level 2. If $(P_{(plr_i)}) \leq (P_{(pll_2)})$, it will get access to level 2. Otherwise, it will be sent to level 3.

In level 3, identifiers and sensitive attributes are removed, so only the quasi-identifiers are available which are anonymized. Third-party from class D which is qualified for low access to users' data will get access to level 3. Thus, various third-parties grant access to different levels of anonymity based on their class authority. Algorithm 2 delineates anonymization algorithm.

Algorithm 2 Anonymization Algorithm

```
1: for i=1 to max(level) do
2:     if Sensitivity-request ≤ Sensitivity-level(i) then
3:         RETURN (Access to level(i))
4:     else
5:         Message (Pass request to level(i+1))
```

5. Experimental results

A set of experiments evaluating the effectiveness and feasibility of the proposed model and applied algorithms are conducted. The employed classification algorithm evaluated on a machine with a 4.0 GHz Intel Pentium processor, 8 GB of RAM and Weka 3.8. Weka requires the Attribute Relation File Format (ARFF) for the selected variables (attributes) under process. The sample of training data in an ARFF file in weka is presented in Fig. 4.

```
@relation
@attribute application-category
        {communication,business,entertainment,finance,fashion,games,
         health&fitness,food&drink,book,education}
@attribute rating                          {5,4,3,2,1}
@attribute required-permission-set         {ID-QI-S,ID-QI,ID-S,QI-S,ID,QI,S}
@attribute external-link-to-post-ratio     {yes, no}
@attribute website-reputation-score        {good, caution,bad,unknown}
@attribute class                           {A,B,C,D,E}
@attribute access                          {full,high,moderate,low,rejected}
@DATA
communication,4,ID-QI,no,good,B,high
fashion,2,ID-QI,yes,unknown,E,rejected
communication ,4,ID-QI-S,no,good,B,high
```

Fig.4. ARFF variables.

Total 150 instances from the gathered dataset from Facebook application were engaged in the experiment. After being processed in Weka, the following described results were obtained as shown in Table 3.

Table 3 Results for three class test.

Class	TP	TN	FP	FN	TPR %	FPR %	Accuracy %	Time (s)
B	20	15	2	3	86.9	11.7	87.5	
C	25	13	15	7	78.1	53.5	63.3	0.08
D	25	11	5	9	73.5	31.2	72	

Table 2 demonstrates that from total 150 instances, 40 instances classified as class B, 60 instances classified as class C and 50 instances classified as class D. The number of relevant instances that were correctly classified (TPR) by the developed algorithm is about 86.9 percent for class B, 78.1 percent for class C, and 73.5 percent for class D. The number of incorrect classifications of relevant instances from all irrelevant instances that is denoted by FPR is about 11.7 percent for class B, 53.5 percent for class C, and 31.2 percent for class D. The classification accuracy for class B is about 87.5 percent, class C is 63.3 percent, and class D is 72 percent.The execution time is 0.08 in seconds.

The receiver operating characteristics (ROC) space of the three prediction class instances is plotted in Fig. 5, to visualize the performance of the classifier by plotting sensitivity or (TPR) on the Y-axis and (1-specificity) or (FPR) on the X-axis. Instances are in the upper side of the diagonal line which denotes well classification results with the least impurity or uncertainty in data. A suitable features selection results in an accurate assigning of all unknown samples to the pre-defined classes.

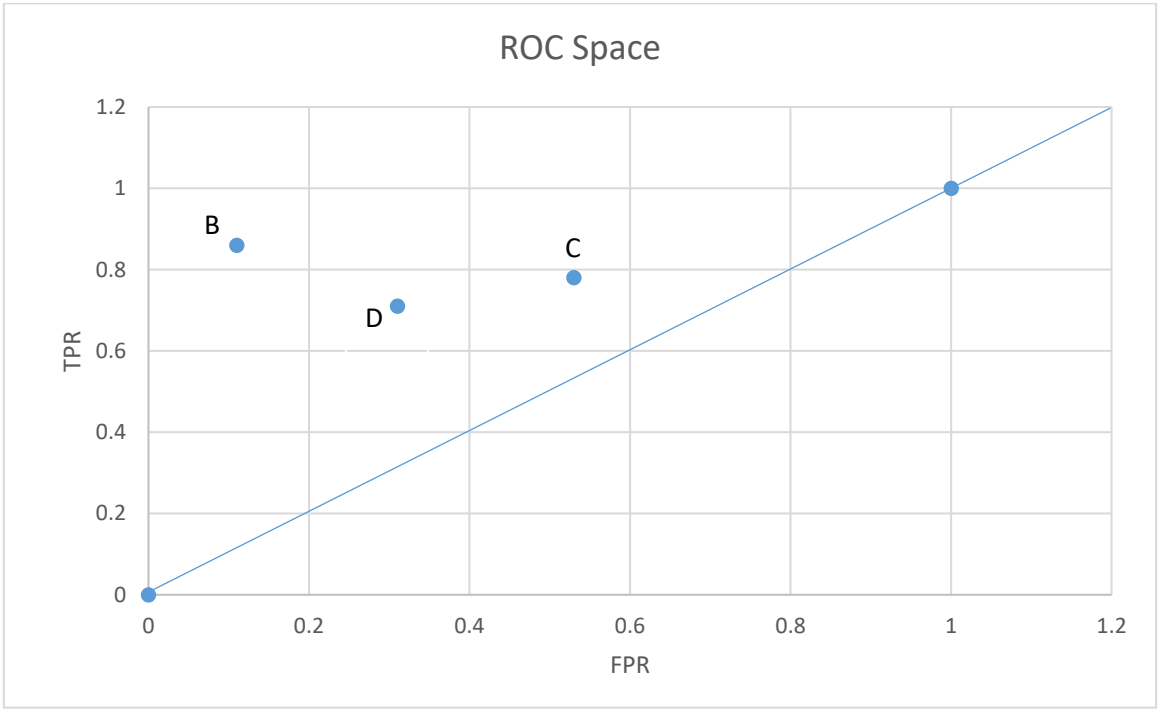

Fig.5. ROC plot.

The performance of the developed classification algorithm is compared with conventional classification algorithms ID3, C4.5, and CART. Table 4 illustrates the outcomes of all classification algorithms tested on the same dataset. The developed classification algorithm outcomes indicate the highest TPR with the weighted average about 79.5 % and the lowest FPR with the weighted average about 32.1 % with 10 folds cross-validation.The execution time is 0.08 in seconds. The TPR value shows that most instances are classified correctly. Hence, the developed classification algorithm outperforms the conventional classification algorithms in terms of TPR and FPR. Furthermore, the developed algorithm represents the highest accuracy of 74.2 % with about 79.23 % correctly classified instances and 20.77 % incorrectly classified instances. Fig.6 depicts the percentage of correctly and incorrectly classified instances of all the classification algorithms.

Table 4 Results of classification algorithms.

Decision Tree Algorithm	TP	TN	FP	FN	TPR	FPR	Class	Time(s)	Accuracy(%)
ID3	10 13 10	8 17 16	16 15 19	8 10 13	0.555 0.565 0.434	0.666 0.357 0.542	B C D	0.01	47.3
C4.5	17 21 18	4 8 16	10 17 15	9 10 8	0.653 0.677 0.692	0.714 0.680 0.483	B C D	0.01	54.6
CART	15 22 12	9 8 10	13 10 14	8 9 11	0.652 0.709 0.521	0.590 0.555 0.583	B C D	0.24	53.7
Developed Classification Algorithm	20 25 25	15 13 11	2 15 5	3 7 9	0.869 0.781 0.735	0.117 0.535 0.312	B C D	0.08	74.2

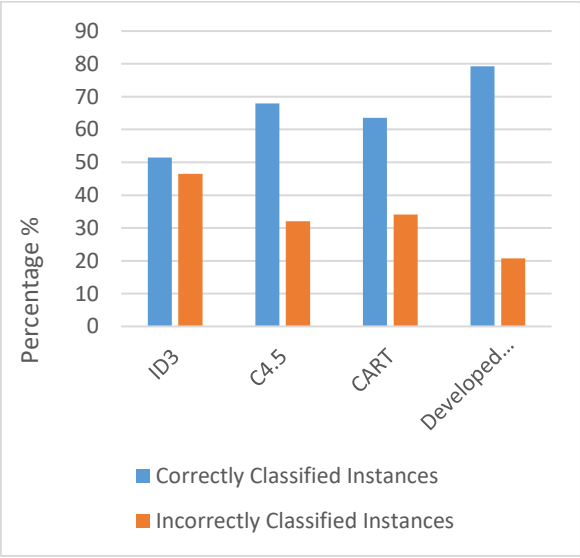

Fig. 6. Results of decision tree algorithms.

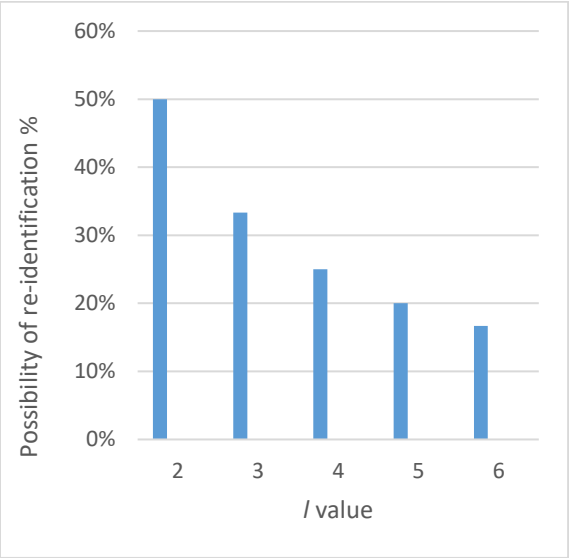

Fig.7. Possibility of re-identification in regards to *l* value.

The collected data from Facebook users' profiles by our developed application described in Section 4.1, were employed for the experiment as an input for the developed anonymization algorithm. This algorithm provides three different access levels which result in less anonymization. The thresholds for the anonymization algorithm were defined as follows. $k \geq 2$ that describes each record should appear at least k times in the equivalent cluster in regards to quasi-identifiers. $l > 2$ that illustrates the sensitive attribute values in each cluster should appear more than two times to satisfy diversity for sensitive attributes. $l = 2$ is also possible, where the appearance of the sensitive attribute values are not too frequent.

By the increment of k value, the amount of information loss increases substantially. This increase is because of the maximum generalization in quasi-identifier attributes which results in the data accuracy reduction. There is a correlation between the defined generalization level of attributes and the data utility. If generalization level increases, amount of information loss will increase, and data utility will decrease accordingly. Generally, information loss increases gradually across all k values as the k value increment results in less conceivable clusters in the dataset. Hence, the generalization level will increase to higher intervals to match remaining records in the equivalent clusters.

Fig.7 delineates that the possibility of extracting a specific users data is minimized by the enhancement number of l and via three different access levels. The developed algorithm is robust against homogeneity and background knowledge attacks through diversity in sensitive attributes and privacy score management. The provided three different levels of access with accurate anonymization control the similarity relation between anonymized and background information to mitigate the possibility of re-identification.

6. Conclusion and future work

SNSs success depends on the number of users which can be achieved by appending interesting features and facilities to attract more users. To fulfill this requirement, SNSs enable TPAs to enhance the user experience on these platforms. Users grant access to third-parties to their profile data which may threaten privacy as third-parties do not necessarily protect data the same as social network service providers would. Lack of control over the transmission of data to TPAs and inadequate privacy setting options in SNSs leads to privacy leakage and re-identification.

SNSs can employ the outcomes of the evaluated privacy model in this research to offer a safe platform with high accuracy in detecting malicious social interactions to enhance users' privacy via interactions with TPAs. The proposed privacy-preserving model performs well in practice as it controls the dissemination of users' data, thus, protecting users' privacy in addition to sustaining TPAs' functionalities. It provides anonymity for users to alleviate the possibility of information leakage and re-identification when users' data is accessible for TPAs. The proposed model is automatically applicable in SNSs with the least users' interference. SNSs service providers can increase their revenue by extending their social network usage by providing a secure space for information sharing and communication, which will attract more users. As the goal of this paper is to prevent users data diffusion to unauthorized parties and protect users' privacy, evaluating the proposed model on a real social network if it could get authorize from a social network administrator can be followed up with further work into how to put these into practice.

References

[1] R. Gu, L.-B. Oh, K. Wang, Developing user loyalty for social networking sites: a relational perspective, Journal of Electronic Commerce Research 17 (1) (2016) 1.

[2] P. Gundecha, H. Liu, Mining social media: a brief introduction, Tutorials in Operations Research 1 (4) (2012) 1-17.

[3] R. Zafarani, W. D. Cole, H. Liu, Sentiment propagation in social networks: a case study in livejournal, in: International Conference on Social Computing, Behavioral Modeling, and Prediction, Springer, 2010, pp. 413-420.

[4] M. Beye, A. J. Jeckmans, Z. Erkin, P. Hartel, R. L. Lagendijk, Q. Tang, Privacy in online social networks, in: Computational Social Networks, Springer, 2012, pp. 87-113.

[5] A. M. Kumar, B. N. Sharma, S. K. Shrivastava, Online social networks: Privacy challenges and proposed security framework for facebook, International Journal of Soft Computing and Engineering (IJSCE) 4 (1).

[6] A. Chaabane, Y. Ding, R. Dey, M. A. Kaafar, K. W. Ross, A closer look at third-party osn applications: Are they leaking your personal information?, in: International Conference on Passive and Active Network Measurement, Springer, 2014, pp. 235-246.

[7] G. Pallis, D. Zeinalipour-Yazti, M. D. Dikaiakos, Online social networks: status and trends, in: New Directions in Web Data Management 1, Springer, 2011, pp. 213-234.

[8] S. Egelman, My profile is my password, verify me!: the privacy/convenience tradeoff of facebook connect, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2013, pp. 2369-2378.

[9] N. Aldhafferi, C. Watson, A. Sajeev, Personal information privacy settings of online social networks and their suitability for mobile internet devices, arXiv preprint arXiv:1305.2770.

[10] C. Richthammer, M. Netter, M. Riesner, J. S¨anger, G. Pernul, Taxonomy of social network data types, EURASIP Journal on Information Security 2014 (1) (2014) 11.

[11] I. Kayes, A. Iamnitchi, A survey on privacy and security in online social networks, arXiv preprint arXiv:1504.03342.

[12] E. Steel, G. Fowler, Facebook in privacy breach, The Wall Street Journal 18 (2010) 21-22.

[13] J. King, A. Lampinen, A. Smolen, Privacy: Is there an app for that?, in: Proceedings of the Seventh Symposium on Usable Privacy and Security, ACM, 2011, p. 12.

[14] R. I. Singh, M. Sumeeth, J. Miller, A user-centric evaluation of the readability of privacy policies in popular web sites, Information Systems Frontiers 13 (4) (2011) 501-514.

[15] B. Viswanath, E. Kiciman, S. Saroiu, Keeping information safe from social networking apps, in: Proceedings of the 2012 ACM workshop on Workshop on online social networks, ACM, 2012, pp. 49-54.

[16] A. Chaabane, Y. Ding, R. Dey, M. A. Kaafar, K. W. Ross, A closer look at third-party osn applications: Are they leaking your personal information?, in: International Conference on Passive and Active Network Measurement, Springer, 2014, pp. 235-246.

[17] W. Wu, Y. Xiao, W. Wang, Z. He, Z. Wang, K-symmetry model for identity anonymization in social networks, in: Proceedings of the 13th international conference on

extending database technology, ACM, 2010, pp. 111-122.

[18] X.-Y. Liu, B. Wang, X.-C. Yang, Survey on privacy preserving techniques for publishing social network data, Journal of software 25 (3) (2014) 576-590.

[19] A. Chakraborty, B. Annappa, A perturbation based approach for privacy preserving publication of social network graphs.

[20] G. Blosser, J. Zhan, Privacy preserving collaborative social network, in: Proceedings of International Conference on Information Security and Assurance (isa 2008), 2008, pp. 543-548.

[21] A. Campan, T.M.Truta, N. Cooper, P-sensitive k-anonymity with generalization constraints, Transactions on Data Privacy 3 (2010) 65-89.

[22] S.Guha, K.Tang, P. Francis, NOYB: Privacy in Online Social Networks, in: Proceedings of the first workshop on online social networks (WOSN'08), 2008, pp.49-54.

[23] P.W.L.Fong, M.Anwar, Z.Zhao, A privacy preservation model for facebook-style social network systems, Computer Security - ESORICS 2009, vol. 5789 (2009) 303-320.

[24] Y.Zhu, Z.Hu, H.Wang, H.Hu, G.J.Ahn, A collaborative framework for privacy protection in online social networks, in: 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2010), 2010, pp. 1-10.

[25] A. Shakimov, H. Lim, R. Cáceres, L.P.Cox, K.Li, D.Liu, A.Varshavsky,Vis-a-Vis: Privacy-preserving online social networking via Virtual Individual Servers, in: Third International Conference on Communication Systems and Networks (COMSNETS 2011), 2011.

[26]A.Masoumzadeh,J.Joshi,Preserving structural properties in edge-perturbing anonymization techniques for social networks, IEEE Transactions on Dependable and Secure Computing 9(6) (2012) 877-889.

[27] M. Fire, D. Kagan, A. Elishar, Y. Elovici, Social Privacy Protector - Protecting Users' Privacy in Social Networks, in International Conference on Social Eco-Informatics (SOTICS), 2012.

[28] R. Heatherly, M.Kantarcioglu, B.Thuraisingham, Preventing private information inference attacks on social networks, IEEE Transactions on Knowledge and Data Engineering 25(8) (2013)1849-1862.

[29] Y. Cheng, J. Park, R. Sandhu, Preserving user privacy from third-party applications in online social networks, in: Proceedings of the 22nd International Conference on World Wide Web, ACM, 2013, pp. 723-728.

[30] C.Sun, P.S.Yu, X.Kong, Y.Fu, Privacy preserving social network publication against mutual friend attacks, in: IEEE 13th International Conference on Data Mining Workshops ,2013.

[31] A. Singh, D. Bansal, S. Sofat, Privacy preserving techniques in social networks data publishing-a review, International Journal of Computer Applications 87 (15).

[32] B. Raghunathan, The complete book of data anonymization: from planning to implementation, CRC Press, 2013.

[33] X. Qi, M. Zong, An overview of privacy preserving data mining, Procedia Environmental

Sciences 12 (2012) 1341-1347.

[34] R. Indhumathi, S. M. Priya, Data preserving by anonymization techniques for collaborative data publishing, Mechanics 20 (21) 20-21.

[35] L. Sweeney, k-anonymity: A model for protecting privacy, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10 (05) (2002) 557-570.

[36] A. Machanavajjhala, D. Kifer, J. Gehrke, M. Venkitasubramaniam, Ldiversity: Privacy beyond k-anonymity, ACM Transactions on Knowledge Discovery from Data (TKDD) 1 (1) (2007) 3.

[37] N. Li, T. Li, S. Venkatasubramanian, t-closeness: Privacy beyond kanonymity and l-diversity, in: Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on, IEEE, 2007, pp. 106-115.

[38] Campan, A., Alufaisan,Y., and Truta,T.M. (2015). Preserving Communities in Anonymized Social Networks. Transactions on Data Privacy, 55 -87.

[39] T. Tassa, D. J. Cohen, Anonymization of centralized and distributed social networks by sequential clustering, IEEE Transactions on Knowledge and Data Engineering 25 (2) (2013) 311-324.

[40] M. E. Skarkala, M. Maragoudakis, S. Gritzalis, L. Mitrou, H. Toivonen, P. Moen, Privacy preservation by k-anonymization of weighted social networks, in: Advances in Social Networks Analysis and Mining (ASONAM), 2012, pp. 423-428.

[41] M. Yuan, L. Chen, S. Y. Philip, T. Yu, Protecting sensitive labels in social network data anonymization, IEEE Transactions on Knowledge and Data Engineering 25 (3) (2013) 633-647.

[42] S. Chakraborty, J. G. Ambooken, B. Tripathy, S. Purushotham, Analysis and performance enhancement to achieve recursive *(c, l)* diversity anonymization in social networks, Transactions on Data Privacy 8 (2) (2015) 173-215.

[43] Y.-Y. Song, L. Ying, Decision tree methods: applications for classification and prediction, Shanghai archives of psychiatry 27 (2) (2015) 130.

[44] S.Rahman, T.K. Huang, H.V. Madhyastha, M. Faloutsos, FRAppE: Detecting Malicious Facebook Applications, in: Proceedings of the 8th International conference on Emerging networking experiments and technologies (CoNEXT '12), 2012, pp.313-324.

[45] S. Kavianpour, Z. Ismail, B. Shanmugam, Classification of third-party applications on facebook to mitigate users information leakage, in: World Conference on Information Systems and Technologies (WorldCIST 2017), 2017, pp.144-154.

[46] J. Leskovec, A. Rajaraman, J. D. Ullman, Mining of massive datasets, Cambridge university press, 2014.

[47] P. Shi, L. Xiong, B. Fung, Anonymizing data with quasi-sensitive attribute values, in: Proceedings of the 19th ACM international conference on Information and knowledge management, ACM, 2010, pp. 1389-1392.

[48] S. Ananthula, O. Abuzaghleh, N. B. Alla, S. Chaganti, P. Kaja, D. Mogilineedi, Measuring privacy in online social networks, International Journal of Security, Privacy and Trust Management 4 (2) (2015) 1-9.