JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 39, 1169-1183 (2023)
DOI: 10.6688/JISE.202309_39(5).0010

Privacy Risk Estimation of Online Social Networks*

SHI-TONG FU[1,2] AND ZHI-QIANG YAO[1,2,3,+]
[1]*College of Computer and Cyber Security*
Fujian Normal University
Fujian Fuzhou, 350117 P.R. China
[2]*Engineering Research Center of Big Data Analysis and Application*
[3]*Engineering Research Center for ICH Digitalization and Multi-Source Information Fusion*
Fujian Provincial University
Fujian Fuzhou, 350117 P.R. China
E-mail: shitongf2022@163.com; yzq@fjnu.edu.cn[+]

With the growing risk of privacy breaches in online social networks, privacy protection has become a key issue. To increase users' privacy awareness and protect their data, there is a need for a simple and effective method of quantifying privacy risk. A user with a higher privacy risk score is more likely to face a serious privacy breach. In this paper, we propose an effective and reasonable privacy risk scoring method. Our method takes into account the granularity of the shared profile items, combines sensitivity and visibility, and generates a privacy risk score for each user. The calculation of sensitivity and visibility are conducted over a response matrix(R) where each element r_{ij} indicates the privacy settings level by user i related to profile item j, and uses improved inverse document frequency (IDF) method to calculate the sensitivity values. Most existing work does not consider profile item granularity. In our study, we define the amount of data shared by users as bytes, classify different granularity levels by one-dimensional clustering, and finally obtain the granularity values using the sigmoid function. With the privacy risk score, users can acquire a more intuitive awareness of their privacy status and then defend it by altering privacy settings or lowering the granularity of shared data. In addition, our experiments analyzing real-world and synthetic datasets demonstrate that our method is capable of effectively assessing user privacy risks in online social networks.

Keywords: online social network, privacy breach, privacy risk score, IDF, granularity

1. INTRODUCTION

In recent years, with the rapid development and widespread popularity of the Internet, an increasing number of individuals prefer to interact via the Internet. Due to the simplicity and effectiveness of online social networks(OSNs), a product of the Internet has attracted a great number of users [1]. Through OSNs, users can connect with people from

Received July 9, 2022; revised September 22, 2022; accepted October 10, 2022.
Communicated by Xiaohong Jiang.
[+] Corresponding author.
[*] International Conference on Networking and Network Applications, 2022, China.
[*] This work was supported by the National Natural Science Foundation of China under Grant 61872090, Fujian Provincial Science and Technology Guidance Project under Grant 2019H0010, and the Open Fund of Fujian Provincial University Engineering Research Center under Grant FJ-ICH201901.

all over the world for purpose of chatting or sharing other resources such as videos and news. Additionally, different types of social network providers offer specialized functions [2, 3]. The majority of them, such as Facebook and WeChat, are used for instant messaging and social media, where users can reconnect with old friends or make new ones. Sina Weibo and Twitter are primarily used for social news or public event posting. In addition, TikTok and YouTube are primarily used for video-centric social networking services.

With the exponential rise of OSNs and users, the risk of the violation of personal privacy is becoming increasingly significant [4]. On the one hand, the majority of OSN service providers encourage or induce users to provide basic information (name, phone number, address, *etc*.) and sensitive information (religious beliefs, political opinions, illnesses, *etc*.) in the cause of enhancing the site's usability for feature recommendations or targeted advertising. And on the other hand, due to the lack of user privacy awareness, that every time a user posts information which appears to be non-sensitive can be easily accessed by malicious actors. For instance, when you release your phone number on OSN's profile items to make it easier for your friends to contact you, but are also bothered by spam and nuisance calls as a result of this activity. In addition, some malicious attackers deduce users' personal and behavioral characteristics from their attributes and actions. For example, consider the well-publicized Uber data breach and the "Facebook Cambridge Analytica incident" [5]. As a result, it is up to users to determine how to avoid privacy breaches and thereby preserve their privacy [1, 6]. In order to avoid the leakage of users' privacy information, several OSNs service providers also give a warning or restrict users from doing the next operation when their privacy information is released, although users are frequently unaware of the risk of privacy leakage caused by various uncontrolled conditions. Because of the frequency of data privacy breaches and users' growing privacy expectations, many OSNs service providers provide users with the ability to customize their profile privacy policies. For example, Facebook provides optional access control objects for each user profile, including public (on and off Facebook), Facebook friends, designated friends, self only, and custom (including or excluding single or multiple friends). Nevertheless, the majority of these options are either too hidden or too complicated for users [7].

To address the above issues, several studies [8–10] have proposed using the sensitivity and visibility of users' profile items to assess the risk of privacy breach for users of OSNs based on their privacy setting strategies, or simplifying the privacy setting process for users through some guidelines and user background [7, 11]. Some other studies have proposed the concept of privacy policy automation to help users by targeting information such as their profiles and locations to setting and managing privacy policies [12,13]. However, the majority of existing research focus on the privacy risk metrics about individual user profiles and their privacy policy settings, which has significant limitations. In fact, users' privacy risk is not confined to their privacy policy preferences, the granularity with which their profile information is shared is also a significant element determining privacy risk [14]. In the case of free text items in personal data such as educational background, life event, and work experience, it's obvious that the more content a user gives, the more information a malicious attacker will have access to, and the more likely the user is to suffer a greater privacy risk.

Quantifying the privacy risk of users and raising their privacy awareness is an effec-

tive method to mitigate the risk of user data leakage. Inspire by Liu and Terzi [9] privacy score, this paper presents a novel scoring function that takes user sharing granularity into account as a potential dimension of the privacy score. This scoring function receives as input the personal attribute information of OSNs users. In this method, the privacy policy settings and published content of each item are used as inputs for calculating the privacy score. Moreover, we provide a detailed description of how to calculate the profile item's sensitivity, as well as the visibility and granularity values for each user to each profile item, and then combine these three factors to obtain a final formula for computing the privacy risk score. It's worth emphasizing that each user's privacy risk score is unique, depending on their level of privacy awareness, the type and amount of data supplied, and the extent to which they disclose. The following summarizes our contribution to this paper:

- We incorporate granularity of data sharing as a component in the privacy risk score, combine improved sensitivity and visibility, and provide a novel method for calculating the privacy risk score for online social networks.
- We use the improved inverse document frequency (IDF) algorithm to quantify sensitivity, and innovatively propose using one-dimensional clustering algorithm and the sigmoid function to measure the shared granularity of the data, which is still able to generate outstanding results.
- We conduct experiments on actual and synthetic datasets then compare them to existing research methodologies to show the validity of our approach.

The remainder of this paper is divided into the following sections: Section 2 summarizes the existing literature on privacy scoring. Section 3 presents our proposed method and the mathematical formulation for calculating privacy risk scores. Section 4 presents the details of using synthetic and real online social network datasets and conducts an experimental study and comparative analysis of our proposed method, and finally, Section 5 concludes the work in this paper and forecast the future work.

2. RELATED WORK

As the number of people using online social networks growing, privacy breaches become a serious issue. In this section, we review several previous studies on privacy risk scoring models. These studies usually take into account the user's privacy settings for individual profile items, the user's network location, the content of text messages, and the user's use of multiple social platforms. The majority of these research examine privacy risk scoring from the user's perspective, with the possibility of providing users with a more intuitive understanding of their privacy status and so enhancing their privacy awareness.

Maximilien [8] first introduced the concepts of user attribute sensitivity and visibility and solved them using a Bayesian methods to obtain the user's privacy metric. As an extension of [8], Liu and Terzi [9] took inspiration from credit risk scoring in financial systems and quantify the leakage risk of users based on user profile and item response theory (IRT) to calculate the sensitivity and visibility of user profile items and they were the first to introduce the concept of privacy scores. They employed both synthetic and

real-world data sets and a chi-square test to demonstrate the effectiveness of their approaches by analyzing the privacy score model's fit with data. Wang *et al*. [15] employed the Privacy Index (PIDX) to quantify the risk of user privacy exposure in OSNs and experimentally validated three user groups: Privacy Fundamentalists, Pragmatic Majorities and Marginally Concerned.

Aghasian *et al*. [16] extended the privacy score from a single platform to multiple platforms, where the authors defined the user's visibility as the accessibility of attributes, the difficulty of data extraction, and reliability, and then used a fuzzy theory approach to combine the sensitivity of attributes to calculate the user's final privacy disclosure score (PSD) across multiple OSNs. Li *et al*. [1] improved on [16] by proposing a method to quantify user privacy awareness as a dimension of user visibility taking into account users' use of disinformation on different social networks, and then they used a simplified half-suppressed fuzzy C-mean clustering algorithm to quantify the visibility. Finally, the surveyed dataset is used to calculate users' privacy risk scores across multiple OSNs.

To assess users' privacy risks, Alemany *et al*. [17] proposed a method named PRS (Privacy Risk Score) that takes into account the accessibility of personal information on OSNs and the centrality of users in a network, among other factors. Pensa *et al*. [18] argued that users' privacy scores are determined not only by their privacy preferences and the extent to which their personal data is exposed, but also by the location of the social network in which the user is linked in. The authors indicated that users who are in a network environment with low-privacy-aware friends are more vulnerable to threats than users who are in a network environment with high-privacy-aware friends. For the adolescent population in OSNs, for purpose of enhancing their privacy awareness, Alemany *et al*. [19] proposed two soft-paternalism mechanisms to help adolescent users make better decisions about privacy risk behaviors in OSNs. The first mechanism shows the profiles and risk level alerts of possible users to whom the young user might be exposed, while the second mechanism shows the quantity and danger level alerts of users with access to the message's target audience. The mechanism considers two types of indicator information that influence privacy risk scores: different levels of friendship and potential users that may be exposed to the disclosed information.

Coban *et al*. [20] proposed a novel sensitivity calculation approach in which the authors interpret the response matrix R as a term-document matrix and then compute the sensitivity of the profile items using the inverse document frequency (IDF) method. However, this privacy risk score system just replaces the method of [18] for calculating sensitivity and did not consider the granularity of data sharing. Kilic *et al*. [14] introduced the sharing granularity of user profile items into the privacy risk score, but the authors only integrated the sharing data granularity into the IRT framework without considering the privacy policy settings of profile items. And the experiment only focuses on a specific OSN-LinkedIn and did not apply to the majority of OSNs.

As indicated previously, there have been numerous research on OSNs privacy risk assessments and analysis. In contrast to the previous studies, we consider introducing data sharing granularity into privacy risk scoring and propose a new method for privacy risk scoring. The experimental results show that the proposed method is effective evaluating a user's privacy disclosure status. By analyzing the final privacy risk score, users can be informed of the privacy risk score of each profile item for the purpose of improving their privacy awareness and protecting data security from the user's own perspective.

3. THE PRIVACY SCORING METHOD

We assume a set of n users in an OSN, here denoted as a undirected graph $G(V,E)$, where V is a set of n nodes $\{v_1, v_2, \ldots, v_n\}$ such that each node $v_i \in V$ stands for a user and E is a set of edges. While $v_i, v_j \in V$, a couple of $(v_i, v_j) \in E$ indicates that there is a connection between users v_i and v_j(*e.g.*, friends with each other). On the other hand, we define each user in V to have a set of m profile items represented as $A = \{a_1, a_2, \ldots, a_m\}$.

Because of user's privacy risk score can be assessed, the user can evaluate his or her privacy risk level intuitively and precisely, and mitigate the risk of privacy leakage by altering the settings for individual profile items to obtain an acceptable level of privacy for the user. In order to compute privacy risk score, we need to identify the factors that contribute to the danger of online social network users leaking their personal information. In previous studies, most of them only considered sensitivity and visibility, and did not focus on the sharing granularity of profile items. As a result, we propose a new privacy risk score formula, which improves the measurement of user privacy risk by considering the sensitivity, visibility, and sharing granularity of profile items.

3.1 Calculation of Visibility

At present, most online social networking service providers provide their users with a variety of privacy settings. Most of these settings allow users to establish profile visibility levels that determine who they want to share their profile content with, ensuring that their privacy is protected. Based on the data shared by users, we can get an size $n \times m$ response matrix R which is linked to the set of n different users over the set of m different profile items. Each element r_{ij} in the matrix R contains an integer value in the range 0 to l, where l indicates the privacy settings level by user v_i related to profile item a_j. The response matrix R is further divided into two forms: dichotomous response matrix and polytomous response matrix. When $l = 2$, matrix R is defined to as a dichotomous response matrix, which contains two levels of visibility: 0 indicates private data (only viewable to the data owner) and 1 epresents publicly shared data (visible to all people). In the other case, when $l > 2$, matrix R is a polytomous response matrix, and we employ the following levels of privacy: 0 indicates information access by only profile owner; 1 represents information access by friends of the list who are specific individuals or group of people, such as family or colleagues, etc; 2 indicates information access by all friends; 3 represents information access by friends of her or his friends; 4 indicates publicly available information in the OSNs. In order to calculate the visibility to each profile item a_j in relation to user v_i, we use the for any degree $k = \{0, \ldots, l\}$ to compute the visibility δ_{ijk} as follows,

$$\delta_{ijk} = P(r_{ij=k}) \times k. \tag{1}$$

Assuming users and profile items mutually independence [8], the probability $P(r_{ij=k})$ that r_{ij} equals k can be calculated as follows,

$$P(r_{ij=k}) = \frac{\sum_{i=1}^{n} I_{(r_{ij}=k)}}{n} \times \frac{\sum_{j=1}^{m} I_{(r_{ij}=k)}}{m}. \tag{2}$$

3.2 Computation of Granularity

Certain attributes of a user's personal profile have a set structure for filling in, such as age, birthdate, gender, *etc*., but the majority of attributes, such as educational background, work experience, family members and relationship status, life events, interests, and so on, are free text items. Nevertheless, it is insufficient to consider solely the visibility of these free text items under privacy settings when evaluating their privacy score. As indicated in Table 1, user v_A and user v_B share their life events and educational backgrounds, and they set the same level of visibility. Since v_A provides more information, he/she has a higher chance of privacy leakage, and hence deserves a higher privacy score. However, according to traditional privacy scoring methods [9, 20], these two users have the same privacy scores on life events and hobbies. We argue that this is impracticable, hence this article also analyzes the granularity of users' shared data as a factor affecting their privacy risk leaks.

Table 1. Users' shared data.

user	Life Events	Educational Backgrounds
user v_A	2020 Strarted New Job at Drexelbrook Friends on Facebook with Eli Wang for 5 Years 2021 Strarted New Job at Spine Media 2022 Strarted New Job at Business Insider	Massachusetts Institute of Technology, Bachelor,Software Engineering, 2016,2020
user v_B	2020 Strarted New Job at Mary Byrnes – Re/Max Main Line	Yale University, Bachelor, Computer Engineering, 2016,2020

We define the quantity of data shared of the users as byte, although a greater amount of shared byte does not necessarily imply that the user is disclosing more private information. When we look at Table 1, for example, it is seen that both user v_A and user v_B disclose their educational backgrounds, and the quantity of data shared by user v_A is 69 and by user v_B is 49, indicating a higher risk of privacy leak for user v_A. However, a closer look at the content indicates that both user v_A and user v_B are publishing their school, bachelor's degrees, major, and time of attendance, meaning that the risk of private disclosure is the same. Based on the aforementioned issues, we define four granularity levels for user profile items: 0 indicate zero granularity (no information shared by the users), 1 represent low granularity, 2 indicate medium granularity, and 3 represent high granularity. Then, for each profile item, we conduct one-dimensional clustering [21], assigning distinct granularity levels to each user's profile item. We utilize the sigmoid function to calculate the user's granularity because granularity rises with granularity level. The reason for using the sigmoid function is that it supports us in differentiating the granularity. The granularity of user v_i in relation to profile item a_j is calculated using the following formula:

$$\gamma_{ij} = \frac{2}{1 - e^{-s}} - 1 \tag{3}$$

where "s" indicates the granularity level. The output of this function is bounded by [0, 1], where the higher the granularity level, the larger the value of the granularity.

3.3 Calculation of Sensitivity

Sensitivity of profile items represents the degree of influence of various profile items on privacy leakage. The higher the profile items sensitivity value, the higher the risk of user privacy leakage and the higher the privacy risk score. Liu and Terzi [9] calculated the sensitivity score for measuring the privacy score based on the item response theory (IRT). Nevertheless, IRT isn't suitable for complicated OSNs since it must meet three key assumptions: items independence, users independence, and items and users independence [15]. As a result, we calculate the sensitivity for privacy risk scores using the method proposed in [20], namely IDF-Sensitivity and improve it. Inverse document frequency (IDF) is an unsupervised weighted statistical method for determining the importance of a keyword t in D documents. The IDF is defined as:

$$IDF_t = log\frac{D}{DF_t} \tag{4}$$

where DF_t denotes the number of documents containing occurrences of keyword t. To avoid the value DF_t in the denominator equal to zero, the value of the denominator is usually expressed as $DF_t + 1$. The IDF value of a phrase increases as the number of documents containing it decreases, showing that the term has excellent category discrimination ability. In privacy risk analysis, intuitively, the more sensitive an item is, the fewer users are inclined to share it. This property of IDF is the algorithm main reasons to apply it in privacy risk scoring. The details are shown in Algorithm 1. However, some extreme cases need to be considered [20]. When the visibility level of all users is less than k, the quantity of users at visibility level k or higher becomes 0, so the value of u is set to $u+1$. In the other case, when all users share profile items at the same visibility level, the value of c is equal to u. In order to eliminate the abnormality in this case and assume that the sensitivity value is monotonically increasing, we use $log((n+u)/u) * 0.5$ to express the sensitivity value.

3.4 Calculation of Privacy Score

By considering the β_{jk} as the sensitivity of profile items a_j at degree k, the δ_{ijk} as the accessibility of the user v_i at degree k for profile items a_j and the γ_{ij} as the granularity of user v_i related to profile items a_j, the privacy risk score for given user v_i and a given profile items a_j can be computed by the function as follows,

$$\varphi_{ij} = \sum_{k=0}^{l} \beta_{jk} \times (\delta_{ijk} + \gamma_{ij}). \tag{5}$$

Finally, the overall privacy risk score of a given user v_i can be explained in Eq. (6),

$$PS(i) = \sum_{j=1}^{m} \varphi_{ij}. \tag{6}$$

According to the above formulas, as the privacy risk score rises, users are more likely to face privacy threats and information disclosure. when the users post all the sensitive information visible to public with the high granularity level, the privacy risk is greatest. As a result, the lower the privacy score value, the better. It is worth noting that the preceding equation applies to both dichotomous and polytomous scenarios for the parameter k.

Algorithm 1 : IDF-base sensitivity value

Input: Response matrix, $R_{(n\times m)}$;
Output: sensitivity values, $\beta_{(l\times m)}$

```
n ← the number of users
m ← the number of profile items
k ← visibility level
l ← maximum visibility level
for j in m do
  for k = 0 to l do
    c ← the number of users who disclose profile item j at level k
    u ← the number of users who disclose profile item j at level h, where k ≤ h ≤ l
    if u = 0 then
      s = log(n/u+1)
    else if u = n then
      if k = l then
        s = log(n/u)
      else if c = n then
        s = log((n+u)/u) * 0.5
      else
        s = log(n/(n−c) * (c/u)
      end if
    else
      s = log(n/u)
    end if
    β[k, j] = s
  end for
end for
β = normalize(β[k, j])
```

4. EXPERIMENTAL EVALUATION

4.1 Datasets

In most privacy risk research, the dataset required for the experiment is generated via a simulation or questionnaire form. It is impractical to generate a polytomous response matrix from an actual dataset retrieved by crawlers, because approaches like crawlers cannot determine the absolute accessibility of users to attribute values. For the evaluation of our proposed model in this research, we employ synthetic datasets and a real-world dataset published by Stanford Network Analysis Project (SNAP) [22].

For the synthesis dataset, we construct three polytomous response matrixes and three dichotomous response matrixes representing the visibility levels of 10K, 20K and 30K users for the 15 profile items, respectively [23]. In the case of polytomous matrices, a random integer between 0 and 4 is generated as the visibility level for that user, and 0 or 1 in the case of dichotomous matrices. We divide the profiles items into two categories, the first one with standard format input, such as *birthday*(a_1), *email*(a_2), *gender*(a_3),

phone number(a_4) and *language*(a_5) , and the second one with free text items (multiple values can be entered), such as *interest*(a_6), *address*(a_7), *links*(a_8), *educational background*(a_9), *work*(a_{10}), *life events*(a_{11}), *family members*(a_{12}), *relational status*(a_{13}), *religious view*(a_{14}) and *political view*(a_{15}). The granularity level for text items with fixed-format input is set to zero granularity level (value of 0) if the visibility level is 0, and to low granularity level (value of 1) if it is not. Similarly, if the visibility level is 0, the granularity level is set to zero (value of 0), and if the visibility level is not 0, the granularity level is generated randomly at low, medium, and high granularity levels for the characteristics of a free text item (values of 1,2, or 3).

For the real dataset [22], it builds the response matrix R in dichotomous form. In this dataset, it contains a total of 8 profile items. *Birthday*(a_1), *gender*(a_2), *hometown*(a_3), *language*(a_4), and *location*(a_5) all have only one form, so the granularity for the filled user is set to low granularity level (value of 1), whereas for the profile items which contain multiple attributes, such as *name*(a_6)(*first_name, last_name, middle_name*), *education*(a_7)(*concentration, degree, school, type, year*)and *work*(a_8)(*start_date, end_date, from, location, position, projects*), we define low granularity level (value of 1) if one is filled, medium granularity level (value of 2) if two are filled, high granularity level (value of 3) if three or more are filled, and zero granularity level(value of 0) if none are filled.

4.2 Experimental Results

Due to space constraints, we chose six users from the real-world dataset. The visibility level and granularity level (expressed as (gs) of the six users in the real-world dataset are listed in Table 2, as are the privacy risk score calculated using the Naive approach [9] (name as PS_naive), the Onder Coban method [20] (name as PS_idf), and our method. Fig. 1 illustrates six users' privacy risk scores using three distinct ways. As can be observed, our method achieves greater scores because we take the case of profile item granularity level into account. In particular, for v_1, his or her granularity levels for free text items a_6, a_7 and a_8 are all high granularity levels. Additionally, because v_6's granularity levels are predominantly low, the privacy risk scores generated by the three methods are similar. As a result, we deem that v_1 has a more serious privacy breach than v_6.

Table 2. Privacy risk scores obtained by three methods for visibility level and granularity level(expressed as (gs)) on five standard format inputs and three free text items from six users selected from real-world dataset.

User	Profile items								Risk scores		
	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	PS_naive	PS_idf	our method
v_1	1(g1)	0(g0)	1(g1)	1(g1)	1(g1)	1(g3)	1(g3)	1(g3)	1.7498	2.3413	5.9276
v_2	1(g1)	0(g0)	0(g0)	1(g1)	1(g1)	1(g2)	1(g3)	1(g3)	1.4998	2.0068	5.1136
v_3	0(g0)	0(g0)	1(g1)	0(g0)	0(g0)	1(g3)	1(g3)	1(g2)	0.9999	1.3379	3.6036
v_4	1(g1)	1(g1)	0(g0)	0(g0)	0(g0)	1(g2)	1(g3)	1(g3)	1.2499	1.6724	4.3590
v_5	1(g1)	1(g1)	0(g0)	1(g1)	1(g1)	0(g0)	1(g3)	1(g3)	1.4998	2.0068	4.9613
v_6	0(g0)	0(g0)	1(g1)	1(g1)	0(g0)	0(g0)	1(g1)	1(g1)	0.9998	1.3379	3.0265

The ultimate goal of calculating the privacy risk score is to provide users with a broad understanding of their privacy leakage risk on online social networks, and then to mitigate that risk by changing the privacy policy or decreasing the profile items granularity

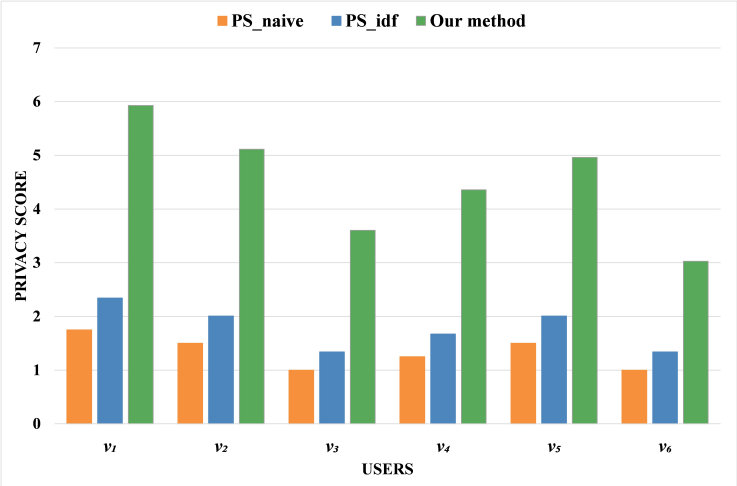

Fig. 1. Six users' privacy risk scores.

level, thereby improving users' privacy protection awareness. We use v_1 as an example to demonstrate that users can change the profile items content in a reasonable manner to reduce the granularity level and hence limit privacy leaks. As presented in Fig. 2, after modifying the profile items content of v_1's free text item in accordance with Table 3 and reducing its granularity level, the free text item attribute's privacy risk score is greatly lowered.

Table 3. Privacy score after a change in v_1 profile item.

profile items	name	education	work
before change	1(g3)	1(g3)	1(g3)
	first_name middle_name last_name	degree year school classes	start_date from position location projects
after change	1(g1)	1(g1)	1(g1)
	first_name	school	position

We provide the above examples to help users better understand their privacy leakage on online social networks, but there is no universal method of privacy protection that will meet the needs of all users, as each user uses different online social platforms for different purposes and requires varying levels of privacy protection. Thus, the primary objective of this study is to cultivate and reinforce users' privacy awareness through privacy risk scores, and to prevent their information from being stolen by outsiders by educating users about privacy protection from the start of their use of online social networks.

In the second experiment, we analyze the experimental results of the synthetic dataset. Table 4 displays the visibility level and granularity level used by the five users in the synthetic dichotomous and polytomous datasets, as well as the results for the three

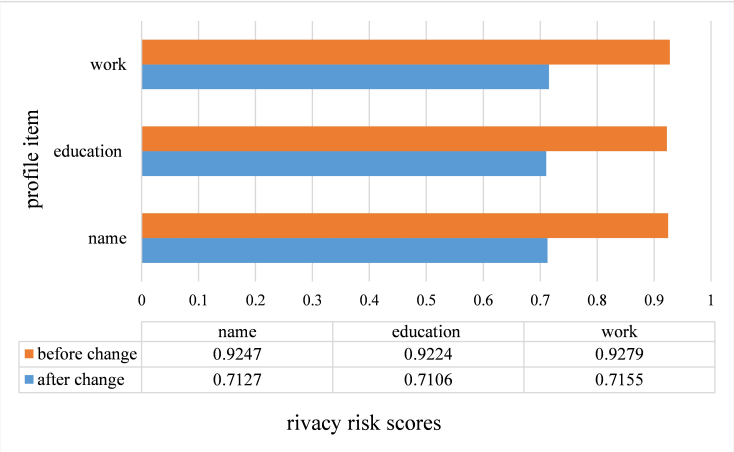

Fig. 2. Comparison of privacy risk scores before and after name,education and work change.

distinct privacy risk scores. We present only the profile items of the free text items here to demonstrate the method's effectiveness. As illustrated in Table 4, the privacy risk scores derived by our method are greater because we take the granularity of data sharing into account. Furthermore, the scores computed by the three approaches are generally greater than those computed by the dichotomous response matrix for the multisubject response matrix. In addition, it can be shown that the privacy risk scores calculated by PS_naive and PS_idf are quite close, as the PS_idf method utilizes the same visibility algorithm as the PS_nave method, and both methods ignore data sharing granularity.

Table 4. Privacy risk scores obtained by three methods for visibility level and granularity level (expressed as (gs)) on synthese dataset.

User	Profile items										Risk scores		
	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	PS_naive	PS_idf	our method
Dichotomous Response Matrix													
v_1	1(g2)	0(g0)	1(g3)	0(g0)	0(g0)	1(g2)	1(g3)	0(g0)	1(g1)	1(g3)	1.4999	2.0068	5.4800
v_2	0(g0)	1(g1)	0(g0)	1(g3)	1(g3)	1(g3)	0(g0)	0(g0)	0(g0)	0(g0)	0.9999	1.3378	3.6604
v_3	1(g1)	1(g1)	1(g1)	0(g0)	1(g1)	1(g3)	1(g1)	1(g2)	1(g1)	1(g2)	2.2498	3.0101	7.3289
v_4	1(g1)	1(g1)	1(g3)	0(g0)	1(g1)	1(g2)	1(g3)	0(g0)	0(g0)	1(g3)	1.7498	2.3412	6.0815
v_5	1(g1)	1(g3)	1(g2)	0(g0)	0(g0)	0(g0)	0(g0)	1(g2)	0(g0)	1(g1)	1.2499	1.6723	4.3092
Polytomous Response Matrix													
v_1	3(g1)	0(g0)	1(g3)	4(g2)	0(g0)	2(g1)	3(g3)	1(g2)	2(g1)	4(g3)	2.6358	1.2590	7.7353
v_2	4(g3)	2(g3)	1(g1)	3(g1)	4(g3)	1(g3)	4(g1)	4(g3)	1(g3)	2(g1)	3.5605	1.8851	10.1149
v_3	4(g3)	3(g1)	1(g1)	3(g1)	0(g0)	2(g1)	3(g1)	3(g1)	3(g3)	4(g3)	3.6277	1.6795	8.3229
v_4	4(g1)	1(g2)	1(g3)	0(g0)	0(g0)	4(g1)	4(g1)	0(g0)	3(g2)	4(g1)	3.1015	1.7480	6.9560
v_5	0(g0)	1(g1)	2(g2)	0(g0)	1(g1)	4(g3)	2(g1)	0(g0)	2(g1)	0(g0)	1.3596	0.6013	4.9447

Analysis of privacy score models can be done using a variety of statistical method. As a result, in the last experiment of this work, we apply our method to the three dichotomous and three polytomous synthetic datasets previously, and then utilize Pearson correlation coefficients [24] to determine the association between the two privacy scoring methods above and our proposed privacy scoring model. The Pearson correlation coefficient is used to describe the strength and direction of the relationship between two sets of linear data. It is equal to the covariance of the two variables divided by the standard

deviation of the two variables and is calculated as shown below,

$$\rho_{X,Y} = \frac{\sum_{i=1}^{n}(X_i - \mu_X)(Y_i - \mu_Y)}{\sigma_X \sigma_Y}. \tag{7}$$

The Pearson correlation coefficient values of the three different privacy scoring methods regarding each dataset is displayed in Table 5. As demonstrated by the experimental results, the correlation between the two scoring techniques, PS_naive and PS_idf, is higher since PS_idf just provides a new way for calculating sensitivity based on the naive scoring method and does not introduce a new dimension affecting privacy risk. Additionally, as illustrated in Table 5, our method has a low correlation with naive and idf privacy scoring methods, which is due to the fact that we include data sharing granularity as a component of privacy scoring. And our method usually has a low correlation with other approaches when calculating privacy risk scores from polytomous response data, indicating that the granularity of data sharing has an effect on users' privacy risk and should be considered when computing privacy risk scores.

Table 5. Pearson correlation coefficient values between privacy risk scoring methods.

No.	the number of users	*R* matrix	Method	PS_naive	PS_idf	our method
1	10W	Synthetic polytomous	PS_naive	1	0.973	0.751
			PS_idf	0.973	1	0.667
			our method	0.751	0.667	1
		Synthetic dichotomous	PS_naive	1	0.998	0.906
			PS_idf	0.998	1	0.927
			our method	0.906	0.927	1
2	20W	Synthetic polytomous	PS_naive	1	0.971	0.764
			PS_idf	0.971	1	0.676
			our method	0.764	0.676	1
		Synthetic dichotomous	PS_naive	1	0.993	0.915
			PS_idf	0.993	1	0.924
			our method	0.915	0.924	1
3	30W	Synthetic polytomous	PS_naive	1	0.982	0.733
			PS_idf	0.982	1	0.665
			our method	0.733	0.665	1
		Synthetic dichotomous	PS_naive	1	0.996	0.912
			PS_idf	0.996	1	0.925
			our method	0.912	0.925	1
4	1000	real-world dataset	PS_naive	1	0.993	0.896
			PS_idf	0.993	1	0.903
			our method	0.896	0.903	1

5. CONCLUSIONS

With the widespread popularity of online social networks in daily life and the explosive growth of users, the issue of data privacy protection on online social networks has become an inevitable problem. The occurrence of several privacy breaches serves as

a reminder to users that relying OSNs service providers alone is insufficient; users must also raise their privacy awareness and take the initiative to secure their private data. In this paper, we consider the concept of data sharing granularity, quantify it using clustering algorithms and sigmoid functions, and take into account sensitivity and visibility, two traditional privacy risk scoring factors, to obtain a final privacy risk score for online social network users. Based on experimental evaluations on real-world and synthetic datasets, we conclude that the proposed approach enables users to assess the privacy risk associated with their OSNs. With the privacy risk score, users can gain a more intuitive understanding of their privacy breach status, and with a specific privacy score for each profile item, users can choose which profile items to remove and hide or reduce the granularity value of data sharing to reduce their privacy risk score according to their privacy needs.

In future research, we will investigate whether additional aspects impact to users' privacy risk when utilizing online social networks and mathematically quantify them to add to the privacy risk score, thereby expanding the privacy risk scoring framework. Additionally, because there is no precise definition for evaluating the advantages of the scoring methods, future study will explore how to quantify the efficacy of numerous privacy scoring approaches.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China under Grant 61872090, Fujian Provincial Science and Technology Guidance Project under Grant 2019H0010, and the Open Fund of Fujian Provincial University Engineering Research Center under grant FJ-ICH201901.

REFERENCES

1. X. Li, Y. Yang, Y. Chen, and X. Niu, "A privacy measurement framework for multiple online social networks against social identity linkage," *Applied Sciences*, Vol. 8, 2018, p. 1790.
2. Z. He, Z. Cai, and J. Yu, "Latent-data privacy preserving with customized data utility for social network data," *IEEE Transactions on Vehicular Technology*, Vol. 67, 2017, pp. 665-673.
3. M. A. Wani, N. Agarwal, S. Jabin, and S. Z. Hussai, "Design and implementation of imacros-based data crawler for behavioral analysis of facebook users," *Computer Science: Social and Information Networks*, 2018, arXiv:1802.09566.
4. H. Jia and H. Xu, "Measuring individuals' concerns over collective privacy on social networking sites," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, Vol. 10, 2016, Article 1.
5. Y. B. Choi, "Organizational cyber data breach analysis of facebook, equifax, and uber cases," *International Journal of Cyber Research and Education*, Vol. 3, 2021, pp. 58-64.
6. L. Bioglio and R. G. Pensa, "Impact of neighbors on the privacy of individuals in online social networks," *Procedia Computer Science*, Vol. 108, 2017, pp. 28-37.

7. L. Fang and K. LeFevre, "Privacy wizards for social networking sites," in *Proceedings of the 19th International Conference on World Wide Web*, 2010, pp. 351-360.
8. E. M. Maximilien, T. Grandison, T. Sun, D. Richardson, S. Guo, and K. Liu, "Privacy-as-a-service: Models, algorithms, and results on the facebook platform," in *Proceedings of IEEE Symposium on Security and Privacy Workshops*, Vol. 2, 2009.
9. K. Liu and E. Terzi, "A framework for computing the privacy scores of users in online social networks," *ACM Transactions on Knowledge Discovery from Data*, Vol. 5, 2010, pp. 1-30.
10. A. Srivastava and G. Geethakumari, "Measuring privacy leaks in online social networks," in *Proceedings of International Conference on Advances in Computing, Communications and Informatics*, 2013, pp. 2095-2100.
11. X. Song, X. Wang, L. Nie, X. He, Z. Chen, and W. Liu, "A personal privacy preserving framework: I let you know who can see what," in *Proceedings of the 41st International ACM SIGIR Conference on Research & Development in Information Retrieval*, 2018, pp. 295-304.
12. K. D. Naini, I. S. Altingovde, R. Kawase, E. Herder, and C. Niederée, "Analyzing and predicting privacy settings in the social web," in *Proceedings of International Conference on User Modeling, Adaptation, and Personalization*, 2015, pp. 104-117.
13. L. Chen, M. Xu, X. Yang, N. Zheng, Y. Wu, J. Xu, T. Qiao, and H. Liu, "A privacy settings prediction model for textual posts on social networks," in *Proceedings of International Conference on Collaborative Computing: Networking, Applications and Worksharing*, 2017, pp. 578-588.
14. Y. Kilic, "Shared data granularity: A latent dimension of privacy scoring over online social networks," *arXiv Preprint*, 2021, arXiv:2105.07845.
15. Y. Wang, R. K. Nepali, and J. Nikolai, "Social network privacy measurement and simulation," in *Proceedings of International Conference on Computing, Networking and Communications*, 2014, pp. 802-806.
16. E. Aghasian, S. Garg, L. Gao, S. Yu, and J. Montgomery, "Scoring users' privacy disclosure across multiple online social networks," *IEEE Access*, Vol. 5, 2017, pp. 13118-13130.
17. J. Alemany, E. del Val, J. Alberola, and A. García-Fornes, "Estimation of privacy risk through centrality metrics," *Future Generation Computer Systems*, Vol. 82, 2018, pp. 63-76.
18. R. G. Pensa, G. Di Blasi, and L. Bioglio, "Network-aware privacy risk estimation in online social networks," *Social Network Analysis and Mining*, Vol. 9, 2019, pp. 1-15.
19. J. Alemany, E. Del Val, J. Alberola, and A. García-Fornes, "Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms," *International Journal of Human-Computer Studies*, Vol. 129, 2019, pp. 27-40.
20. O. Coban, A. Inan, and S. A. Ozel, "Inverse document frequency-based sensitivity scoring for privacy analysis," *Signal, Image and Video Processing*, Vol. 16, 2022, pp. 735-743.
21. H. Wang and M. Song, "Ckmeans. 1d. dp: optimal k-means clustering in one dimension by dynamic programming," *The R Journal*, Vol. 3, 2011, p. 29.
22. J. Leskovec and A. Krevl, "SNAP datasets: Stanford large network dataset collection," Ann Arbor, MI, USA, 2014.

23. O. Coban, A. Inan, and S. A. Ozel, "Towards the design and implementation of an osn crawler: A case of turkish facebook users," *International Journal of Information Security Science*, Vol. 9, 2020, pp. 76-93.
24. J. Adler and I. Parmryd, "Quantifying colocalization by correlation: the pearson correlation coefficient is superior to the mander's overlap coefficient," *Cytometry Part A*, Vol. 77, 2010, pp. 733-742.

Shi-Tong Fu received the BS degree in Computer Science and Technology from Chengdu University of Technology, China, in 2020. He is now an MS candidate of Fujian Normal University, China. His research interests include big data security, privacy protection and application security.

Zhi-Qiang Yao received the Ph.D. degree in Computer System Architecture from Xidian University, Xian, China, in 2014. He is currently a Professor with Fujian Normal University, Fuzhou, China. He has authored or coauthored over 100 research papers and holds 10 patents. His current research interests include big data security and privacy protection, multimedia security, and application security. Dr. Yao is a Professional Member of the ACM and a Senior Member of the CCF.