A Smart Access Control Mechanism Based on User Preference in Online Social Networks

Fangfang Shan[1,2(✉)], Peiyu Ji[1], Fuyang Li[1], and Weiguang Liu[1]

[1] Zhongyuan University of Technology, Zhengzhou 450000, China
6129@zut.edu.cn
[2] Zhengzhou University, Zhengzhou 450000, China

Abstract. Data privacy protection is crucial in the era of big data, and although access control mechanisms can effectively prevent privacy leakage, existing access control mechanisms of social networks rarely consider users' personal privacy preferences in the process of generating access control policies, so they cannot provide personalized services to users. We proposed an intelligent access control mechanism based on users' privacy preferences by extracting their privacy preference values through a quantifiable analysis mechanism, and then using the values and some key user social resource information as feature vectors. The experiments show that this mechanism can automatically generate appropriate access control policies to meet the potential privacy needs of different users, so as to better protect the privacy of social network data.

Keywords: Personal preference · Access control mechanism · Online social network

1 Introduction

Online social network can provide digital users with social interaction and information sharing, but it has privacy security problems. The overwhelming amount of user information can be collected by enemies using illegal means and correlated to deduce some more private user information, threatening the security of users' personal and property. However, few users are aware of the serious harm that can be caused by privacy breaches. Therefore, it is crucial to study the access control mechanism of social networks for protecting users' private data.

In general, most of the current social network access control is based on relationships, cryptographic algorithms, game theory and face recognition technologies. Pang et al. [1] proposed an access control scheme for Facebook social networks, which implements access control on resources according to the relationship between users. Cheng et al. [2] used regular expression to define access control policy, so that user-user relationship, user-resource relationship and resource-resource relationship can control access requester access resources. Backes et al. [3] proposed a new social relationship reasoning mechanism, which can predict the social relationship between two people without

J. Xiong et al. (Eds.): MobiMedia 2021, LNICST 394, pp. 577–590, 2021.
https://doi.org/10.1007/978-3-030-89814-4_42

any prior knowledge. Shan et al. [4] proposed a method to control the access rights of resources in social networks by using different relationships to correspond to different access rights. Voloch et al. [5] proposed a new role and trust based access control model to evaluate each user's trust by several standards. Users with specific roles and appropriate permissions can access some instances of data if they do not reach a sufficient level of trust. These roles and trust assessments provide more accurate and feasible information sharing decisions and better control of privacy in social networks. Yousra et al. [6] proposed a community-centered broker-aware access control (CBAC) model, which uses important concepts from social network analysis (SNA), namely broker, one-to-many relationship, temporary relationship and emerging access control models such as attribute-based and trust-based access control and decentralized strategies. Xu et al. [7] proposed a trust-based access control mechanism Trust2Privacy to protect the privacy of users after releasing information, which can effectively realize the conversion from trust to privacy. Zhu et al. [8] proposed an online social network rumor propagation model with forced silence function. Aljably et al. [9] proposed a privacy protection model, which uses limited local differential privacy (LDP) to save the composite copy of the collected data, so as to purify the user information collected from social networks. The model further uses reconstructed data to classify user activities and detect differences. Alemany et al. [10] proposed two soft-paternalism mechanisms that provide information to the user about the privacy risk of publishing information on a social network. That privacy risk is based on a complex privacy metric. The results show that there are significant differences in teenagers' behaviors towards better privacy practices.

Shan et al. [11] proposed a social network forwarding control mechanism based on game theory on the basis of analyzing the benefits of both forwarding parties. On the basis of analyzing the benefits of different game strategies selected by the forwarder and the publisher, they compared the historical data of forwarding operations with the threshold set by the publisher, and gave the final decision whether to allow forwarding. Can effectively prevent the forwarder's dishonest forwarding behavior. Wu et al. [12] verified the constructed privacy random game model and the new privacy risk measurement criterion, and solved the strategy by reinforcement learning algorithm, and obtained effective personal access control strategy.

In order to protect the privacy information of users in multi-user photos, Xu et al. [13] proposed a multi-user photo privacy protection model based on face recognition technology. Bernstein et al. [14] further proposed a screen shooting interference system to prevent camera privacy leakage. Li et al. [15] proposed an access control model CoAC for cyberspace, which can effectively prevent the security problems caused by the separation of data ownership and management rights, and the secondary/multiple forwarding of information. Marinescu et al. [16] proposed an access control method that can automatically learn the authorization rules to form a model, judge the newly launched access request, and prevent any access request that may attempt to use the loopholes in the authorization logic of social networks. In addition, privacy protection access control schemes [17] applied to information-centric networks and access control schemes for health information [18] also emerged.

Zhang PanPan et al. [19] proposed a game metric model based on privacy preference for the equilibrium problem between privacy protection and service quality. Zhang

Chao et al. [20] proposed a privacy-preserving social network information recommendation method based on information dissemination model. Lei [21] et al. proposed a hierarchical management scheme for friend matching using attributes to promote secure friend discovery in MSN. The scheme involves the establishment of several attribute centers, which perform fine-grained management according to various user attributes. Alshareef [22] et al. proposed a new collaborative access control framework that takes into account the relationship between multiple users' viewing and sharing items, and ultimately resolves conflicts in user privacy settings. G Liu et al. [23] model trust by proposing the three-valued subjective logic (3VSL) model. 3VSL properly models the unertainties that exist in trust, thus is able to compute trust in arbitrary graphs. Based on the 3VSL model, they further design the AssessTrust (AT) algorithm to accurately compute the trust between any two users connected in an OSN. And it is verified that 3VSL can accurately simulate the trust relationship between any pair of indirectly connected users in Advogato and PGP.

The existing access control mechanism for social privacy protection has formulated access strategies for users' privacy needs in different environments, but it ignores the impact of users' personal preferences on access control strategies. To solve this problem, this paper proposes a user preference analysis mechanism, and constructs an information sensitivity model by using the amount of privacy information. On the basis of this model, the influence of user personality differences on the degree of privacy is studied. By using the method of arctangent and privacy measurement, combined with information entropy, weighted information entropy and other technologies, the user preference analysis mechanism for social networks is finally constructed. This mechanism is used to quantify the user preference value as one of the feature vectors of SVM for the analysis of access control strategy. Experiments show that the access control strategy with the personal preference analysis mechanism significantly improves the protection of privacy information of different users for different social objects. More reasonable and effective solution to social platform user privacy resources leak.

2 Basic Knowledge

2.1 SVM

The earliest origin of SVM is in pattern recognition, a classifier algorithm developed from generalized portrait algorithm, which is an algorithm for binary classification of the data to be processed in a supervised learning manner, a generalized fast and reliable linear classifier, and also supports nonlinear classification, which is better for solving the problem of small samples.

The sample set $S = \{(x_i, y_i); i = 1, ..., m\}$ of the given training, where $x_i \in R^n$ represents the n-dimensional input vector, and y_i is the marker for each vector. SVM works by constructing a hyperplane (w, b).

$$w^T x_i + b = 0 \tag{1}$$

The distance between any point x and the hyperplane is:

$$\gamma = \frac{|w^T x + b|}{||w||} \tag{2}$$

After the duality problem and the soft spacing

$$\min_{w,\,b} \frac{1}{2} w^T w + C \sum_{i=1}^{N} \xi_i \tag{3}$$

$$y_i \left(w^T x_i + b \right) \geq 1 - \xi_i \tag{4}$$

$$\xi_i \geq 0, i = 1, 2, ..., N \tag{5}$$

$y_i \left(w^T x_i + b \right) \geq 1 - \xi_i$ is a quadratic programming problem, which becomes a maximization problem after duality:

$$\max_{\alpha} \sum_{i=1}^{N} \alpha_i - \frac{1}{2} \sum_{i=1}^{N} \alpha_i \alpha_j y_i y_j K\left(x_i, x_j\right) \tag{6}$$

$$s.t. \sum_{i=1}^{N} \alpha_i y_i = 0;\ 0 \leq \alpha_i \leq C, i = 1, 2, \ldots N \tag{7}$$

2.2 Information Entropy

Shannon proposed the concept of "information entropy" to solve the problem of quantitative measurement of information. From the perspective of information transmission, information entropy can represent the value of information. Simply put, the lower the probability of an event happening, the more information it can give when it happens. The calculation formula of information entropy is as follows:

$$H(x) = -\sum P(x_i) \log(2, P(x_i)) \tag{8}$$

3 Smart Access Control of User Preferences Based on SVM

3.1 Quantitative Analysis of User Preferences

The factors affecting user access control privileges are not only uniform or generalized sensitive information, but also influenced by user personality traits, social circles, specific content of posted resource information, etc. In order to more accurately formulate access control policies for network users, it is required to add the analysis of different users' personalized preferences based on the traditional social access control architecture. Therefore, this paper proposes a user preference analysis mechanism, and its technical route is shown in Fig. 1.

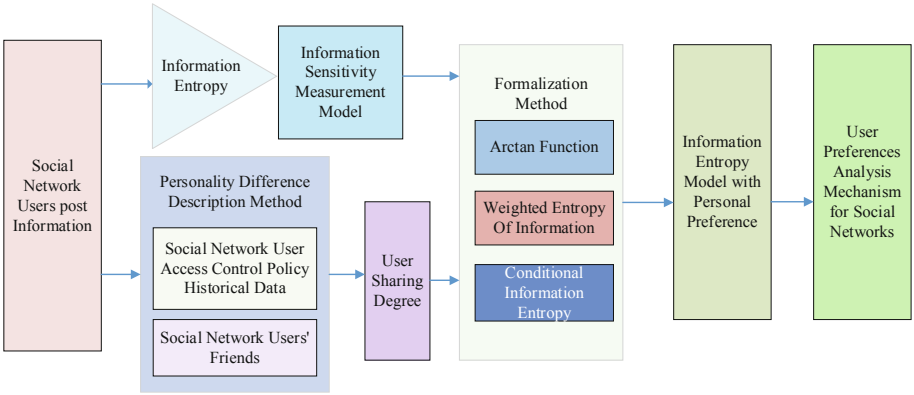

Fig. 1. A mechanism for analyzing user preferences.

In social networks, the information uploaded by users to social networks contains different degrees of privacy information, which requires different access control strategies. Firstly, information entropy is used to describe the privacy information contained in the information, to determine the degree of privacy of the information, and to construct the basic information sensitivity measurement model.

Specifically, $x_i \in X$ denotes the ith message posted by a social network user, $p(x_i)$ denotes the proportion of the amount of private information contained in the ith message to the amount of all the user's private information, and the source of the information posted by the user in the social network is denoted as below.

$$\begin{pmatrix} X \\ P(x) \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \ldots & x_i & \ldots & x_n \\ p(x_1) & p(x_2) & \ldots & p(x_i) & \ldots & p(x_n) \end{pmatrix} \tag{9}$$

Where $0 \leq p(x_i) \leq 1$, $\sum_{i=1}^{n} p(x_i) = 1$.

The information source entropy of the released information is denoted as:

$$H(x) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i) \tag{10}$$

$H(x)$ represents the average private amount of information released by users in the social network, where N represents the total amount of information released by users.

Specifically, $x_i \in X$ denotes the ith message posted by the user in the social network, $f \in N$ denotes the number of friends the user has in the social network, f_a^i denotes the number of allowed visible friends set when the user uploads the ith message, and $w(f)$ is the user's social breadth function, calculated as follows.

$$w(f) = 2/(\pi \arctan f) \tag{11}$$

Where $f \in N, 0 \leq f < +\infty$. This function satisfies the following properties: (1) the social breadth of the user $w(f) \in (0, 1)$; (2) social breadth increases with the number of

users' friends in the social network. Therefore, function $w(f)$ monotonically increases within the value range of f.

h_i denotes the degree of confidentiality of the ith message and is calculated as follows:

$$h_i = f_a^i / f \tag{12}$$

Denotes the ratio of the number of friends allowed to view the ith message xi to the total number of friends of the user, the greater of the number of friends allowed to view, the lower the degree of confidentiality of the information.

s_i denotes the sharing degree of the ith message, which is calculated as follows:

$$s_i(f, f_a^i) = h_i \times w(f) = (2f_a^i)/(\pi f \arctan f) \tag{13}$$

The above equation is used to describe the number of friends f of a user and the influence of the number of friends f_a^i allowed to be seen in the access control policy on the sharing degree of information x_i. The more friends a user has and the more friends they are allowed to view, the higher the sharing degree of information xi, and vice versa.

The sharing space of information released by users is as follows:

$$\begin{pmatrix} X \\ S(X) \end{pmatrix} = \begin{pmatrix} x_1 x_2 \ldots x_i \ldots x_n \\ s_1 s_2 \ldots s_i \ldots s_n \end{pmatrix}, \quad 0 < s_i < 1, i = 1, 2, \ldots n \tag{14}$$

Define source entropy with personal preferences:

$$H_s(x) = -\sum_{i=1}^{n} s_i p(x_i) \log_2 p(x_i) \tag{15}$$

$H_s(x)$ describes the influence of different user preferences on the privacy degree of information published in social networks by sharing degree S_i (i = 1, 2…N), and realize the analysis and measurement of user preferences.

3.2 Access Control Mechanism of Social Network Based on User Preference

An access control mechanism model based on user preferences is shown in Fig. 2, the model includes:

User: Used to describe a registered user in a social network platform, user set U, $U \in \{u_1, u_2, ..., u_n\}$. Each user can upload user resources through the social platform and access other user resources under the conditions of permission. User resources include text, images, videos, etc. And different access control requests can be made according to different user resources.

User resources: Used to describe the user information generated by the user in using the social platform, including the user's autonomously uploaded resources and the access control policy records for the resources and the user's social network relationship graph.

All user's resource: It is used to describe the user information based on all registered users in the social platform in the process of use. Including all user resources and their access control policy records.

Preference analysis mechanism: Quantitative analysis of user's personal preferences and obtaining user preference values by analyzing user's access control policy records and user resources. It is one of the evaluation elements of the access control evaluation module.

Access control module: Generate resource access control policies with user preferences by analyzing user resources, user preference values, all user resources and their access control policy records.

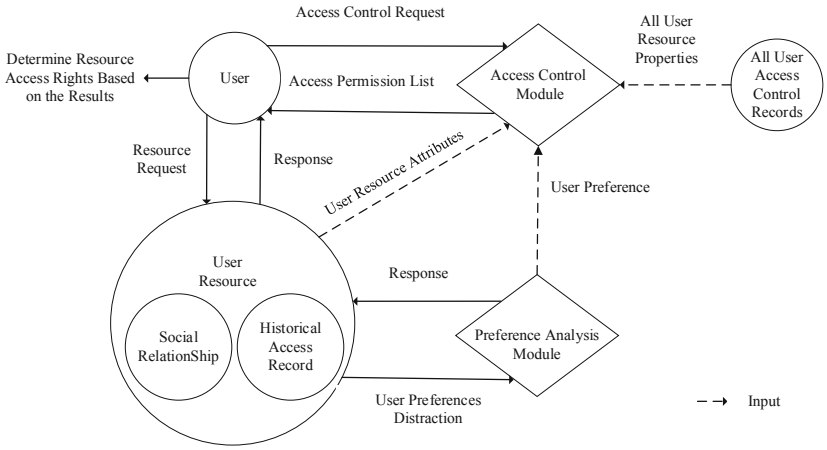

Fig. 2. An access effect model based on user preferences.

The basic steps are as follows:

When users publish user resources, they first make resource request and access control request for user resources and access control module respectively.

The user resource responds after receiving the request, and the user's historical access control records and social network relationships are analyzed to form user access control attributes.

User resources are taken as input to conduct user preference analysis and obtain user preference values.

Analyze all user resources and their access control policy records, and get all user resource attributes.

When the access control evaluation module receives the user resource attribute, all user resource attribute and user preference value, it generates the user resource access control policy, and returns the access permission list to the user after responding to the user's access control request.

The user determines the resource access control rights through the result of the permission list.

3.3 Access Control Policy Generation Method

We preprocessed the data of users' historical resource records, friend relationship graphs and user preferences obtained through preference analysis mechanism in the social network platform, and divided the processed data into training set and test sets, so as to avoid the over-fitting problem. After that, the machine learning model will be generated by the training set through the machine learning algorithm, and the prediction model will be generated through the test set. Finally, the resources to be processed will be input as the model, so as to get the access rights list of the user's resources this time. Training and validation of access control model is shown in Fig. 3.

User resource information is divided into high, medium and low levels (represented by H, M and L respectively). Personal privacy preference is divided into high, medium and low levels (represented by H, M and L, respectively). The degree of privacy is divided into five grades: very high, high, medium, low and very low (represented by VH, H, M, L and VL, respectively). The higher the amount of privacy information a user requests for access control resources, the higher the corresponding privacy degree will be, the higher the personal privacy preference will be, and the corresponding privacy degree level will also improve. The details are shown in Table 1.

4 Analysis of Experiment and Application Examples

In this experiment, the prediction model of SVM is used to carry out the experiment. The author conducted research in this field during his doctoral study and published relevant papers in this field. From the author's previous research results, we can conclude that SVM algorithm is the best choice for this mechanism.

4.1 Data Set

The author's research group has developed its own information sharing system with functions such as instant messaging and information release in social networks. The

Table 1. The relationship between the degree of privacy and Privacy information/Personal Privacy preference.

Privacy information	Personal privacy preference	Degree of privacy
H	H	VH
H	M	H
H	L	M
M	H	H
M	M	M
M	L	L
L	H	M
L	M	L
L	L	VL

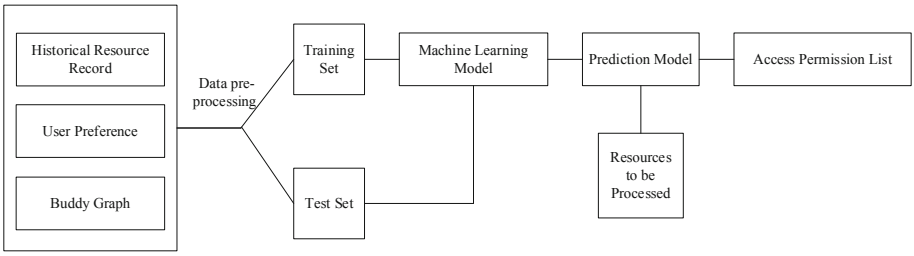

Fig. 3. Training and validation of access control model.

system is open to use in the institute. Registered users can add friends, upload resources and set access control policies. After several months of operation, the data of 60 users in the system were selected as the research object. The study subjects had an average of 200 friends in the system. Then, 10 generated resources of each research object are extracted as decision data, and the amount of decision data of the research object is equal to the number of its friends, with an average of 200. A total of 120,000 pieces of basic data were generated by 60 research subjects, which constituted the data set of the experiment in this paper. Each basic data is preprocessed to obtain a five-dimensional vector eigenvalue and a Boolean target value, which correspond to the training data. 120,000 training data after processing constitute the training sample set.

4.2 Comparison of Models

In this experiment, SVM algorithm is used to build the model. In order to verify the effectiveness of the personal preference analysis mechanism proposed by the author, the SVM algorithm is used to construct two models, one model with the personal preference analysis mechanism proposed by the author, the other model without the personal preference analysis mechanism. Compare the performance of the two models. When comparing results, the index of model performance is accuracy.

$$Accuracy = \frac{TP}{TP + FP} \tag{16}$$

Where TP represents the number of people the system recommends to be visible and the user Settings are also visible. FP represents the number of people whose user Settings are not visible but whose system Settings are.

4.3 Development Platform and Environment

The experimental environment is as follows.

CPU: Dual core I7-3770, 3.4 GHz;
Memory is DDR 4B; The hard disk is 256;
The operating system is Windows 10.
The design language is Python 3.6.5 (64-bit).
In the process of programming, SVM model is realized by Sklearn 0.21.3 package.

4.4 Experimental Results Comparison

The data set of this experiment is trained by proposing solutions. When SVM is used for data training, RBF function is selected. Constant C is used to balance training error and γ is used by RBF kernel function in machine learning process. When optimizing parameters C and γ, the grid search algorithm is used to improve the accuracy of the algorithm. Grid search method is an exhaustive search method for specifying parameter values. The optimal learning algorithm can be obtained by optimizing the parameters of the evaluation function through cross validation.

After grid search optimization, the values of the optimal parameters C and γ are 2^{10} and 2^{0}. It can be clearly seen from Fig. 4 that when the number of folds of cross validation is 10, the SVM model with the personal preference analysis mechanism is the most accurate. With the increase of the number of folds, the accuracy will increase and decrease, but 10 folds cross validation is the best. However, the SVM model without the personal preference analysis mechanism, no matter how many folds, is not as good as the SVM model with the personal preference analysis mechanism.

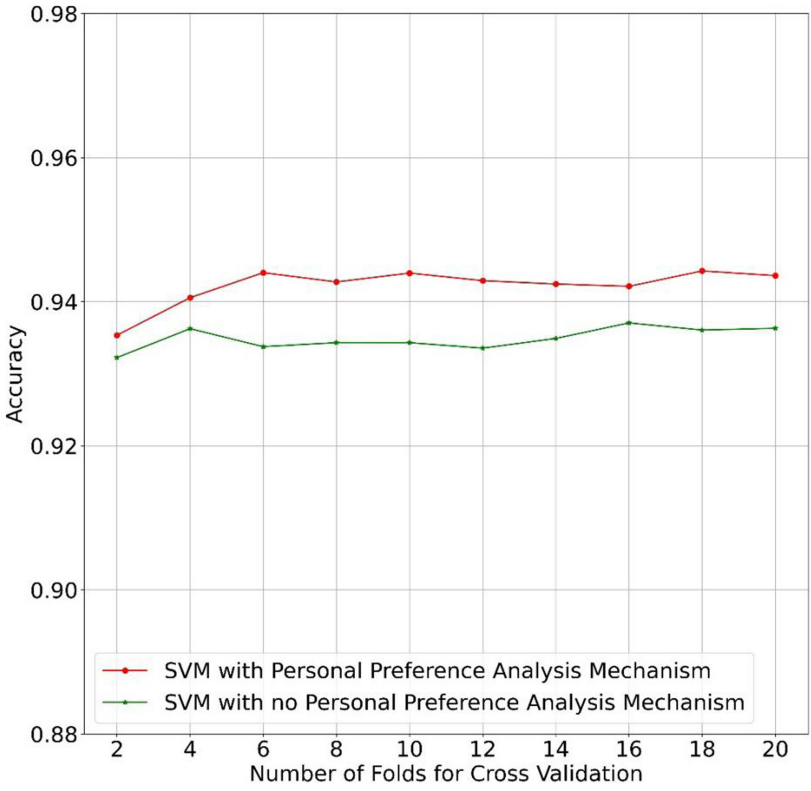

Fig. 4. Comparison of model accuracy with different cross-validation fold.

Figure 5 shows the AUC (Area Under Curve) image. What we know is that this model is optimal if the AUC value is closer to 1. It can be seen from Fig. 5 that the AUC value of the SVM model with the personal preference analysis mechanism added is greater than that of the SVM model without the personal preference analysis mechanism added. Through program calculation, the AUC value of the SVM model with the personal preference analysis mechanism is 0.9599, and that of the SVM model without the personal preference analysis mechanism is 0.9518. The difference between the two is 0.0081. According to Fig. 5, it can also be concluded that the SVM model with personal preference analysis mechanism is the optimal one.

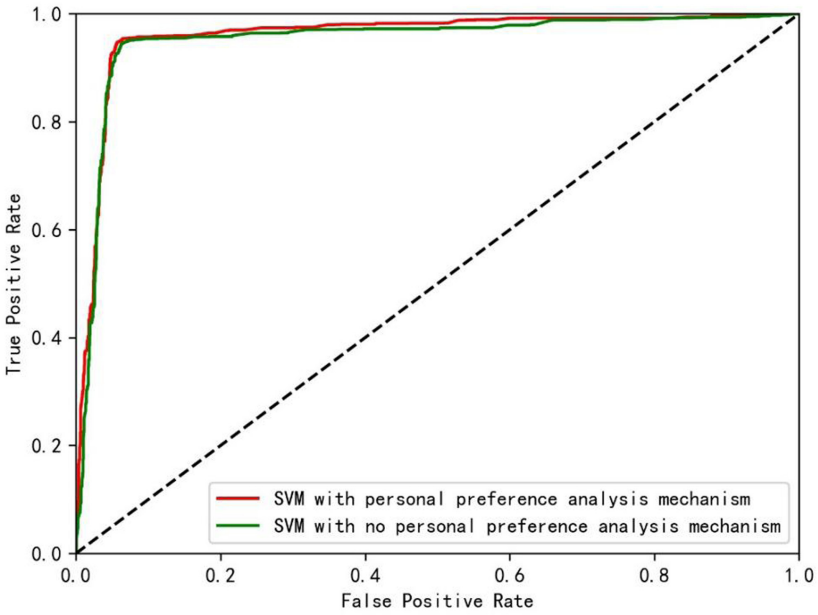

Fig. 5. AUC image.

5 Comparison

This section discusses several related works on access control schemes based on personal preferences, and compared with the schemes proposed in literature [7, 21, 22], the comparison results are shown in Table 2.

Table 2. Comparison of characteristics of different schemes.

	Literature [21]	Literature [22]	Literature [7]	The scheme of this paper
Quantify personal preferences	×	×	×	√
Privacy metric	×	√	√	√
User relationship	√	√	√	√
Sensitive level	√	×	√	√
Trust value	√	×	√	√
Policy individualization	√	√	×	√
History	√	√	√	√

The first column of Table 2 represents seven characteristics to be discussed in this section. The three columns in the middle are the characteristics of the other three programmes. The last column is the characteristics of the scheme in this article.

The scheme proposed in [21] a multi-user collaborative access control framework, which considers the relationship between multiple users and projects, solving conflicts in the privacy settings of the users involved. The method was experimented on an open source social network called Diaspora. However, this solution only solves the privacy Settings between users related to the project, users unrelated to the project are not taken into account. At the same time, users related to the project are difficult to define, and it is difficult to determine which users are related to the project and which are not. There is no privacy measurement and no integration of personal preferences into access control mechanisms.

Literature [22] proposed a scheme that only the friend data requestor whose attributes meet the access policy can decrypt the ciphertext and continue to conduct further communication. In this scheme, it was proposed that taking Weibo social network as an example, everybody has different attributes under different scenarios. However, when registering on Weibo, it is possible to initialize its own properties without setting the properties. Then according to the rules of the scheme, only friends with the access policy satisfied by the attribute can access the data, which is very unfair to a new user who has not set the attribute. At the same time, it also causes pressure to users. This scheme does not take into account the trust value between users and the sensitivity of privacy items, but only generates an access control policy after matching the encryption and decryption of attributes. The scheme in this paper will be more convenient to generate an access policy.

Literature [7] proposed Trust2Privacy, a trust-based access control mechanism to protect the personalized privacy of users after posting their information, which can effectively realize the transformation from trust to privacy. The scheme is similar to the scheme proposed in literature [21] and this paper, for example, the trust value between users and the relationship between users are considered. It is worth noting that the

individual location information is taken into account in literature [7]. It is interesting and innovative to add location information to the privacy protection of social networks, but location can also expose a person's privacy. As for the transmission and protection of location, this literature does not involve more studies and put forward corresponding measures. Also, as we know, the current social media software needs to be authorized by the mobile device to obtain an individual's location, so I think the acquisition of location information is difficult for this mechanism. Similarly, literature [7] does not take into account the personal preferences of users, and the access control policies formulated are not more personalized.

6 Conclusion

This paper proposed a social network access control model based on user preferences, proposes a quantification of user privacy preferences by analyzing user historical access control records, and integrates relationship types, access control contents, and user personal preference information entropy as feature vectors, proposes access control policies for user resources in social network platforms by support vector machine algorithm, and generates corresponding access control permission list. The proposed method of quantifying user privacy preferences first constructs an information sensitivity model by the amount of user privacy information and the degree of information privacy, then determines the user sharing degree by personality difference description, and later uses a formal method to determine the information entropy of user personal preferences. Thus, the access control policy is made more consistent with users' personal privacy needs. Therefore, in the next step of the research, natural language processing is used to analyze user text resources and informative labeling and classification so as to protect user privacy in terms of public privacy information attributes, and privacy analysis of user audio and video resources to expand the scope of social network access control processing.

Acknowledgments. The research activities described in this paper have been conducted within "the key R & D and Promotion of Special Science and Technology Projects of Henan Province (212102310480)".

References

1. Pang, J., Yang, Z.: A new access control scheme for Facebook-style social networks. Comput. Secur. **54**(1), 44–59 (2015)
2. Cheng, Y., Park, J., Sandhu, R.: A user-to-user relationship-based access control model for online social networks. In: Cuppens-Boulahia, N., Cuppens, F., Garcia-Alfaro, J. (eds.) DBSec 2012. LNCS, vol. 7371, pp. 8–24. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-31540-4_2
3. Backes, M., Humbert, M., Pang, J, et al.: walk2friends: inferring social links from mobility profiles. ACM (2017)
4. Shan, F., Hui, L., Li, F., et al.: HAC: hybrid access control for online social networks. Secur. Commun. Netw. **2018**, 1–11 (2018)

5. Voloch, N., Nissim, P., Elmakies, M., Gudes, E.: A role and trust access control model for preserving privacy and image anonymization in social networks. In: Meng, W., Cofta, P., Jensen, C.D., Grandison, T. (eds.) IFIPTM 2019. IAICT, vol. 563, pp. 19–27. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-33716-2_2
6. Yousra, A., Kamran, M.A., Basit, R., et al.: Community-centric brokerage-aware access control for online social networks. Future Gener. Comput. Syst. **109**, 469–478 (2018)
7. Xu, G., Liu, B., Jiao, L., et al.: Trust2Privacy: a novel fuzzy trust-to-privacy mechanism for mobile social networks. IEEE Wirel. Commun. **27**(3), 72–78 (2020)
8. Zhu, L., Wang, B.: Stability analysis of a SAIR rumor spreading model with control strategies in online social networks. Inf. Sci. **526**, 1–9 (2020)
9. Aljably, R., Yuan, T., Al-Rodhaan, M., et al.: Anomaly detection over differential preserved privacy in online social networks. PLoS ONE **14**(4), e0215856 (2019)
10. Alemany, J., Val, E.D., Alberola, J., et al.: Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms. Int. J. Hum. Comput. Stud. **129**, 27–40 (2019)
11. Shan, F., Li, H., Zhu, H.: A game theory-based forwarding control mechanism for social networks. J. Commun. **39**(003), 172–180 (2018)
12. Yu, W., Li, P.: SG-PAC: a stochastic game approach to generate personal privacy paradox access-control policies in social networks. Comput. Secur. **102**, 102157 (2020)
13. Xu, K., Guo, Y., Guo, L., et al.: My privacy my decision: control of photo sharing on online social networks. IEEE Trans. Dependable Secure Comput. **14**(2), 199–210 (2017)
14. Bernstein, M., Bakshy, E., Burke, M., et al.: Quantifying the invisible audience in social networks. In: Proceedings of Human Factors in Computing Systems, pp. 21–30 (2013)
15. Li, F.H., Wang, Y.C., Yin, L.H., et al.: A cyberspace-oriented access control model. J. Commun. **7**(5), 9–20 (2016)
16. Marinescu, P., Parry, C., Pomarole, M., et al.: IVD: automatic learning and enforcement of authorization rules in online social networks. In: S&P 2017, pp. 1094–1109 (2017)
17. Li, B., Huang, D., Wang, Z., et al.: Attribute-based access control for ICN naming scheme. IEEE Trans. Dependable Secure Comput. **15**(2), 194–206 (2018)
18. Yeh, L., Chiang, P., Tsai, Y., et al.: Cloud-based fine-grained health information access control framework for lightweight IoT devices with dynamic auditing and attribute revocation. IEEE Trans. Cloud Comput. **6**(2), 532–544 (2018)
19. Zhang, P.P., Peng, C.G., He, C.Y.: A privacy protection model based on privacy preference and its quantification method are presented. Comput. Sci. **45**(006), 130–134 (2018)
20. Zhang, C., Liang, Y., Fang, H.S.: Social network information recommendation method that supports privacy protection. J. Shandong Univ. (Nat. Sci. Ed.) **55**(03), 13–22 (2020)
21. Alshareef, H., Pardo, R., Schneider, G., et al.: A collaborative access control framework for online social networks. J. Logical Algebraic Meth. Program. **114**, 100562 (2020)
22. Lei, Z.A., El, B., Gw, C., et al.: Secure fine-grained friend-making scheme based on hierarchical management in mobile social networks. Inf. Sci. **554**, 15–32 (2021)
23. Liu, G., Yang, Q., Wang, H., et al.: Trust assessment in online social networks. IEEE Trans. Dependable Secure Comput. **18**(2), 994–1007 (2021)