IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON MOBILE MULTIMEDIA: METHODOLOGY AND APPLICATIONS

Received December 3, 2019, accepted December 17, 2019, date of publication January 3, 2020, date of current version January 17, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2963932

A Smart Access Control Method for Online Social Networks Based on Support Vector Machine

FANGFANG SHAN[1,2,3], JIZHAO LIU[2], XUEYUAN WANG[3], WEIGUANG LIU[2], AND BING ZHOU[1,3]

[1]School of Information Engineering, Zhengzhou University, Zhengzhou 450000, China
[2]School of Computer Science, Zhongyuan University of Technology, Zhengzhou 450000, China
[3]Collaborative Innovation Center of Internet Healthcare, Zhengzhou University, Zhengzhou 450000, China

Corresponding author: Fangfang Shan (6129@zut.edu.cn)

This work was supported in part by the Science and Technology Research Program of Henan Province of China under Grant 182102210130.

ABSTRACT With the rapid development of Internet technology, online social networks (OSNs) has become one of the main ways for people to develop social activities. In order to maintain and strengthen interpersonal relationships, users are willing to share personal behaviors, feelings and other things through OSNs. Whether these resources reveal private information or not depends on the appropriateness of the access control policies set by the owner. However, with the increasing number of friends and complex relationships, it becomes more and more difficult for OSNs users to set appropriate access control policies. Aiming at above problems, a smart access control method for online social networks is proposed based on SVM algorithm to realize smart access control on the basis of integrating relationship types and description information of published content as eigenvectors. The experimental results show that this mechanism can automatically recommend the list of visible friends according to the content published by users and the relationship between users and friends, allowing users to modify the list to obtain the final access control policy, which can effectively protect users' privacy information.

INDEX TERMS Online social networks, access control method, support vector machine, machine learning.

I. INTRODUCTION

With the rapid development of Internet technology and communication technology, more and more people choose to communicate with each other through OSNs, and lots of enterprises use OSNs to carry out business activities. In OSNs, users can share various resources which may be public or protected by access control policies, including text, photos, videos and other contents. The users and the relationships between them constitute the social network graph. Information and resources flow in the online social network under the constraint of the graph.

Friendly and easy-to-use interface, convenient and diverse functions attract a lot of users to use online social networks more frequently. As the development of wireless communication technology, for example, the development of 5G, it becomes more and more convenient for people to access to the internet through wireless networks [1], [2]. This boosts the development of online social networks. It brings a lot of information security issues as well [3]. According to statistics, Facebook has 1.55 billion active users each month, and 84% of them use mobile clients to log on to Facebook [4], [5]. Its daily online users are even close to 100 million. While making it easier for users to share information, online social network also brings privacy issues [6], [7]. One of the important reasons is that adding strangers as friends in the virtualized social network environment may expose a lot of personal information [8]–[10]. However, few users realize that the disclosure of private information may do harm to them [11], and even fewer users can set access control policies correctly when publishing resources in OSNs.

A smart access control method for online social networks is proposed in this paper. The proposed method uses support vector machine (SVM) algorithm to study the access control problem in social networks. Firstly, it integrates relationship type, the description of the content information as feature vector. Then, the support vector machine (SVM) algorithm is adopted to realize the automatic generation of access control policies. The grid search method is used to optimize parameters for SVM machine learning algorithm.

The associate editor coordinating the review of this manuscript and approving it for publication was Dapeng Wu.

Finally, experiments are arranged to verify the effectiveness of the proposed mechanism in helping users to generate effective access control policy. By allowing users to modify the access control policies on the basis of personal characters, the proposed mechanism can better achieve the purpose of privacy protection.

In summary, the contributions of this paper are as follows:

1) We use both attributes of resources and relationships between users to generate access control policies in OSNs. Compared with access control methods that just consider relationships, this method can express different protect need of various contents that contain different privacy information. It can achieve fine-grained access control of contents uploaded to OSNs.

2) After a lot of experiments, we use SVM to train the prediction model. As the 10-fold cross-validation method and the grid search method are used in the model training procedure, high computational accuracy can be achieved.

3) We propose a smart access control method for OSNs which can intelligently and automatically generate access control policies according to the resource that will be uploaded to the OSN and relationships between friends and the OSN user. It can recommend a list of friends who can access a specific piece of resource according to the resource's attributes without any help of users which simplifies the generation of access control policies and save time of OSNs users.

The rest of this paper is organized as follows. Section 2 discusses the related work. Section 3 introduces related theories and techniques. Smart access control method for online social networks and parameter optimization of SVM prediction model based on grid search are presented in Section 4. Section 5 presents experimental results and discussions. Section 6 compares several access control methods of OSNs with the smart one proposed in this paper. Section 7 concludes the paper.

II. RELATED WORK

For the problem of social network privacy protection, the current academic solutions focus on access control technology. Most of them fall into one of three categories listed below.

A. RELATIONSHIP BASED ACCESS CONTROL

Gates [12], Carminati and Ferrari [13], and Fong *et al.* [14] used the relationship between users in social networks to determine whether visitors can access to resources. Fong [15], Fong and Siahaan [16], and Bruns *et al.* [17] used modal logic language to define access control strategies in social networks and proposed an access control model based on mixed logic. Park *et al.* [18] and Cheng *et al.* [19] used regular expressions to define access control policies, enabling user-user relationships, user-resource relationships, and resource-resource relationships to control visitors' access to resources. This kind of methods provides users with a way to control access rights to resources in OSNs. Different relationship is related to different access rights. Relationship based access control method is simple to understand and easy to implement in commercial OSNs. However, given a resource, it is hard for users to determine to which access rights a relationship should be related.

B. CRYPTOGRAPHY BASED ACCESS CONTROL

Pang and Zhang [20] used cryptography to solve access control and privacy protection problems in social networks, which also pointed out a new development direction for access control technology in social networks. This kind of access control method is capable to describe situations like 'k-common friends' and 'k-depth'. It is more powerful than traditional relationship based access control methods. However, as cryptography algorithms need to be performed, it may take up more spacial and computational resources of computers.

C. GAME THEORY BASED ACCESS CONTROL

Wellman and Berkowitz [21] used game theory to analyze the benefits of content visitors and content owners in social networks and proposed a new access control mechanism. Tian and Lin [22] proposed a game control mechanism, which used game theory to analyze the behavior of users in social networks and controls access to resources in social networks through trust prediction of user behavior. Yu *et al.* [23] established a game model for competitive information dissemination in social networks to understand the influence of human behaviors such as knowledge, interest, money and learning desire on competitive information dissemination. Zhang *et al.* [24] used game theory to calculate the income of resource visitors and resource publishers to obtain Nash equilibrium and decide whether to allow access to resources. Zhu *et al.* [25] applies repeated games and incentive mechanism to improve the efficiency of resource sharing in social networks. Zhang *et al.* [26] used game theory to protect the privacy information of users in social networks from the perspective of the benefits of both parties to social network content access and considering the impact of historical access data on current benefits. However, all the above access control methods cannot intelligently give users advices about how to make access control policies.

The existing access control methods which are based on relationship and game theory only restrict the access operation of resources and cannot provide appropriate access control policies to users. Inappropriate access control policies will bring serious consequences to OSNs users, and even threaten the security of themselves and their families. For example, uploading information related to users' daily routines frequently may make criminals infer the family situation and daily working hours, which may lead to the occurrence of robbery cases and even threaten the safety of their lives. The users who post pictures of their children and school schedules may arouse strangers to abduct them by pretending to be relatives to pick them up. Therefore, it is very important for resource publishing users in social network to set appropriate access control policies for resources. How to judge whether

the access control policies are appropriate or not and how to recommend them to users intelligently are urgent problems to be solved.

III. RELATED THEORIES AND TECHNIQUES

Support vector machine (SVM) is a supervised learning model based on VC dimension theory and structural risk minimum principle. Provided with a limited sample set, it can balance the accuracy and the learning ability of the model, and solve the problem of small sample learning pretty well. Its core theory was proposed by Vapnik and Cortes in the 1990s [27]–[29].

Suppose there is a set of training samples $\{x_l, y_l\}_{l=1}^{n}$, where $x_l \in R^d$ is the input vector of d dimension and $y_l \in \{-1, +1\}$ is the category marker. SVM needs to construct an optimal classification hyperplane to correctly separate the two types of training samples and ensure the maximum classification interval (margin). The classified hyperplane can be obtained by solving the following optimization problems.

Under the constraints of equations (1) and (2), minimize equation (3).

$$y_i((w \cdot x_i) + b) \geq 1 - \xi_i \tag{1}$$

$$\xi_i \geq 0, \quad i = 1, 2, \ldots, n \tag{2}$$

$$\frac{1}{2}(w^T \cdot w) + C \sum_{i=1}^{n} \xi_i \tag{3}$$

where ξ_i is the training error of the linearly indivisible training sample. Equation (1) is used to ensure the correct classification of training samples. The constant C in equation (3) is used to balance training errors and algorithm complexity.

The above minimization problem is a quadratic programming problem, which is equivalent to maximize equation (6) under the constraints of equations (4) and (5).

$$\sum_{i=1}^{n} \alpha_i y_i = 0 \tag{4}$$

$$0 \leq \alpha_i \leq C, \quad i = 1, 2, \ldots, n \tag{5}$$

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

By solving the above quadratic programming problem, the decision function shown in equation (7) is finally obtained.

$$f(x) = sign\left[\left(\sum_{i=1}^{n} \alpha_i y_i K(x, x_i)\right) + b\right] \tag{7}$$

In order to solve the problem of linear inseparability of training samples, kernel function is introduced. Any function that satisfies the Mercer condition can be used as a kernel function in SVM. Common kernel functions include polynomial kernel, RBF kernel, Sigmoid kernel and so on. The most commonly used RBF kernel is selected in this paper.

$$K(x, x') = \exp\left\{-\frac{\left\|x - x'\right\|^2}{\gamma}\right\} \tag{8}$$

where γ is the parameter to be optimized in the process of machine learning.

IV. RESEARCH METHOD

According to the characteristics of access control data in OSNs and the related technologies described in section 3, this section presents the SVM-based access control method for online social networks and introduces the corresponding parameter optimization algorithm based on grid search.

A. SMART ACCESS CONTROL METHOD FOR ONLINE SOCIAL NETWORKS

The SVM-based smart access control model for online social networks is shown in Figure 1. The model includes user, session, history record, user record, social network graph and smart access control part.

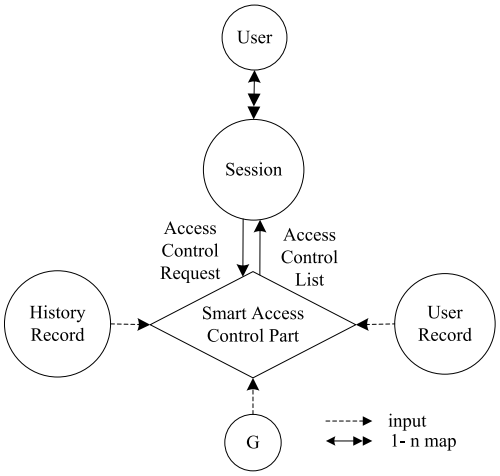


FIGURE 1. The SVM-based smart access control model.

User: Users are social network registered person who initiate access control request, upload texts, pictures, videos and other resources through online social network, and set their access control policies. The user set is denoted as U, and its elements are denoted as u.

Session: Session is used to describe an active entity of a logged user in online social network. The set of user sessions is called S_U.

History Record: History records are resources uploaded by OSNs users and access control policies set for resources, which are denoted as H_R.

User Record: User record is the resource will be uploaded by the registered OSNs user who initiated the access control request, which is recorded as UR.

Social Network Graph: The social network graph is used to describe relationships between registered users of a social network, denoted as G.

First, the user U initiates an access control request to the smart access control part through the session S_U. Then, the smart access control part trains access control model based on the data set H_R. At last, the access control model is

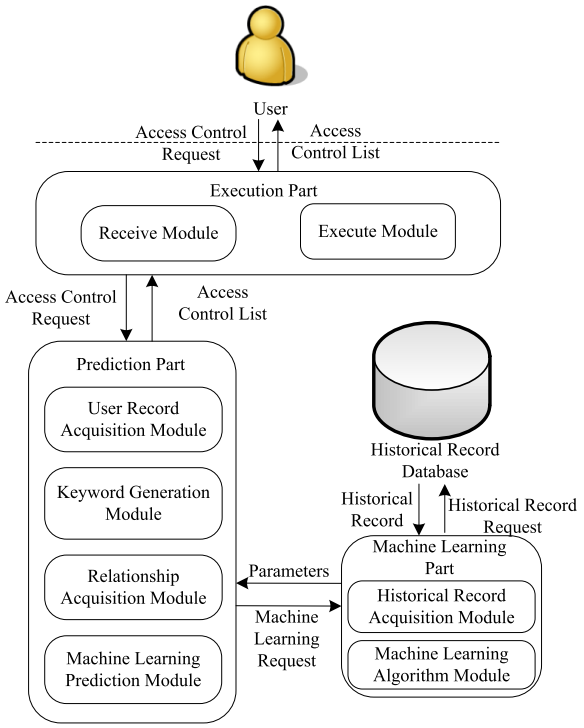


FIGURE 2. Smart access control mechanism architecture based on SVM.

used to predict user's record *UR*, and finally the access control list is obtained.

1) SMART ACCESS CONTROL MECHANISM ARCHITECTURE BASED ON SVM

Considering the data characteristics of access control in OSNs and the basic principle of support vector machine, the architecture design of smart access control mechanism based on SVM constructed in this paper is shown in Figure 2, including four components, namely the execution part, the prediction part, the machine learning part and the historical record database. The execution part is responsible for receiving access control requests from users, calculating the final access control lists, and allowing users to modify access control lists based on personal needs. The prediction part uses the machine learning model obtained from the machine learning prediction module to predict the access control list based on the user's personal data. The machine learning part trains the machine learning model with historical data provided by historical record database through executing the machine learning algorithm. The historical record database is responsible for recording all resources uploaded by users to the social network and the access control lists set for those resources.

The execution part consists of a receive module and an execute module. The receive module acquires the access control request of the user, including the relevant information of the social network resources uploaded, and provides this information to the prediction part. The execute module receives and displays the access control list provided by the prediction part to the user, and allows the user to modify the access control list according to personal needs.

The prediction part is composed of user record acquisition module, keyword generation module, relationship acquisition module and machine learning prediction module. The user record acquisition module extracts the user record from the access control request, including the resources uploaded to the social network. The keyword generation module generates keywords according to social network resources. The relationship acquisition module obtains the relationships between the user and all the friends from the social network relationship graph. The machine learning prediction module runs the machine learning model obtained by the machine learning part, and inputs resource keywords and relationships between the user and the friends so as to obtain the prediction result.

The machine learning part is composed of a historical record acquisition module and a machine learning algorithm module. The historical record acquisition module requests the uploaded resources and the corresponding access control policies in the historical record database. The machine learning algorithm module uses the relevant history data obtained by the historical record acquisition module as input, and the machine learning algorithm module is trained to obtain the machine learning model.

The historical record database holds the resources uploaded by all users in the social network system and the access control policy set for those resources.

2) ACCESS CONTROL PREDICTION METHOD

Figure 3 summarizes the training and verification process of the prediction model. After data preprocessing, historical

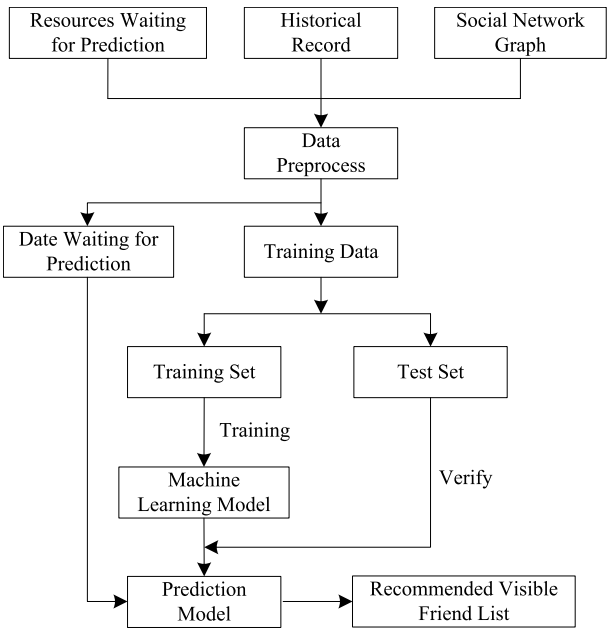


FIGURE 3. Training and verification of prediction model.

records and social network graph together constitutes the training data. In order to avoid the problem of over-fitting in the process of machine learning, the training data is divided into two parts: training set and test set. The machine learning algorithm is used to train the classification model on the training set, and the machine learning model is tested and optimized on the test set to obtain the prediction model. The resources to be uploaded to the social network are preprocessed to generate the data to be predicted (Data Waiting for Prediction). The prediction model takes the data to be predicted as the input, and obtains the recommended visible friend list of the resources.

B. PARAMETER OPTIMIZATION OF SVM PREDICTION MODEL BASED ON GRID SEARCH

Support vector machine algorithm (SVM) was used to train the machine learning model, and RBF kernel function was selected to process nonlinear fractional data. As described in section 3, the SVM algorithm with RBF kernel function uses two parameters C and γ. Constant C is used to balance training error and algorithm complexity. The parameter γ is used by RBF kernel function in machine learning. In order to find the classification model that can meets the requirements, the most appropriate C and γ [30] should be found. The grid search method is used to optimize the values of C and γ to obtain the highest accuracy. In order to avoid the problem of over-fitting in the process of machine learning, the accuracy of the model is evaluated by means of 10-fold cross validation for each group of values of parameter C and γ. The pre-processed training sample set is divided into ten subsets, with each subset being further divided into a verification set and nine training sets, to obtain ten models. The average classification accuracy of the ten models in the verification set is taken as the accuracy of cross validation. The C and γ with the highest cross-validation accuracy were selected as the final parameters.

Compared with genetic algorithm [31], random search algorithm [32] and other parameter optimization methods, grid search is more simple and practical, which can well meet the task requirements of smart access control in online social networks. In this paper, the grid search of parameter C and γ is carried out in a hierarchical way. Firstly, for the two-dimensional search space constituted by C and γ, a sparse grid is constructed with a large search step size (for example, the value of C is 2^{-5}, 2^{-4}, 2^{-3}, …, 2^{14}, 2^{15} while the value of γ is 2^{-10}, 2^{-9}, 2^{-8},…,2^{8}, 2^{9}, respectively), and the region with high cross-validation accuracy is $\{2^{10} \leq C \leq 2^{12}, 2^{-1} \leq \gamma \leq 2^{1}\}$. The optimization of grid parameters on the first layer is shown in figure 4. Then, the small step length was used to conduct parameter search in the region with high cross-validation accuracy (for example, the value of C is $2^{9.5}$,$2^{9.75}$, 2^{10}, …,$2^{12.25}$, $2^{12.5}$ while the value of γ is $2^{-1.5}$, $2^{-1.25}$, $2^{-1.0}$,…,$2^{1.25}$, $2^{1.5}$, respectively). The final value of C and γ is 2^{11} and 2^{0}, and the corresponding cross-validation accuracy is 0.9378. The two-layer grid parameter optimization is shown in figure 5.

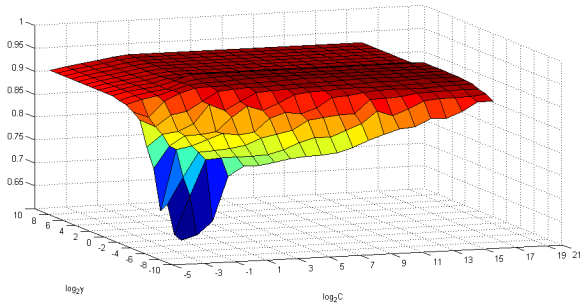


FIGURE 4. The first layer of grid parameter optimization.

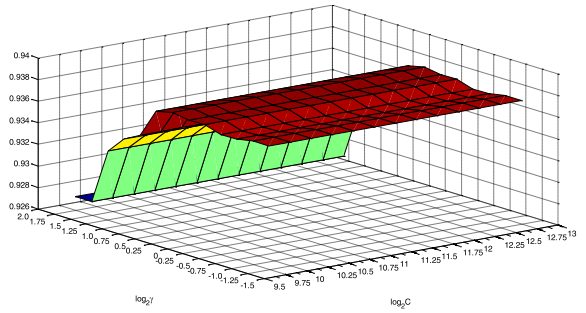


FIGURE 5. The second layer of grid parameter optimization.

V. RESULTS AND DISCUSSIONS

This section uses the actual data in the SVM prediction model with parameter optimization algorithm proposed in section 4 to verify the smart access control method. The experiment compared the accuracy of SVM algorithm with Naive Bayes and Random Forest algorithm. Then the comparison with other access control methods is presented in this section.

A. PREPARATION FOR THE EXPERIMENT

The data sets used in the experiment are introduced, as well as other models compared with the SVM model proposed in this paper. Then, the experimental operation platform and hardware and software environment configuration is presented.

1) DATA SET

The information sharing system developed by the author's research group has functions such as instant messaging and information publishing in social networks. The system will be open to use in the institute, registered users can add friends, upload resources and set access control policies. After running for several months, the data of 60 users in the system were selected as the research object. The selected research objects had an average of 200 friends on the system. Then, the decision data of 10 uploaded resources of each research object were extracted, and the decision data amount of the research object was equal to the number of his friends, with an average of 200. A total of 120,000 basic data were generated by 60 research objects, which constituted the data set of the experiment in this paper.

Each basic data is preprocessed to obtain the eigenvalue of a four-dimensional vector and a Boolean type target value, which correspond to one piece of training data. After preprocessing, the 120,000 pieces of training data constitute the training sample set. The purpose of the experiment is to give the detection rate and total detection accuracy of the algorithm for various access control decisions in the data set.

2) MODELS COMPARED WITH SVM

In this paper, experimental comparison is made between SVM model and the following two models.

a: NAIVE BAYES

Naive Bayes algorithm classification model is a classification method based on Bayes theorem and independent hypothesis of feature conditions. Because of its good performance and simple implementation, Naive Bayes classification algorithm has attracted extensive attention. At the same time, the algorithm has been widely applied in many fields due to its high computational accuracy and efficiency [33]–[35]. Suppose there is a feature vector $X = \{x_l\}_{l=1}^{m}$, a set of categories $C = \{c_k\}_{k=1}^{n}$, where the feature vector X uniquely belongs to a certain category c_k. Use $P_k = \{p_h\}_{h=1}^{n}$ to represent the probability that the vector set $X = \{x_l\}_{l=1}^{m}$ belongs to category C_k, then the category corresponding to max $\{p_h\}_{h=1}^{n}$ is the category to which X belongs. As most of data in the data set are multivariate discrete values, the MultinomialNB is chose here and parameters are set to be the default values.

b: RANDOM FOREST

Random Forest is an algorithm that uses multiple decision trees to train and predict samples, which was proposed by Breiman in 2001 [36]. The Random Forest uses the self-service resampling technique to put back sampling from the training sample set. For each input sample, each decision tree gives a classification result, and the random forest integrates all classification voting results, and the one with the most voting times becomes the final category. Random Forest Classifier is adopted in this paper for training, and the parameters are all set to be the default values.

3) THE PLATFORM

The experimental environment is as follows. CPU: dual-core i7-3770, 3.4 GHz; Memory of DDR 8 GB; The hard disk is 500GB, 7200rpm; The operating system is Windows 7. The programming language is Python 3.5.2 (64-bit); The simulation software is Matlab 7.11.0 (R2010b). In the process of program design, SVM model, Naive Bayes model and Random Forest model are implemented by sklearn 0.19.1 package.

B. EXPERIMENTAL RESULT

The method proposed in section 4 is applied to train the data collected above. Among them, the parameters are determined by optimizing the parameters in section 4.2, and the final values of C and γ are 2^{11} and 2^{0} respectively. In order to verify the advantages of the model described in this paper in different types of machine learning algorithms, SVM algorithm was replaced with Naive Bayes and Random Forest algorithm. Figure 6 shows the changes in accuracy of SVM, Naive Bayes and Random Forest models with different cross-validation folds under the same parameters. As can be seen from the figure, SVM and random forest are close to each other in accuracy and both are better than Naive Bayes algorithm. When cross validation is adopted, the higher the fold number, the higher the accuracy is. However, after 10 folds, the accuracy rate remained the same or improved slowly. Considering the accuracy and time consumption, the cross validation with 10 folds is the best.

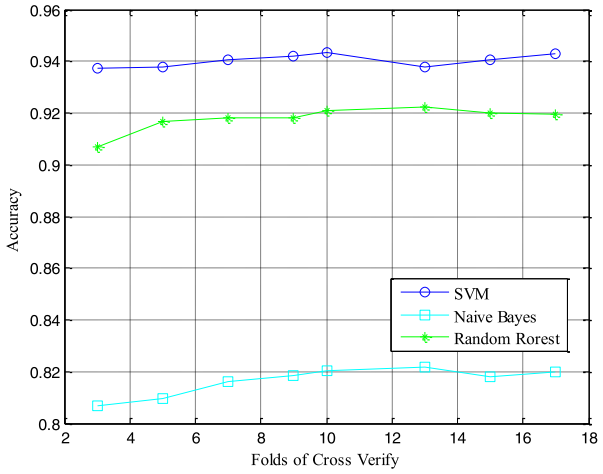


FIGURE 6. Comparison of model accuracy with different cross-validation fold.

VI. COMPARISON

This section discusses several related works of relationship based access control schemes and compares the scheme proposed in this paper with [14], [19], [37] and [38] (see Table 1).

The first column of Table 1 represents eight characteristics discussed in this section. The next four columns represent the characteristics of the access control schemes discussed below. Characteristics of the scheme proposed in this paper are listed in the last column.

The scheme in [14] is a formal algebraic access control model for Facebook-style systems. But user attributes and relationships beyond friendship are not supported in this model. OSNs access control models presented in other methods have similar user graph as [19]. However, these models do not explicitly take into account user attributes.

Despite its flexibility, UURAC_{A} [37] is still far from perfect. It does not support specific user attribute. More concretely, its policy specification language can merely figure out common attribute requirements of one or several users on the relationship path, lacking specification ability of different attribute requirements of different users along the path. Additionally, it cannot describe some policies, such as ''the adult colleagues of my friend Tom can access the

TABLE 1. Comparison.

	Fong et al. [14]	UURAC [19]	$UURAC_A$ [37]	HAC[38]	This paper
Multiple Relationship Types		√	√	√	√
User Profile Attributes			√	√	√
Specific User Attribute				√	√
User-user Relationship	√	√	√	√	√
Directional Relationship		√	√	√	√
Relationship Depth	√	√	√	√	√
Policy Individualization	√	√	√	√	√
Policy Recommendation					√

resource'', which requires the attribute of my friend ''name is Tom'' and the attribute of the colleagues of my friend Tom ''age $>$ 18''. Besides, compared with $UURAC_A$, HAC [38] is simple and easy to understand. It is easier for users in the OSNs to set up access control policies with HAC.

Compared with other four access control models, the scheme presented in this paper can automatically generate access control policies according to the resource that will be uploaded to the OSN and relationships between friends and the OSN user.

VII. CONCLUSION

The rapid development and widespread popularity of social networks not only bring convenience to people, but also bring the possibility of privacy disclosure. However, the large number of friends and the complex friendship relationship bring great trouble for users to set appropriate access control policies, and further bring the risk of privacy disclosure. In order to solve the problem of smart access control in the social network, the relationship type, the description of the content information are integrated as a feature vector, and the support vector machine (SVM) algorithm is used to realize smart access control, and then the grid search method is used for SVM parameter optimization algorithm, put forward a kind of smart access control method for online social networks based on SVM algorithm, and finally experiments are arranged to verify the effectiveness of the proposed mechanism by recommend proper access control strategy to users, achieve the purpose of better protection of privacy.

Because of personality differences, different online social network users may set different access control policies on the same set of resources. In order to obtain more accurate recommendations, the future research will focus on using machine learning algorithms to classify social users, and then according to different categories of users using machine learning algorithm to recommond the access control policy.

ACKNOWLEDGMENT

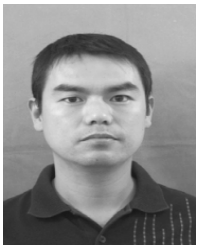
The authors would like to thank the editor and the anonymous referees for their constructive comments.

REFERENCES

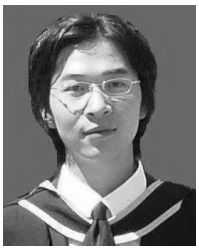
[1] C. Luo, J. Ji, Q. Wang, X. Chen, and P. Li, ''Channel state information prediction for 5g wireless communications: A deep learning approach,'' *IEEE Trans. Netw. Sci. Eng.*, to be published, doi: 10.1109/tnse.2018.2848960.
[2] D. Wu, H. Shi, H. Wang, R. Wang, and H. Fang, ''A feature–based learning system for Internet of Things applications,'' *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1928–1937, Apr. 2019.
[3] D. Wu, B. Liu, Q. Yang, and R. Wang, ''Social-aware cooperative caching mechanism in mobile social networks,'' *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102457.
[4] C. Akcora, B. Carminati, and E. Ferrari, ''Privacy in social networks: How risky is your social graph?'' in *Proc. IEEE 28th Int. Conf. Data Eng.*, Apr. 2012, pp. 9–19.
[5] P. Ilia, I. Polakis, and E. Athanasopoulos, ''Face/off: Preventing privacy leakage from photos in social networks,'' in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, Denver, CO, USA, 2015, pp. 781–792.
[6] J. Xiong, X. Chen, Q. Yang, L. Chen, and Z. Yao, ''A task-oriented user selection incentive mechanism in edge-aided mobile crowdsensing,'' *IEEE Trans. Netw. Sci. Eng.*, early access, 2019, doi: 10.1109/TNSE.2019.2940958.
[7] F. Li, H. Li, B. Niu, and J. Chen, ''Privacy computing: Concept, computing framework, and future development trends,'' *Engineering*, vol. 5, no. 6, pp. 1179–1192, Dec. 2019.
[8] R. Gross and A. Acquisti, ''Information revelation and privacy in online social networks,'' in *Proc. ACM Workshop Privacy Electron. Soc.*, New York, NY, USA, 2005, pp. 71–80.
[9] J. Xiong, R. Ma, L. Chen, Y. Tian, Q. Li, X. Liu, and Z. Yao, ''A personalized privacy protection framework for mobile crowdsensing in IIoT,'' *IEEE Trans. Ind. Informat.*, early access, 2019, doi: 10.1109/TII.2019.2948068.
[10] G. Liu, Q. Yang, H. Wang, and A. Liu, ''Three-valued subjective logic: A model for trust assessment in online social networks,'' *IEEE Trans. Dependable Secure Comput.*, to be published.
[11] J. Xiong, J. Ren, L. Chen, Z. Yao, M. Lin, D. Wu, and B. Niu, ''Enhancing privacy and availability for data clustering in intelligent electrical service of IoT,'' *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1530–1540, Apr. 2019, doi: 10.1109/jiot.2018.2842773.
[12] C. Gates, ''Access control requirements for Web 2.0 security and privacy,'' in *Proc. IEEE Symp. Secur. Privacy*, Jan. 2007, pp. 249–256.
[13] B. Carminati and E. Ferrari, ''Enforcing relationships privacy through collaborative access control in Web-based Social Networks,'' in *Proc. 5th Int. Conf. Collaborative Comput., Netw., Appl. Worksharing*, New York, NY, USA, Nov. 2009, pp. 1–9.
[14] P. W. L. Fong, M. Anwar, and Z. Zhao, ''A privacy preservation model for facebook-style social network systems,'' in *Proc. Eur. Symp. Res. Comput. Secur.*, 2009, pp. 303–320.
[15] P. W. L. Fong, ''Relationship-based access control: Protection model and policy language,'' in *Proc. ACM Conf. Data Appl. Secur. Privacy*, New York, NY, USA, 2011, pp. 191–202.
[16] P. W. L. Fong and I. Siahaan, ''Relationship-based access control policies and their policy languages,'' in *Proc. ACM Symp. Access Control Models Technol.*, New York, NY, USA, 2011, pp. 51–60.
[17] G. Bruns, P. W. L. Fong, and I. Siahaan, ''Relationship-based access control: Its expression and enforcement through hybrid logic,'' in *Proc. ACM Conf. Data Appl. Secur. Privacy*, New York, NY, USA, 2012, pp. 117–124.
[18] J. Park, R. Sandhu, and Y. Cheng, ''A user-activity-centric framework for access control in online social networks,'' *IEEE Internet Comput.*, vol. 15, no. 5, pp. 62–65, Sep. 2011.

[19] Y. Cheng, J. Park, and R. Sandhu, "A user-to-user relationship-based access control model for online social networks," in *Proc. ACM Conf. Data Appl. Secur. Privacy*. New York, NY, USA, 2012, pp. 8–24.
[20] J. Pang and Y. Zhang, "Cryptographic protocols for enforcing relationship-based access control policies," in *Proc. IEEE Comput. Softw. Appl. Conf.*, New York, NY, USA, 2015, pp. 484–493.
[21] B. Wellman and S. D. Berkowitz, "Social structers: A network approach," *Amer. Political Sci. Assoc.*, vol. 35, no. 4, p. 746, 1990.
[22] L. Q. Tian and C. Lin, "A kind of game-theoretic control mechanism of user behavior trust based on prediction in trustworthy network," *Chin. J. Comput.*, vol. 30, no. 11, pp. 1930–1938, 2007.
[23] J. Yu, Y. Wang, J. Li, H. Shen, and X. Cheng, "Analysis of competitive information dissemination in social network based on evolutionary game model," in *Proc. 2nd Int. Conf. Cloud Green Comput.*, New York, NY, USA, Nov. 2012, pp. 748–753.
[24] S. B. Zhang, W. D. Cai, and Y. J. Li, "A game-theory based access control method suitable for social network," *J. Northwesern Polytech. Univ.*, vol. 29, no. 4, pp. 652–657, 2011.
[25] P. Zhu, G. Wei, and A. V. Vasilakos, *Knowledge Sharing in Social Network Using Game Theory*. Berlin, Germany: Springer, 2012.
[26] Y. X. Zhang, J. S. He, and B. Zhao, "A privacy protection model base on game theory," (in Chinese), *Chin. J. Comput.*, vol. 39, no. 3, pp. 615–627 2016.
[27] B. E. Boser, I. M. Guyon, and V. N. Vapnik, "A training algorithm for optimal margin classifiers," in *Proc. Workshop Comput. Learn. Theory*, 1992, pp. 144–152.
[28] C. Cortes and V. Vapnik, "Support-vector networks," *Mach. Learn.*, vol. 20, no. 3, pp. 273–297, 1995.
[29] V. Vapnik, "The nature of statistical learning theory," *Technometrics*, vol. 38, no. 4, p. 409, 1995.
[30] Y. Zeng, J. Liu, K. Sun, and L.-W. Hu, "Machine learning based system performance prediction model for reactor control," *Ann. Nucl. Energy*, vol. 113, pp. 270–278, Mar. 2018.
[31] P.-W. Chen, J.-Y. Wang, and H.-M. Lee, "Model selection of SVMs using GA approach," in *Proc. IEEE Int. Joint Conf. Neural Netw.*, New York, NY, USA, Jul. 2004, pp. 2035–2040.
[32] K. Greff, R. K. Srivastava, J. Koutník, B. R. Steunebrink, and J. Schmidhuber, "LSTM: A search space odyssey," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 28, no. 10, pp. 2222–2232, Oct. 2017.
[33] Z. Chelly and Z. Elouedi, "Hybridization schemes of the fuzzy dendritic cell immune binary classifier based on different fuzzy clustering techniques," *New Gener. Comput.*, vol. 33, no. 1, pp. 1–31, Jan. 2015.
[34] A. Khedr, G. Gulak, and V. Vaikuntanathan, "SHIELD: Scalable homomorphic implementation of encrypted data–classifiers," *IEEE Trans. Comput.*, vol. 65, no. 9, pp. 2848–2858, Sep. 2016.
[35] J. S. Friedman, L. E. Calvet, P. Bessière, J. Droulez, and D. Querlioz, "Bayesian inference with Muller C-elements," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 6, pp. 895–903, Jun. 2016.
[36] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, vol. 2001.
[37] Y. Cheng, J. Park, and R. Sandhu, "Attribute-aware relationship-based access control for online social networks," in *Proc. IFIP Annu. Conf. Data Appl. Secur. Privacy*. Berlin, Germany: Springer, Jul. 2014, pp. 292–306.
[38] F. F. Shan, H. Li, and F. H. Li, "HAC: Hybrid access control for online social networks," in *Secur. Commun. Netw.*, vol. 2018, May 2018, Art. no. 7384194.

FANGFANG SHAN was born in 1984. She received the M.S. degree in computer architecture and the Ph.D. degree from Xidian University, in 2009 and 2018, respectively. She became a Teacher with the Zhongyuan University of Technology, in 2009. She is currently a Postdoctoral Student with the Collaborative Innovation Center of Internet Healthcare, Zhengzhou University. Her main research interests are access control model and information security and privacy.



JIZHAO LIU received the M.S. degree from the Henan University of Technology, in 2012, and the Ph.D. degree from Xidian University, in 2016. He is currently a Teacher with the Zhongyuan University of Technology. His research interests include the Internet of vehicles, information security, and wireless ad-hoc networks.



XUEYUAN WANG received the Ph.D. degree from Zhengzhou University, in 2015. He is currently a Postdoctoral Student with the Collaborative Innovation Center of Internet Healthcare, Zhengzhou University. His research interests include computer networks, social network information dissemination, and VR on logistic.

WEIGUANG LIU received the Ph.D. degree from Xidian University. He is currently a Professor with the Zhongyuan University of Technology. His research interests include graph and image processing and deep learning.

BING ZHOU was born in 1964. He is currently a Professor with Zhengzhou University. His main research interests include multimedia information processing and transmission, smart video surveillance, and image/video office.