Journal of Information Security and Applications 47 (2019) 217–222

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

A new user behavior evaluation method in online social network

Min Yang[a], Shibin Zhang[a,*], Hang Zhang[a], Jinyue Xia[b]

[a] Chengdu University of Information Technology, Chengdu, Sichuan 610225, China
[b] International Business Machines Corporation (IBM), New York, USA

ARTICLE INFO

Keywords:
Cloud model
Fuzzy comprehensive evaluation
User behavior evaluation
Behavior attribute cloud
Hierarchical cloud
Online social network

ABSTRACT

Due to the limitations of existing user evaluation in online social network (OSN), a new user behavior evaluation model is proposed. Considering the high degree of uncertainty, complexity, dynamics of user behavior in OSN, cloud model theory is innovatively introduced to evaluate the user behavior, on this basis, a credible evaluation scheme concerning user behavior combined with entropy weighting is proposed in this paper. The user's original behavior is classified as the evaluation factors according to the attribute, then the behavior attribute cloud is established via Reverse Cloud Generator algorithm; At the same time, the user is divided into different trust levels according to the actual situation, and hierarchical cloud is generated through Positive Cloud Generator algorithm. The membership matrix of the behavior attribute cloud to the hierarchical cloud is calculated by employing a mathematical formula, and the weight of each attribute is adaptively calculated by the entropy method, overcoming the limitations of subjective weight assignation. This model provides a new thinking of user behavior evaluation in OSN, meanwhile, also expands the application of cloud model theory and fuzzy comprehensive evaluation method. Finally, as an example of embodiment, a case study is presented for user behavior evaluation in Facebook, both the feasibility and effectiveness are verified.

1. Introduction

With people's increasing demand of the Internet, network is acting as a vital role in searching materials, accessing important information, and communicating with others. However, the convenience of accessing a variety of data and contacting each other leads to potential risk. Illegal individuals or groups can easily intercept information and initiate malicious attacks. By the end of 2017, the National Internet Emergency Center, acronym CNCERT released a safety report [1], which indicated that the number of hosts infected with viruses, and networks that have been tampered with, as well as newly added security vulnerabilities has increased. Many fields, such as industry, finance, government, etc. are confronted with security incidents. Hence, how to establish a 'trusted network' [2,3] has always been a tireless task for scholars. Lin et al. [4] pointed out that user behavior trust would become a hot spot for future research. So far, behavioral quantitative assessment has been a subject of concern in most of the research areas, a broad view of related evaluation model of user behavior is concluded as shown in Fig. 1.

Ji et al. [5] firstly employed the ordered hierarchical structure model to evaluate user behavior, and using the Analytic Hierarchy Process (AHP) to calculate the weights of all behavior evidences and attributes. In [6], a new access control model was proposed based on trust of users' behaviors for cloud computing, so as to solve the problem that the role of the user cannot be changed dynamically over time in access control model of cloud computing. Considering the dynamics and uncertainty of user behavior, FAHP was utilized to compute the direct trust value of users. In [7], a combination of fuzzy logic and AHP was used to formulate trust, in this way, the vague, uncertain and subjective nature of trust were fully reflected. Based on user's history behavior, Hidden Markov Model (HMM) and Bayesian network were adopted to predict user real-time behavior [8-12]. In order to implement the conversion between qualitative and quantitative of trust, reflecting the randomness, fuzziness and unpredictability of trust, the trust evaluation approach based on cloud model was proposed in [13,14]. On the basis of analyzing user real-time behavior, Tian and Lin [15] and Chen et al. [16] proposed a user behavior trust model of dynamic game theory, and the trustworthiness of end users was analyzed through multi-stage game. To make the results of trust evaluation are in line with the subjective experience of human beings and reflect the actual changes of user behavior, sliding window was introduced to guarantee the credibility and scalability of the behavior evaluation by setting the size of the window [17-19].

All the methods and theories mentioned in the above for evaluating user behavior have their own emphasis varying application

* Corresponding author.
E-mail address: cuitzsb@cuit.edu.cn (S. Zhang).

https://doi.org/10.1016/j.jisa.2019.04.008
2214-2126/

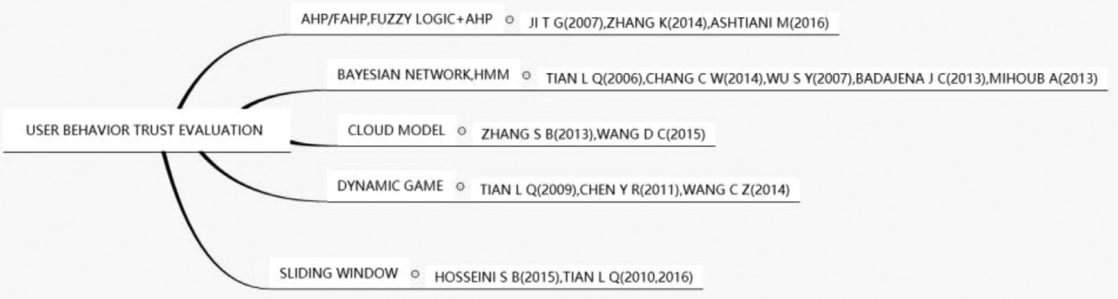

Fig. 1. A summary of existing behavior evaluation methods.

scenarios, but each of them has limitation to some extent. For example, the determination of weight tends to subjectivity when employing AHP. HMM, Bayesian network, including Dynamic Game is mainly used to predict the tendency of user behavior, widely applied to anomaly detection. Although the Cloud Model reflects the essence of trust, it doesn't involve the application of user behavior evaluation. In addition, those methods or theories rarely apply to OSN.

The rest of this paper is organized as follows. Section 2 summarizes the current status of social network trust assessment. In Section 3, after explaining some definitions, we propose the architecture of our approach. Section 4 presents the system for user behavior evaluation in detail. The experimental results are reported in Section 5. In Section 6, we summarize our work and give some ideas about the future work.

2. Related work

Online social network (OSN) has become a popular platform for disseminating information and connecting people. Individuals can communicate and keep in touch with their families, friends and even strangers. Governments, commercial organizations can open up new possibilities for business, politics, as well as deliver their services to citizens and consumers [20]. However, because of the complexity of OSN environment and easy access to all the data lead to potential risk, such as information tampering, various attacks, and etc. Therefore, it is important and indispensable to assess user trust in OSN. A lot of work has been done to assess user trust in social networks. Unlike other areas, users trust in OSN consists of direct trust and recommended trust. According to the data model, it can be divided into 3 categories, that is: (i) Graph-based: Approaches that leverage network structures to compute trust capture one aspect of trust computation, namely, how members are related to each other and how trust flows through their network [21]. (ii) Interaction-based: Interaction-based social trust models consider interactions in the community to compute trust, but ignore the social network structure. (iii) Hybrid: Hybrid trust models use both interactions and social network structure to compute social trust [22]. most of the study merely concentrates on building models based on user interaction and relationship, for example, FOFA network [23], STrust model [24], opportunistic network [25]. However, users' personal or static behavior, such as, comment, reply, like in OSN, etc. hasn't been carefully analyzed. Thus, an efficient solution specially for modeling user behavior is required. Therefore, this paper proposes cloud model aggregated fuzzy comprehensive evaluation to assess user behavior in OSN. The contribution of the work presented in the paper are:

- Formation of behavior attribute clouds and hierarchical clouds. On the one hand, user behavior is achieved from qualitative to quantitative conversion. On the other hand, fuzzy relation matrix is constructed.
- Implementation of adaptive weight assign for each behavior attribute.
- Reduction the computational complexity in the process of evaluating.
- Application the proposed model into Facebook to validate the feasibility and effectiveness. To best of our knowledge, this is the first try in integrating cloud model and fuzzy comprehension evaluation into online social network.

3. Model overview

In this section, we firstly introduce some definitions and related concepts to our paper, and then the architecture of proposed model is present.

3.1. Preliminary

3.1.1. Overall activities

Overall activities can be described though a vector $U=\{u_1,u_2,\ldots,u_m\}$, where u_i represents the ith one-time activity during the observed period of time. Thus, U is composed of all one-time activities that a user completes when logging in a certain website or system. For example, a student logs in his school official website, then clicks library resource, searches a paper, and downloads, finally logs out, we can extract his overall activities through the whole process, each activity is called one-time activity. In this paper, we regard U as the evaluated objects, called factor set, and u_i is one factor.

3.1.2. Evaluation set

The evaluation set is a set of various evaluation results that may be judged by the evaluation subject on the evaluated object. It is represented by the vector $C=\{c_1,c_2,\ldots, c_n\}$, which is actually a division of the trust levels for the evaluated object, where c_j represents the jth evaluation result and n is a total number of rating levels. The specific level is described in an appropriate description, such as when evaluating student learning attitudes $C=\{\text{good, general, bad}\}$, when assessing the degree of risk of the stock $C=\{\text{high, medium, low}\}$.

3.1.3. Fuzzy relation matrix

Fuzzy relationship matrix mainly demonstrates the relation between overall activities and corresponding rating levels, $R=\begin{bmatrix} r_{11} & \cdots & r_{1m} \\ \vdots & \ddots & \vdots \\ r_{n1} & \cdots & r_{nm} \end{bmatrix}$, where the element r_{ij} in the matrix indicates the degree of membership of the ith evaluation factor to the jth level. The row elements $(r_{i1},r_{i2},\ldots, r_{im})$ are the degree of membership of the ith evaluation factor to each rating level. The column elements $(r_{1j},r_{2j},\ldots, r_{nj})$ are the evaluation factor to the degree of membership of jth

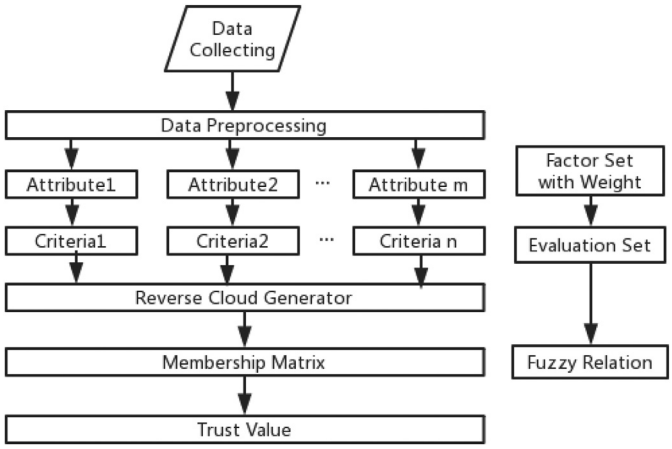

Fig. 2. The system architecture of user behavior evaluation.

standard. The method of calculating the degree of membership generally constructs a structural membership function, but in this paper, we will introduce a more objective method.

3.1.4. Behavior weight

When computing a user comprehensive trust value, each activity has a different contribution to the final result. The behavior weight is the measurement of a certain attribute's importance among overall activities. The higher the proportion is, the greater the influence of this attribute on the overall behavior is.

3.2. Architecture

Fig. 2 illustrates the process of our approach of the user behavior evaluation to the whole scale, which includes four steps. For each individual, firstly, we collect the overall activities and extract the behavior attribute to obtain factor set, then the weight for each attribute is assigned according to entropy weight method. Secondly, we divide an interval into n numbers of rating level, thus, n number of hierarchical clouds are established through positive cloud generator. Thirdly, we describe each attribute of the user behaviors using normal cloud (here is a consensus on the existing cloud model theory: the feature of user behavior in the internet obeys normal distribution), and the relationship among graded clouds and behavioral clouds is calculated by a certain formula. Finally, a comprehensive score is calculated by the multiplication of the fuzzy matrix and the weight vector.

4. User behavior evaluation

In this section, we will describe the specific steps of how to compute the user's trust value. We firstly extract a set of behavior attributes from his trace in the internet. Next, behavioral normal clouds are built to describe the uncertainty of the user behavior. And then hierarchical cloud based on evaluation set is constructed. Finally, the final assessment is carried out.

4.1. Basic concepts

4.1.1. Cloud and cloud drops

Suppose a quantitative domain U, C represents the qualitative concept, and f(x) represents the random mapping relationship from U to C, the value of f(x) exists in the interval [0,1], which has a certain stable tendency. The distribution x on U is called the cloud, and each x is a cloud drop [26].

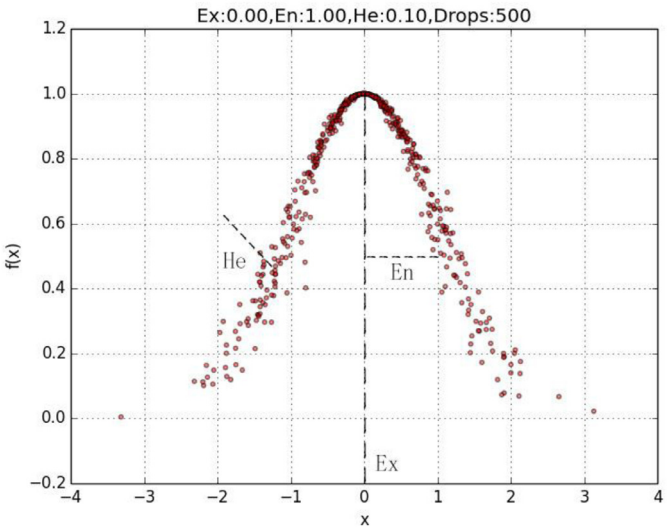

Fig. 3. The digital characteristics of clouds and cloud drops.

4.1.2. The digital characteristics of the cloud

In order to describe a qualitative concept through a quantitative way, three features of expectation (E_x), entropy (E_n), and hyperentropy (H_e) are used to characterize the characteristics of a qualitative concept [26].

E_x: It represents the expectation of the distribution of cloud drop x on the domain U, which is a typical sample point that best represents qualitative concepts.

E_n: It is a measure of the uncertainty of the qualitative concept, which demonstrates the range of cloud drops x accepted in the domain U. E_n reflects the randomness and ambiguity of the qualitative concept.

H_e: It is a measurement of the uncertainty of E_n, and an important index used to measure whether a sample can form a concept.

Therefore, qualitative concepts C, here refers to the user overall activities in OSN can be characterized according to (E_x,E_n,H_e). Fig. 3 shows the digital characteristics of clouds and cloud drops.

4.1.3. Positive cloud generator

It is a conversion process of transforming qualitative concepts to quantitative values. Cloud drops can be generated from the three digital features of the cloud [26].

4.1.4. Reverse cloud generator

Contrary to the positive cloud generator, it is the process of obtaining the digital characteristics of the cloud from inputting the number of drops [26].

4.2. Construct model

Due to the complexity and openness of the network, the user behavior in the network is complex and full of uncertainty. On the one hand, in order to make these characteristics of the user behavior in the network be better reflected, we build behavioral clouds through Reverse Cloud Generator algorithm. On the other hand, considering that the interval assigned for each rating level exist the problem of boundary ambiguity, we propose graded cloud to expand the range of levels. The specific stages are as follows.

4.2.1. Fuzzy relation matrix based on cloud model

Assume that the rating range is $[r_{min}, r_{max}]$, and a hierarchical cloud is established. The parameters,E_x, E_n and H_e are determined by the following formulas.

$$E_x = \frac{r_{min} + r_{max}}{2} \quad (1)$$

$$E_n = \frac{r_{max} - r_{min}}{6} \tag{2}$$

$$H_e = 0.02 \tag{3}$$

In which, the selection of H_e is in the light of Ref [13].

The factor set $U=\{u_1,u_2,\ldots, u_m\}$, u_i is called factor set and represents the ith activity, which can represent the user behavior as a series of attributes, and each attribute is a factor. $u_i=\{Ex_i,En_i,He_i\}$, the equation explains that a user's abstract behavior can be quantitatively represented by three digital features of cloud model. Suppose input n data, behavioral normal clouds are constructed using Reverse Cloud Generator algorithm [27], and selecting drops lying in the interval $x_i=[Ex_i-3En_i,Ex_i+3En_i]$ of the cloud to calculate the fuzzy relation matrix. R can be calculated from the formula (4).

$$r = \frac{1}{n}\sum_{i=1}^{m} \exp\left(-\frac{x_i - E_x{}^2}{2E_n{}^2}\right) \tag{4}$$

In which x_i represents the drop in the behavioral cloud, E_x and E_n stand for the expectation and entropy of different hierarchical clouds respectively.

A pseudocode description of Reverse Cloud Generation Algorithm without Certainty Degree (RCGAU) is provided as Algorithm 1.

Algorithm 1 RCGAU.

Input: x_i
Output: E_x, E_n, H_e
1: input the number of one behavior attribute
2: **for** $i=1$ to m
3: **Calculate** $E_x = \frac{1}{m}\sum_{i=1}^{m} x_i$
4: **Calculate** $E_n = \sqrt{\frac{\pi}{2}} \times \frac{1}{m}\sum_{i=1}^{m} |x_i - E_x|$
5: **Calculate** $S^2 = \frac{1}{N-1}\sum_{i=1}^{N} (x_i - E_x)^2$
6: **if** $S^2 - E_n{}^2 \geq 0$ **then goto** 8
7: **delete** $(\sum_{j=1}^{N \times 0.01} \mathrm{sort}(|x_i - E_x|))$, $N = N \times 0.99$ **then goto** 5
8: $H_e = \sqrt{S^2 - E_n{}^2}$.
9: end for

4.2.2. Calculation of user behavior weight

Considering that each activity has different effects on the final assessment result, so the weight of each activity should not be the same when describing the user behavior in the network. In order to ensure objectivity, entropy method is introduced emphasizing the diversity of each attributes impact on the final assessment.

$$p_{ij} = \frac{r_{ij}}{\sum_{i=1}^{n} r_{ij}} \tag{5}$$

$$E_i = -\sum_{j=1}^{n} p_{ij} \ln p_{ij} \times \frac{1}{\ln n} \tag{6}$$

$$E_i' = \frac{1}{E_i} \tag{7}$$

$$w_i = \frac{E_i'}{\sum_{i=1}^{m} E_i'} \tag{8}$$

In which, r_{ij} is one of the elements in the fuzzy relation matrix. The principle of entropy weight allocation is that if there is no difference in each behavior attribute at each rating level, it is considered that the activity does not provide useful information for the final evaluation result, thus the corresponding weight value is smaller. On the contrary, if a certain activity has greater difference in each rating level, the entropy value is smaller and the weight of corresponding attribute should be larger, which means that the behavior attribute provides a larger amount of information for the final evaluation result.

Table 1
Level boundaries of each behavior attribute.

Attribute	Level			
	1	2	3	4
Post	(0,5)	(5,10)	(10,15)	(15,20)
Comment	(60,80)	(40,60)	(20,40)	(0,20)
Like	(0,15)	(15,30)	(30,45)	(45,60)
A	1	3	6	9

4.2.3. Calculation the score of a user's overall behavior

The fuzzy relation matrix and weight vector have already been obtained from the formulas from (4) to (8). Therefore, the evaluation vector **V** is obtained using **W** multiplies **R**. The user's trust level is evaluated referring to the different intervals of rating levels we have determined beforehand.

In order to eliminate the interference caused by other factors in the network, the interference factor α is utilized to modify the original evaluation result. The larger the trust score, the closer **V′** is to 0, which indicates the greater the interference from outside, the less accurate the evaluation result. The corrected trusted value is as follows:

$$\mathbf{V}' = (1-\alpha) \times \mathbf{V} \tag{9}$$

A trust score for the user's overall activities can be obtained from the above evaluation method, which not only embodies the randomness and ambiguity of the user behavior in OSN, but also eliminates the impact of other factors in the network during the evaluation process, so the result obtained is more objective, and more in line with the actual situation.

5. Simulation experiments and analysis

5.1. Description of experimental data and related standards

In order to verify the rationality and feasibility of the proposed model, this section simulates the real data collected from Facebook, including post, comment, like [28]. More specifically, we explain these data as follows:

Post: users posted his mood, likes, dislikes on the platform.

Comments: users make comments on news, articles, blogs, and so on.

Like: Corresponding to the user's liking or disliking content on Facebook.

The level boundaries of each behavior attribute are shown in Table 1.

Due to the increasing relationship among levels, the values of each level are integrated by the formula (10):

$$A = v_1 + 3 \times v_2 + 6 \times v_3 + 9 \times v_4 \tag{10}$$

The trust status of a user is quantitatively assessed by the value of A. The higher the rating level is, the larger the value of A is, and the greater degree of the user trust is. When $A > 0.15$, one is in a high trustworthiness state, $A < 0.05$, in extreme untrustworthiness.

The range value of evaluation set is [0,0.2], we divide it into four trust levels, to be clearer, a table is drawn and shown as in Table 2.

For each level, it is inevitable to exist boundary blurring excluded ideal conditions. Whereas cloud model can be used to describe ambiguity, so we innovatively transform each level into hierarchical cloud through Positive Cloud Generator algorithm, the related formulas are about (1)(2)(3), and the result is shown below (Fig. 4).

Table 2
A detailed description of four levels.

Interval value	Level	Description
[0,0.05]	1	Extreme untrustworthiness
[0.05,0.10]	2	Low trustworthiness
[0.10,0.15]	3	General trustworthiness
[0.15,0.2]	4	High trustworthiness

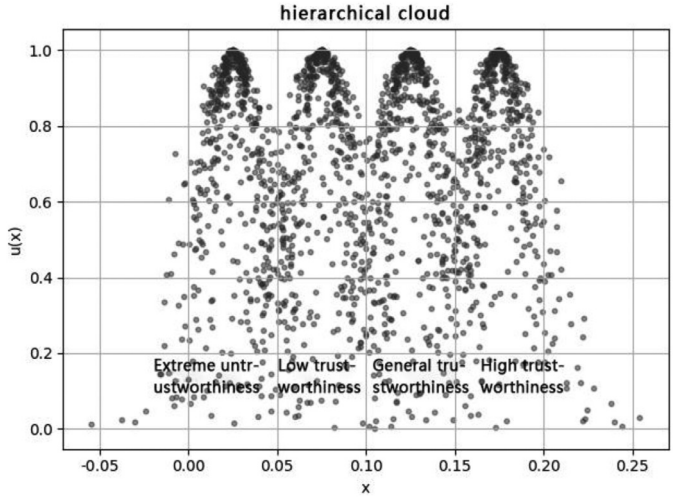

Fig. 4. Four kinds of hierarchical clouds.

5.2. The specific steps and results of the experiment

In the simulation experiment, this paper collects over one-year activities from over 100 users. For space reasons, we only list the following 10 data, and the specific information is seen in Table 3.

In order to better illustrate the effectiveness of the proposed model, we deliberately select one normal user and one seemingly suspicious user's data in the simulation process, then divide the one-year activity into 12 months as the input data of RCGAU. More precise data is shown as below.

User1: Post = [13, 8, 13, 9, 7, 2, 3, 5, 0, 1, 3,1], Comment = [31, 25, 40, 14, 28, 7, 14, 3,17, 0, 12,4], Like = [59, 20, 33, 33, 46, 31, 19, 7, 28, 45, 15, 48].

User7: Post = [0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0], Comment = [12, 11, 28, 31, 25, 14, 21, 32, 74, 94, 11, 79], Like = [43, 68, 72, 36, 147, 25, 87, 59, 52, 63, 37, 19].

5.2.1. Fuzzy relation matrix

According to the data in Table 3, the eigenvalues of the three behavior attributes of the user1 restored by RCGAU are (5.42, 4.79, 1.49), (16.25, 12.48, 3.77), (32, 15.04, 3.13) separately. In this way, the fuzzy relation matrix **R** is calculated from these digital features using the formula (4.4).

$$\mathbf{R} = \begin{bmatrix} 0.0610 & 0.0620 & 0.0436 & 0.0287 \\ 0.0122 & 0.0069 & 0.0006 & 0.0021 \\ 0.0017 & 0.0033 & 0.0047 & 0.0066 \end{bmatrix}$$

Table 3
The data information of users.

User	Post	Comment	Like
1	65	195	378
2	8	122	298
3	29	67	88
4	3	13	11
5	7	20	21
6	20	45	2
7	2	432	708
8	3	315	40
9	24	118	72
10	37	189	650

5.2.2. User behavior weight

According to the formula from (5) to (8), the attribute weight vector of the user1 is obtained, $\mathbf{W} = [0.08, 0.72, 0.20]$.

The evaluation result $\mathbf{V}_1 = \mathbf{W} \times \mathbf{R} = [0.0067, 0.0061, 0.0094, 0.0124]$. However, when calculating the degree of membership matrix, the selection of drops in behavioral clouds has a certain influence on the final evaluation result, so the interference factor is taken as 0.01 in this paper, after being revised according to the formula (9), $\mathbf{V}_1' = [0.0066, 0.0060, 0.0093, 0.0123]$, so the final evaluation value $A = 0.191$ by adopting the formula (10). Comparing the result with the interval of four rating levels, the User1 is in a high trustworthiness state. In fact, after tracking the user's Facebook account, we verify that the user is indeed an ordinary user by analyzing the posts and comments he has sent. Therefore, the evaluation result is in line with the actual situation. In the same way, the same calculation procedure is used to calculate the trust value of user7. The final trust value $A = 0.079$, so the user7 is in low trustworthiness. We track the user7's whereabouts in Facebook and find that he sent only 2 posts, a lot of comments is made in many places, moreover, most of the comments were related to sex and crime, so we regard him as a potentially dangerous user, the trust value obtained through the proposed model is low.

6. Conclusion and future work

Trust evaluation, especially in the aspect of user behavior is a major issue for a successful OSN. In this paper, we propose an approach to evaluate user behavior with a combination of Cloud Model and adaptive entropy weight method. Through the feature of Cloud Model, not only user behavior is quantitatively transformed, but also the uncertain and dynamic essence of user behavior in OSN are embodied. More importantly, due to that the function involved in the proposed model obeys normal distribution, with the help of its characteristics, the complicate multiplication is converted to the simple addition, which largely reduces the complexity in the process of behavioral assessment. Meanwhile, the weight entropy method is used to determine the weight of each behavior attribute adaptively, which avoids the error caused by subjective distribution weights. In the process of evaluation, the interference factor is used to eliminate the impact of other factors in the network, so it is more accordant with practical situation, and the result obtained is more objective. This paper provides a new idea for measuring users' direct trust in OSN. The next step is to explore that whether the proposed model can combine with the existing credible schemes, to measure the credibility of users in OSN from both static and dynamic aspects and make a contribution to creating a trusted environment.

Conflict of interest

The authors declared that they have no conflicts of interest to this work.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.jisa.2019.04.008.

References

[1] China internet cyber security report, 5. Beijing: People Post Press; 2018. p. 17–33.

[2] Li DH, Zhang GZ. Modelling the roles of cewebrity trust and platform trust in consumers' propensity of live-streaming: an extended TAM method. Comput Mater Continua 2018;55(1):137–50.
[3] Xie XL, Yuan TW, Zhou X. Research on trust model in container-based cloud service. Comput Mater Continua 2018;56(2):273–83.
[4] Lin C, Tian LQ, Wang YZ. Research on user behavior trust in trustworthy network. J Comput Res Dev 2008;45(12):2033–43.
[5] Ji TG, Tian LQ, Hu ZX, et al. AHP - based user behavior evaluation method in trustworthy network. Comput Eng Appl 2007;43(19):123–6.
[6] Zhang K, Pan XZ. Access control model based on trust of users' behavior in cloud computing. J Comput Appl 2014;34(4):1051–4.
[7] Ashtiani M, Abdollahi Azgomi M. Trust modeling based on a combination of fuzzy analytic hierarchy process and fuzzy VIKOR. Soft Comput 2016;20(1):399–421.
[8] Tian LQ, Lin C, Ji TG. Quantitative analysis of trust evidence in internet. International conference on communication technology. IEEE; 2007.
[9] Chang CW, Xu JK. Research on behavior assessment and access control for terminal. J Chin Comput Syst 2014.
[10] Xie Y, Yu SZ. A large-scale hidden semi-markov model for anomaly detection on user browsing behaviors. IEEE/ACM Trans Netw 2009;17(1):54–65.
[11] Badajena JC, Rout C, Badajena JC, et al. Incorporating hidden Markov model into anomaly detection technique for network intrusion detection. Int J Comput Appl 2013;53(11):42–7.
[12] Mihoub A, Bailly G, Wolf C. Social behavior modeling based on incremental discrete hidden markov models. International workshop on human behavior understanding; 2013.
[13] Zhang SB, Xu CX. Study on the trust evaluation approach based on cloud model. J Univ Electron Sci Technol China 2013;42(1) 92-97+104.
[14] Wang DC, Zhang SB, Xu Y. Study on the dynamic computer forensic evaluation model based on business user's behavior. J Univ Electron Sci Technol China 2015;44(6).
[15] Tian LQ, Lin C. A kind of game-theoretic control mechanism of user behavior trust based on prediction in trustworthy network. Chin J Comput 2007;30(11):1930–8.
[16] Chen YR, Tian LQ, Yang Y. Model and analysis of user behavior based on dynamic game theory in cloud computing. Acta Electron Sinica 2011;39(8):1818–23.
[17] Tian L Q, Lin C. Evaluation mechanism for user behavior trust based on DSW. Tsing Hua Univ 2010;50(5).
[18] Hosseini SB, Klement U, Yao Y, et al. Formation mechanisms of white layers induced by hard turning of AISI 52100 steel. Acta Mater 2015;89:258–67.
[19] Tian LQ, Li JJ, Wu ZN. Trust evaluation of web user behavior with weight optimal balance. J Beijing Univ Posts Telecommun 2016;39(6).
[20] Meng X, Ma J, Wang Y, et al. MCTE: a trust evaluation model for multiple context in social networks. J Xian Jiaotong Univ 2015;49(4):73–7 and 103.
[21] Ying L, Li JB, Chen JW. Seed selection for data offloading based on social and interest graphs. Comput Mater Continua 2018;57(3):571–87.
[22] Sherchan W, Nepal S, Paris C. A survey of trust in social networks. ACM Comput Surv 2013;45(4):1–33.
[23] Golbeck J, Parsia B, Hendler J. Trust networks on the semantic Web. In: Proceedings of the 7th international workshop on cooperative intelligents; 2003. p. 238–49.
[24] Nepal S, Sherchan W, Paris C. STrust: a trust model for social networks. IEEE international conference on trust. IEEE; 2012.
[25] Trifunovic S, Legendre F, Anastasiades C. Social trust in opportunistic networks. Infocom IEEE conference on computer communications workshops. IEEE; 2010.
[26] Li DY, Du Y. Artificial intelligence with uncertainty. In: International conference on computer and information technology. IEEE; 2004. p. 2. -2.
[27] Chen H, Bing LI, Liu CY. An algorithm of backward cloud without certainty degree. J Chin Comput Syst 2015.
[28] Wang G, Konolige T, Wilson C, et al. You are how you click: clickstream analysis for Sybil detection. Usenix Conf Secur 2013:241–56.