Journal of Computational Science 26 (2018) 468–477

Contents lists available at ScienceDirect

Journal of Computational Science

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

A novel crowd evaluation method for security and trustworthiness of online social networks platforms based on signaling theory

Zhiyong Zhang*, Jing Wen, Xiaoxue Wang, Changwei Zhao

Information Engineering College, Henan University of Science and Technology, Luoyang 471023, PR China

ARTICLE INFO

Article history:
Received 27 March 2017
Received in revised form 7 May 2017
Accepted 18 May 2017
Available online 24 May 2017

Keywords:
Online social network
Security
Trustworthiness
Signaling theory
Crowd computing

ABSTRACT

Along with the convenience provided by the open online social networks (OSNs) for the users, there are also many burning problems like insecure platform, untrustworthy information, malicious propagation, even illegal cheating. Especially, security and trustworthiness of social platforms, as the foundation of social interactions, plays an important role in active users' sharing and communication. The available research efforts of the aspects mainly focus on exploring security mechanisms and methods, as well as establishing trust relationship among social users. However, the evaluation and measurement for social platforms have not yet been well conducted. This paper proposed a novel method for crowd evaluating the security and trustworthiness of OSNs platforms based on signaling theory, which have been generally employed in the fields of economics and information management. Firstly, we classified the security and trust-critical signals of generic OSNs platform itself, and formalized static attributes and dynamic behaviors features by using the OWL and the temporal logic. Then, a comprehensive computational model for security and trustworthiness measurement was proposed inspired by crowd computing, after signals' weights were yielded based on Fuzzy Analytic Hierarchy Process Comprehensive Evaluation. Finally, the evaluation experiments were carried out by using crowd evaluation architecture on a real-world multimedia social network platform called CyVOD MSN. The experimental results denote that the proposed approach can effectively achieve the assessments of every security and trust-critical signals of the social platforms, and further realize the functional evolution of CyVOD MSN through improving insecure and untrustworthy vulnerabilities found by the crowd evaluation.

1. Introduction

The social media platform is a well-known application for numerous users to interact, share data, and keep in contact. The social network environment is open and self-governed, which is convenient for users to join in and manage. However, uncertainty and fraudulence of trust exist particularly because of commercial interest, in which the third-party platform may provide false, incomplete, and suspect information. When the security-critical topic of (mobile) social media has been attempted to resolve, trust between users and content (service) providers or even third-party supervisors has been another controversial issue for the social media ecosystem to exist steadily and to ensure successful application. Given different trust relationships among various users, the extent of trust relationship among same users in different fields varies [1], resulting in the uncertainty of trust relationship being the most significant challenge for trust prediction.

Traditional trust evaluation focuses on the trust relationship among users [2,3], whereas the trust relationship between users and the platform is the foundation to build the relationship among users. At present, the evaluation system for the security and trustworthiness of the platform is incomplete [4]. Users grasp different types of information while applying the social media platform. When users cannot determine whether the platform is trustworthy, obtaining more information to assess the platform and generate a standard trust evaluation system can effectively decrease interaction risks.

The main contributions of the paper are highlighted on the following three aspects: the first is to classify the security-critical and trust-critical signals of general OSNs platform itself, and formalize static attributes and dynamic behaviors features to avoid semantic ambiguity; the second is to propose a comprehensive computational model for security and trustworthiness evaluation inspired by crowd computing; last but not the least, we made evaluation experiments by using a proposed crowd evaluation architecture

* Corresponding author.
E-mail address: xidianzzy@126.com (Z. Zhang).

https://doi.org/10.1016/j.jocs.2017.05.018
1877-7503/

Table 1
Definition of action symbols.

Symbols	Description
$k_1, k_2, k_3 \ldots k_n$;	Action symbols
$\neg, \wedge, \vee, ^*$;	Conjunction
$\Diamond$sometimes, $\Box$always, $\bigcirc$next, $\triangleright$until, $\blacklozenge$once;	Main tense operators
AD	User sends access request
AID	User ID
D	content with copyright protection
ND	Non-copyrighted content
PL	Platform
CS(Cradible Strategy)	Platform customized decision strategy
CS > 0	Satisfy decision strategy
CS ≤ 0	Not to satisfy decision strategy
√DD	Trustworthy login
√NDD	Common login
√Vit	Access the page
√NVit	Non-access the page
SS	Submitted successfully
NSS	Not submitted

on a real-world multimedia social network platform to verify our holistic approach.

The rest of the paper is organized as follows: the related research works are in detail presented in Section 2; the following section is the definition and description of security and trust-critical signals; in Section 4, there is a proposed comprehensive evaluation method for security and trustworthiness measurement; our experiment is clearly represented in Section 5. The final section is conclusion.

2. Related works

2.1. Trust prediction for the social network

In the information technology (IT) field, Marsh distinguished the extent of trust and the concept of contents in 1994 with respect to the subjective features of trust relationship and generated a mathematical model for trust measurement, which laid the foundation for applying trust in the IT field [5].

In 2012, Bao et al. [6] applied the concept of group when examining trust among users, considered each user as one node, investigated the reasonability of reliability for each node in groups, and transformed trust as a one-to-one relation to calculate the direct reliability among groups. In 2013, Huang et al. [7] proposed a model of "joint social network exploration" that collected heterogeneous social networks from the target trust domain and supplementary information field to predict trust. Building the matrix of the trust diagram among users and between users and contents has solved sparse data without interaction history among users. In 2014, Fernandez-Gago et al. [8] proposed to use context similarity and to build a trust model. They simulated the ideal conditions of users. That is, users tend to trust others who have common hobbies or like to share their opinions. Therefore, they inferred a similar network to define a trust model to build a trust path among entities. Zhang et al. proposed a multi-layer architecture for crowd evaluation and measurement based on signaling theory in economics and information management [9].

Meo [10] and Agreste et al. [11] stated that understanding the dynamic features behind the formation of social groups and the evolution of topological structure was vital. However, during user gathering and community forming, trust relationship among users is another important factor. They proposed a quantifiable and measurable method of group compactness and considered the similarity and reliability among users. Through the introduction of "centrality metrics," empirical research results based on actual social networks, such as Epinion, Ciao, and Prosper ("small-scale loan" stations with implicit trust), have been obtained to demonstrate the superiority of this new method. Evolutionary algorithms have been adopted to deal with community detection problem by Kaur [12]. Xiao et al. proposed a new centralized location-sharing system, which does not depend on the third-part server, can achieve the protection goal on the users' privacy. Finally it can improve efficiency and enhances security strength in the communication [13]. Besides, Medhane et al. represented a novel algorithm for position monitoring applications [14].

In user trust problems with respect to social media [15], an intra-regional and inter-domain trust evaluation model has been proposed, and a simulation experiment conducted via the UCINET social network has shown the increase and/or decrease in user trust in sharing and spreading multimedia contents. First, combined with the essential features and topological structure of the multimedia social network and based on the roughness method of the binary relation in a rough set, the potential path definition, inference, and findings of digital rights management among cross-community users in MNS have been achieved. Second, based on the discovered potential paths and combined with the trust evaluation method, potential path trust has been measured and potential trustworthy path has been discovered within the user-customized scope of trust threshold values. Finally, we designed and generated the discovery algorithm for the potential path and potential trustworthy path, selected the security strategies under the scenario of sharing digital contents, applied the actual data set of the social network simulation software UCINET and YouTube to build a large-scale virtual social network from common sense, derived a complete and potential trustworthy path, and verified the accuracy and efficiency of the algorithm [16].

For a large-scale mobile social network, users may belong to multiple communities or clusters, and such overlapped users may play a special role in a complex network. At present, the key problem is how to evaluate or explain user security and trustworthiness. Under such a scenario, "trust inference" plays a key role in social contact of trust built among mobile users. In order to infer fuzzy trust relationship in a large-scale social network in overlapped community, an effective trust inference system called kappa-fuzzy trust has been proposed in the literature [17]. Subsequently, the scholar proposed an algorithm that was used to detect the community structure of a complex network under the kappa-fuzzy extent and built a fuzzy and implicit social diagram. Finally, the major performances of kappa-fuzzy trust have been evaluated through simulation experiments.

2.2. Signaling theory

"Signaling theory," which mainly focuses on asymmetric market interaction information between buyer and seller in e-commerce, was proposed by economist Michael Spence in 1974 [18,19]. William Boulding stated that signals were used to solve problems about classification for consumers encountering potentially bad sellers. Asymmetric information in communication featured more information from the seller about products or more information from the management about company financial affairs [20]. Such asymmetry and effectiveness of signals would further expand the communication experience of the seller [21]. In their paper, Boulding and Kirmani described that, when the third-party agency suffered from loss after sending false signals, such signals would be considered trustworthy [20]. Thus, if an individual does not care about trust cultivation in the short term in the social network, but spreads false information for the purpose of gaining a certain amount of interest, then resulting in the corresponding punishment of interest. Mavlanova and Benbunan-Fich proposed a 3D framework to classify signals in an online e-commerce application, which would help online users to select trustworthiness-critical and security-critical signals and eliminate false signals [22].

In the social network, users can only assume security and trustworthiness via the signals shown in the social media platform. Thus, signals that can effectively increase the trust and participation of social media users and how trustworthiness-critical and security-critical signals can influence user trust should be distinguished. Therefore, how to correctly introduce signaling theory into the online social network can solve problems about trust. Likewise, the quality of the site has become a signal that affects the purchase intention and as a product quality. This suggests that the classification of signals can be used as a set of factors to evaluate an online social networking platform.

3. Definition and description of security and trust-critical signals

3.1. Definition of signals classification

The signal is a concept in e-commerce, and "signals" of the social network platform are also shown to users in various forms. We classified and defined signals in the social network platform to collect, describe, and evaluate these signals. The signal is defined as a triple to standardize in definite form: $C = <ID, Atb, ActSet(\Phi)>$, where *ID* is the name number, *Atb* is the static attribute, $ActSet(\Phi)$ is the dynamic behavior set that is constituted by action formulas. Meanwhile, the action formula is constituted by action and relation symbols.

3.1.1. Definition 1 (Signal)

Signals of the social network platform are objective in the social media platform and objectively show the platform attribute set to users or perceived by users.

In the social network, signals influence the trust and decision-making of users in different roles from various aspects. The platform signal W is a four-tuple including signal usability U, transparency T, security and privacy SP, and quality assurance QA.

3.2. The static attributes of signal

Descriptive languages of ontology are introduced in this section to strengthen rigorous semantics for formal description to understand the significance of signals in the social media platform more deeply, achieve a query and inference service, and avoid ambiguity in understanding signals. In the artificial intelligence field, ontology is a definite standard for shared conceptual information. Nicola Guarino [23] defined conceptual information *C* as $C = <D, W, R>$, where *D* is a domain, *W* is a set of related transaction states in the domain, *R* is a set of conceptual relationships in the domain space $<D, W>$. Thus, the terms in one domain, definitions of terms, and semantic relation network among various terms are required for ontology modeling. Ontology Web Language (OWL) is a modeling tool for the logic description of the information system at the semantic level. The OWL can definitely express the relationship between words and complicated vocabularies. In building an ontology, the concepts of signals in the social media platform and the relationship among various concepts should be accurately and completely described.

3.2.1. Definition 2 (static attribute of signal)

The static attribute of a signal refers to the identification number, relation of subordination, and name of the role. The OWL is applied to define different types of signals, as follows:

● The definition of the "Usability" classes and subclasses, roles, and categories:

<OWL: Classrdf:ID = "Usability"/>
<rdf: subclassof: resource = "<U_1, U_2, U_3, . . . U_n>"/>
<usability rdfs:subClassOf role>
</rdfs:subClassOf>
</OWL: Class>

● The definition of the "Transparency" classes and subclasses, roles, and categories:

<OWL: Classrdf:ID = "Transparency"/>
<rdf: subclassof:resource = "<T_1, T_2, T_3, . . . T_n>"/>
<transparency rdfs:subClassOf role>
</rdfs:subClassOf>
</OWL:Class>

● The definition of the "Security, Privacy" classes and subclasses, roles, and categories:

<OWL: Classrdf:ID = "Security, Privacy"/>
<rdf: subclassof:resource = "<SP_1, SP_2, SP_3, . . . SP_n>"/>
<security and privacy rdfs:subClassOf role.>
</rdfs:subClassOf>
</OWL:Class>

● The definition of the "Quality-Assured" classes and subclasses, roles, and categories:

<OWL: Classrdf:ID = "Quality-Assured"/>
<rdf: subclassof:resource = "<QA_1, QA_2, QA_3, . . . QA_n>"/>
<quality-assured rdfs:subClassOf role.>
</rdfs:subClassOf>
</OWL:Class>

Various types of roles are designed with subcategories. For example, available signal includes navigation and FAQ; transparency signal includes historical information and various items; security and privacy signal includes data encryption and permission setting; and quality assurance signal includes digital fingerprinting and copyright protection. "Navigation" is taken as an example to define OWL, as follows:

<OWL: navigation rdfs:subClassOf usability>

The roles of signals are classified from the aspect of user perception, including direct show signal "s," operation hint signal "o," and feedback signal "f," that is,

R = <s, o, f>.

For example, "submit hint" belongs to available signal and operation hint signal.

3.3. The dynamic behaviors of signal

User behavior varies and results in significant randomness of display. An abstract model is built for analysis to describe the dynamic behavior of platform signals. In this study, temporal logic language is used to describe the dynamic behavior of platform signals in the social media platform formally, and a formal method is proposed by Lamport in 1993 [24,25]. The TLA formula includes typical connectors ($\wedge$ and $\vee$), quantifiers ($\exists$ and $\forall$), and unary operators ($\Diamond$, $\Box$, and $\triangleright$), and its sematic explanation is behavior, state, and action.

3.3.1. Definition 3 (dynamic behavior of signal)

The dynamic behavior of a signal refers to the platform feedback or experience after certain operations of the user, such as "use", "click" and "inquiry", that could be defined by the following symbols and semantics (Tables 1 and 2).

The following examples of the description of platform signals, including static and dynamic: are represented in detail:

● Trustworthy login determination

When a user sends an access request, the platform will perform a CS decision. When the user ID is satisfied with the CS, the user achieves a trustworthy login; otherwise, the user achieves a common login.

C1 = <ID, Atb_1, $ActSet(\Phi)_1$>
Atb $_1$:
Defined0bject rdf: ID = " SP_7"//Defining the signal's name " SP_7"

Table 2
Semantics of behaviors.

Symbols	Description
?k	performs action k immediately
¬k	does not perform action k right now
k∧l	performs actions "k" and "1" simultaneously
k∨l	performs action "k" or "1" or both
k*l	performs action "1" in case of not performing action "k"
□k	performs the action "k" forever
◊k	may perform action 'k"
○k	performs action "k" at the next moment
♦k	has performed action "k"
A▷B	always performs action "A" until performing action "B", showing the sequence of these two actions

<rdfs: subClassOf rdf: resource = "<P_1, SP_2, SP_3,... SP_n>"//Defining class resources

<0bjectProperty rdf: about = "#SP_7">//Defining object-oriented domain relationships

<domain rdf: resource = "# Security, Privacy">

<range rdf: resource = "# o">

<ObjectIntersectionOf: SP: o>//Defining the signal interaction

ActSet(Φ)$_1$: $AD \rightarrow \bigcirc CS(k_1 \wedge k_2 \wedge k_3 \wedge \ldots \wedge k_n) \rightarrow ?(CS > 0 \wedge \surd DD)^*(CS \leq 0 \wedge \surd NDD)$

● Graded copyright protection

When a user sends an access request, the platform will determine the AID. If the AID is larger than 0, then the VIP member or purchaser can watch all AVs. If the AID equals to 0, then the user can watch ND media only. If the AID is less than 0, then the user can not watch D media, but some ND media.

C2 = <ID, Atb_2, ActSet(Φ) $_2$>

Atb_2:

Defined0bject rdf: ID = "QA_7"//Defining the signal's name "QA_7"

<rdfs:subClassOf rdf: resource = "<QA_1, QA_2, QA_3,... QA_n>"">//Defining class resources

<0bjectProperty rdf: about = "#QA_7">//Defining object-oriented domain relationships

<domain rdf: resource = "# Quality-Assured">

<range rdf: resource = "# o">

<ObjectIntersectionOf: QA: o>//Defining the signal interaction

ActSet(Φ)$_2$: $AD \rightarrow \bigcirc CS(k_1 \wedge k_2 \wedge k_3 \wedge \ldots \wedge k_n) \rightarrow ?(AID > 0\ (D \cap ND))^*(AID = 0 \wedge (ND \cap \neg D))^*(AID < 0 \wedge$ (part of $ND \cap \neg D$))

● Determine access control

When a user sends an access request, the platform will perform an access control strategy to determine the user ID. If the ID satisfies the access strategy set up by another user, then the user can access successfully; otherwise, the user cannot access successfully.

C3 = <ID, Atb_3, ActSet(Φ)$_3$>

Atb_3:

Defined0bject rdf: ID = "SP_4"//Defining the signal's name " SP_4"

<rdfs: subClassOf rdf: resource = "<SP_1, SP_2, SP_3,... SP_n>" > //Defining class resources

<0bjectProperty rdf: about = "# SP_4">//Defining object-oriented domain relationships

<domain rdf: resource = "# Security, Privacy">

<range rdf: resource = "# o">

<ObjectIntersectionOf: SP: o>//Defining the signal interaction

ActSet(Φ)$_3$: $AD \rightarrow \bigcirc CS(k_1 \wedge k_2 \wedge k_3 \wedge \ldots \wedge k_n) \rightarrow ?(AID > 0 \wedge \surd Vit)^*(AID \leq 0 \wedge \surd NVit)$

● System alerting for submitting operations

After the user request for content submission, according to the submission strategy to determine, if it is successful, there will be a pop-up prompts, after confirm, it will return to the original page, if t is fails to submit, will pop up an unsuccessful prompt, and returns to the content submission page.

C4 = <ID, Atb_4, ActSet(Φ)$_4$>

Atb_4:

Defined0bject rdf:ID = "U_5"//Defining the signal's name " U_5"

<rdfs:subClassOf rdf:resource = "<U_1, U_2, U_3,... U_n >" > //Defining class resources

<0bjectProperty rdf:about = "#U_5">//Defining object-oriented domain relationships

<domain rdf:resource = "# Usability">

<range rdf:resource = "# o">

<ObjectPropertyAssertion>

<:submit prompt>

<ObjectIntersectionOf(:U:o)>//Defining the signal interaction

</ObjectProperty>

ActSet(Φ)$_4$: $AD \rightarrow \bigcirc CS(k_1 \wedge k_2 \wedge k_3 \wedge \ldots \wedge k_n) \rightarrow ?(SS \wedge \surd Vit \bigcirc PLPrompt)^*(NSS \wedge \surd NVit \bigcirc PLPrompt)$

● Vulnerabilities fixing prompt

After the regular repairing, the platform will send a message to the user immediately, after the user login operation pop-up message prompts.

C5 = <ID, Atb_5, ActSet(Φ)$_5$>

Atb_5:

Defined0bject rdf:ID = "SP_3"//Defining the signal's name " SP_3"

<rdfs:subClassOf rdf:resource = "<SP_1, SP_2, SP_3, ... SP_n >"">//Defining class resources

<0bjectProperty rdf:about = "#SP_3">//Defining object-oriented domain relationships

<domain rdf:resource = "# Security, Privacy">

<range rdf:resource = "# o">

<ObjectPropertyAssertion>

<:submit prompt>

<ObjectIntersectionOf(:SP:o)>//Defining the signal interaction

</ObjectProperty>

ActSet(Φ)$_5$: $AD \rightarrow \bigcirc CS(k_1 \wedge k_2 \wedge k_3 \wedge \ldots \wedge k_n) \rightarrow ?$ PLPrompt▷ $(\surd DD \vee \surd NDD)$

In this section, the general method of constructing ontology is applied to OSNs evaluation. The signals' extraction of security and trustworthiness was completed with the help of domain experts. OWL was used to describe the entities, attributes and relationships, as well as the axiom was added to the association attribute to define the constraints between the concepts better. The knowledge ontology proposed here provides a semantic basis and logical model for solving both security and trust signals integration and platform heterogeneity, and its final realization would depend on the specific web services.

4. Comprehensive crowd evaluation method for security and trustworthiness measurement

When using the social media platform, users can apply the signal classification model to analyze signals shown in the platform and understand whether these signals satisfy the aforementioned definitions. For the platform administrator, the building signaling theory evaluation model can systematically manage platform signals. In the platform, different signals have different weight influences on users. With respect to the comprehensive evaluation of problems, every factor will be designed with a definite score. However, one score is insufficient to evaluate several problems. For example, when the quality of a commodity is evaluated, influencing factors, such as color, price, and style, should be considered. Different results may be obtained under the same evaluation factor, so that such result is not a definite number, but a range or even a fuzzy concept. In the evaluation under the premise of different user age, occupation, the use of social software frequency, the

Table 3
Trust evaluation index system for the online social networks platform.

Target Layer A	Criterion Layer B	Index Layer C
Evaluation of the signal conditions of the social media network	B1 Usability	C1 The system has popped up successful/failed submission hint
		C2 Access to the social website will be damaged because of information loss and disconnection
	B2 Transparency	C3 The platform is officially certified or not
		C4 Website contents will not be mixed with ads
	B3 Security and privacy	C5 Background encryption of user data
		C6 Safe guarantee for the transmission of the sensitive information of users
		C7 The platform will regularly repair security vulnerabilities and provide hints
		C8 The user can set those who can see the information
		C9 Trustworthy login determination for users
		C10 The platform provides hints/cues about how to prevent security threats
	B4 Quality-Assured	C11 The social network allows users to evaluate and score platform information or not
		C12 The platform provides a reliable feedback/report system for objectionable contents
		C13 The platform provides and implements a graded digital copyright protection system

Table 4
List of index measurements.

Value range	Meaning
$a_{ij} = \tilde{1}$	Element "i" has equivalent importance for factors in the previous layer with element "j."
$a_{ij} = \tilde{3}$	Element "i" is slightly more important than element "j."
$a_{ij} = \tilde{5}$	Element "i" is more important than element "j."
$a_{ij} = \tilde{7}$	Element "i" is far more important than element "j."
$a_{ij} = \tilde{9}$	Element "i" is extremely more important than element "j."
$a_{ij} = \tilde{2}n$, $n = 1, 2, 3, 4$	Importance of "i" and "j" is between $a_{ij} = 2n-1$ and $a_{ij} = 2n+1$.
Otherwise	$a_{ij} = 1/a_{ji}$

evaluation results are uneven, especially when user is not filtered, in order to improve the accuracy of evaluation results, the user evaluation results should be blurred. Therefore, when the security and trustworthiness of the platform is evaluated, the fuzzy comprehensive evaluation method is applied to obtain the correct evaluation results. The description of the static and dynamic interactive behaviors of the signals in the platform that need to be evaluated could be applied to the setting of crowd evaluation environment, together with clarifying the logical relationships and optimizing the consistency. FAHP (The Fuzzy Analytic Hierarchy Process) is a multi-criteria decision-making method proposed by T.L.Saaty, a professor at the University of Pittsburgh in the mid-1970s. Its ambiguity is mainly manifested in the representation of the judgment matrix. And it also be used to evaluate the outcome of global software development project [26] and predict HF(Heart faiure) risks in medical science [27]. Fuzzy AHP (FAHP) can solve the existing problems of traditional analytic hierarchy process and improve the reliability of decision making. This article is based on a fuzzy consistency matrix.

4.1. The computation of signal weight using AHP method

4.1.1. Determining the evaluation index system

The trust evaluation index system for the multimedia social network is determined and the trustworthiness-critical and security-related signals are extracted from the classified signals in signaling theory, as shown in Table 3.

4.1.2. Determining the evaluation standards

The evaluation indices include six levels, i.e., no effect, little effect, medium effect, main effect, significant effect, uncertainty.

4.1.3. Calculating the index weight

When measuring the relative importance of indices, the AHP method has a list of measurements for relative importance with nine levels, as shown in Table 4.

Table 5
Trust evaluation index system and weight of Online social network platform.

Target layer A	Criteria layer B	Index layer C	The weight relative to A	Rank
Evaluation of the signal conditions of the social media network	B1 Usability	C1 The system has popped up successful/failed submission hint.	0.013	10
		C2 Access to the social website will be damaged because of information loss and disconnection.	0.040	7
	B2 Transparency	C3 The platform is officially certified or not.	0.024	9
		C4 Website contents will not be mixed with ads.	0.120	3
	B3 Security and Privacy	C5 Background encryption of user data.	0.153	(2)
		C6 Safe guarantee for the transmission of the sensitive information of users.	0.153	(2)
		C7 The platform will regularly repair security vulnerabilities and provide hints.	0.074	(5)
		C8 The user can set those who can see the information.	0.074	(5)
		C9 Trustworthy login determination for users	0.026	(8)
		C10 The platform provides hints/cues about how to prevent security threats.	0.026	(8)
	B4 Quality-Assured	C11 The social network allows users to evaluate and score platform information or not.	0.045	6
		C12 The platform provides a reliable feedback/report system for objectionable contents.	0.081	4
		C13 The platform provides and implements a graded digital copyright protection system.	0.170	1

Table 6
Fuzzy evaluation matrix *W* of OSNs platform signals.

Criteria layer B	Index layer C	Fuzzy Comprehensive Evaluation Matrix					
		Uncertainty	No effect	Little effect	Medium effect	Main effect	Significant effect
B1 Usability	C1 The system has popped up successful/failed submission hint.	0.042	0.042	0.105	0.314	0.251	0.246
	C2 Access to the social website will be damaged because of information loss and disconnection.	0.026	0.037	0.079	0.325	0.319	0.215
B2 Transparency	C3 The platform is officially certified or not.	0.021	0.026	0.084	0.183	0.288	0.398
	C4 Website contents will not be mixed with ads.	0.026	0.063	0.079	0.262	0.246	0.325
B3 Security and Privacy	C5 Background encryption of user data.	0.010	0.047	0.037	0.199	0.230	0.476
	C6 Safe guarantee for the transmission of the sensitive information of users.	0.005	0.031	0.068	0.173	0.188	0.534
	C7 The platform will regularly repair security vulnerabilities and provide hints.	0.005	0.063	0.052	0.267	0.277	0.335
	C8 The user can set those who can see the information.	0.000	0.073	0.031	0.288	0.277	0.330
	C9 Trustworthy login determination for users	0.005	0.042	0.042	0.188	0.283	0.440
	C10 The platform provides hints/cues about how to prevent security threats.	0.016	0.084	0.094	0.262	0.293	0.251
B4 Quality-Assured	C11 The social network allows users to evaluate and score platform information or not.	0.010	0.105	0.147	0.351	0.188	0.199
	C12 The platform provides a reliable feedback/report system for objectionable contents.	0.010	0.079	0.068	0.225	0.325	0.293
	C13 The platform provides and implements a graded digital copyright protection system.	0.042	0.079	0.115	0.283	0.230	0.251

Table 7
Fuzzy comprehensive evaluation results of Signal weights.

	Uncertainty	No effect	Little effect	Medium effect	Main effect	Significant effect
C1	0.0005	0.0005	0.0014	0.0041	0.0033	0.0032
C2	0.0010	0.0015	0.0032	0.0130	0.0128	0.0086
C3	0.0005	0.0006	0.0020	0.0044	0.0069	0.0096
C4	0.0031	0.0076	0.0095	0.0314	0.0295	0.0390
C5	0.0015	0.0072	0.0057	0.0304	0.0352	0.0728
C6	0.0008	0.0047	0.0104	0.0265	0.0288	0.0817
C7	0.0004	0.0047	0.0038	0.0198	0.0205	0.0248
C8	0.0000	0.0054	0.0023	0.0213	0.0205	0.0244
C9	0.0001	0.0011	0.0011	0.0049	0.0074	0.0114
C10	0.0004	0.0022	0.0024	0.0068	0.0076	0.0065
C11	0.0004	0.0047	0.0066	0.0158	0.0085	0.0090
C12	0.0008	0.0064	0.0055	0.0182	0.0263	0.0237
C13	0.0071	0.0134	0.0196	0.0481	0.0391	0.0427

Experts were invited to compare the importance of various factors in different evaluations, and the results were used to derive the weight distribution of the AHP determination matrix. The relative importance of the factors in layers B and C is investigated to obtain the determination matrices, i.e., A–B and B–C.

According to the formula (1):

$$w_i = \sum_{f=1}^{6} \frac{a_{ij}}{6}, i = 1, 2, \ldots, 6 \quad (1)$$

① Calculate the A–B determination matrix and determine the weight to obtain the following results:

W = [w_1, w_2, w_3, w_4] = [0.419, 1.133, 4.000, 2.333].

② Implement normalization processing for w and obtain the weight of layer B relative to layer A:

W = [0.053, 0.144, 0.507, 0.296].

③ Sort in accordance with the weights in index layer C relative to layer A, as shown in Table 5.

4.2. Comprehensive fuzzy evaluation

The understanding of the user of trustworthiness-critical and security-critical signals is applied to implement qualitative grade evaluation, and the determination grades include six levels, i.e., no influence, slight influence, general influence, major influence, important influence, and uncertain. From the data through the online survey results, the fuzzy evaluation matrix for each platform signals was obtained, as shown in Table 6.

The fuzzy comprehensive evaluation method is adopted for the fuzzy subset of the weight coefficient "*W*" and fuzzy comprehensive evaluation matrix "*R*" (see Table 7 for $C = W \times R$ results).

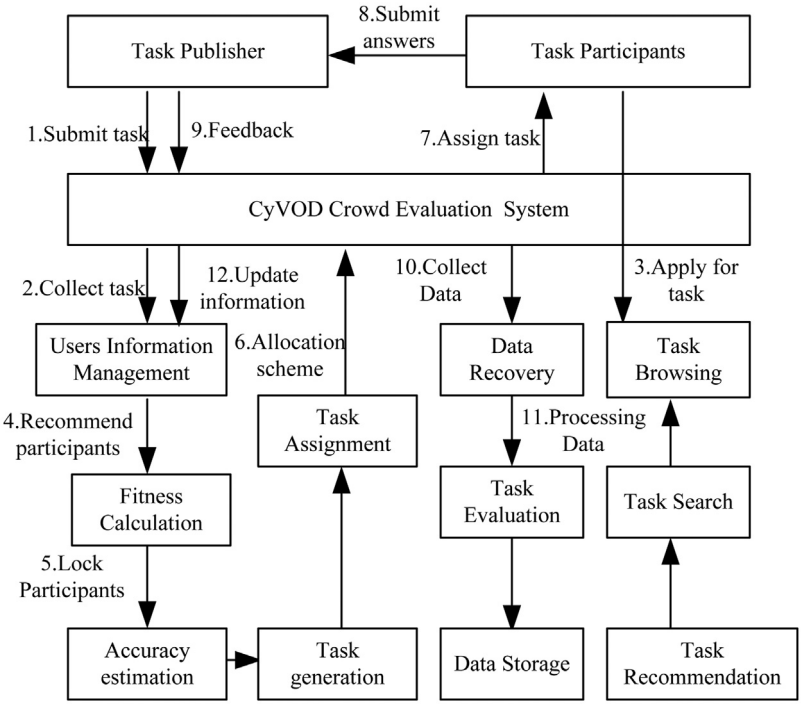


Fig. 1. Crowd evaluation architecture of CyVOD multimedia social network platform.

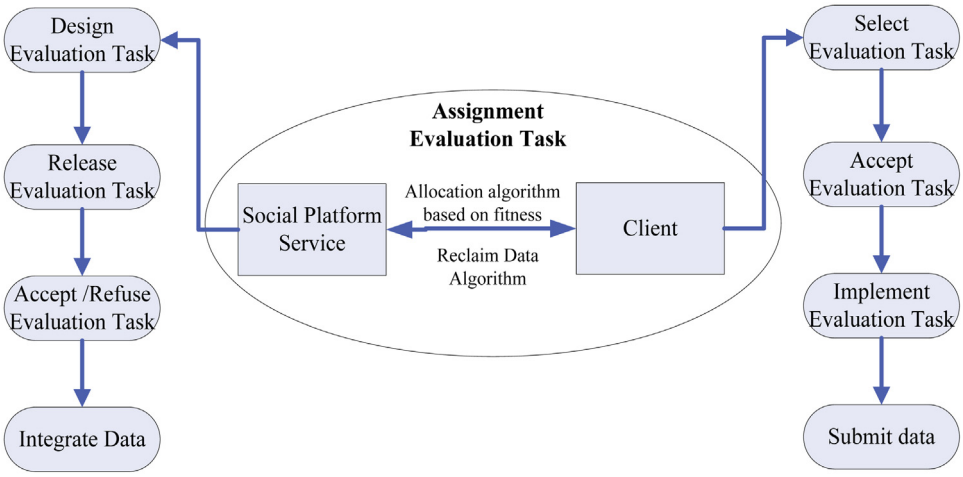


Fig. 2. Task assignment graph of crowd evaluation on CyVOD multimedia social network platform.

From the maximum membership principle and quantitative analysis results of the influence factors, 13 platform signals are selected and sorted, and the result is as follows: C6 > C5 > C4 > C7 > C8 > C9 > C3 > C12 > C10 > C13 > C11 > C2 > C1.

4.3. Crowd evaluation computation model for security and trustworthiness

Version upgrade for the social network platform is conducted to ensure improvement of previous user evaluation, feedback, and experience. User trust on the platform changes with the platform version. Generally,

(1) the weight value wi (seen in Formula(1)) from the F-AHP calculation for trustworthiness-critical and security-critical signals is shown in the platform;

Table 8
Signal evaluation values on CyVOD Multimedia social platform V2.0.

Signal	F-AHP signal integrated evaluation value
TR_{C1}	0.0520
TR_{C4}	0.5261
TR_{C7}	0.3187
TR_{C8}	0.2941
TR_{C10}	0.1133
TR_{C12}	0.3447
TR_{C13}	0.7453

(2) the difference value of update time t_{e_n} between latest version number and previous version number $t_{e_{n-1}}$ at the moment of trust evaluation for entity users is derived as follows:

$$t_{ver} = t_{e_n} - t_{e_{n-1}}; \quad (2)$$

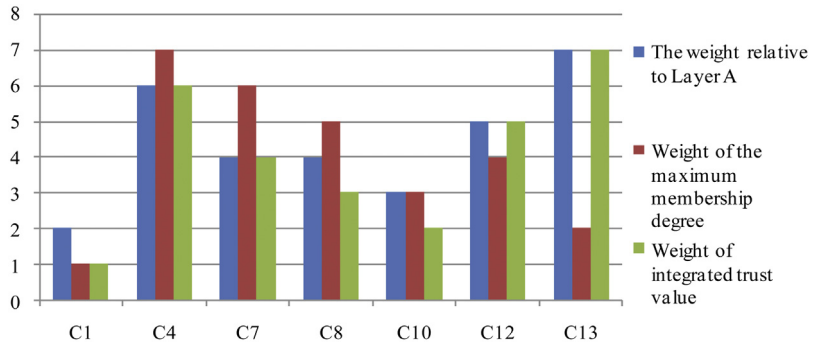


Fig. 3. Comparisons of signal integrated evaluation value on CyVOD Multimedia social platform V2.0.

Table 9
Experimental comparison chart on CyVOD Multimedia social platform.

Signal	Experiment 1 comprehensive trust value	Experiment 2 comprehensive trust value	Increment of trust value
TR_{C1}	0.0520	0.0521	0.0001
TR_{C4}	0.5261	0.5366	0.0105
TR_{C7}	0.3187	0.3268	0.0081
TR_{C8}	0.2941	0.3175	0.0234
TR_{C10}	0.1133	0.1136	0.0003
TR_{C12}	0.3447	0.3566	0.0119
TR_{C13}	0.7453	0.7650	0.0197

(3) the assessed value of dynamic crowd for trustworthiness-critical and security-critical signals under the current version is S_{e_n};

(4) the one-dimensional comprehensive evaluation value for the F-AHP signal in the social network platform is obtained:

$$TR_n = \sum_{i=1}^{m} \frac{S_{e_n} * w_i}{m}; \tag{3}$$

(5) the platform security and trustworthiness changes from version e_n to e_{n-1}:

$$f_{Trust} = \frac{TR_{ver}}{t_{ver}} = \frac{\sum_{i=1}^{m} \frac{S_{e_n} * w_i}{m} - \sum_{i=1}^{m} \frac{S_{e_{n-1}} * w_i}{m}}{t_{e_n} - t_{e_{n-1}}}; \tag{4}$$

5. Experiments and results analysis

The CyVOD (Dream of the hurricane (VOD × Cyclone, referred to as CyVOD)) platform is a multimedia social network platform that supports online audio/video play and is designed with the crowd evaluation model and online investigation system [28,29]. This system provides data support for the model. This experiment is divided into two parts. In Experiment 1, crowd evaluation under the CyVOD V2.0 platform is performed and evaluation grades for signals that can be referred to by users in the platform are set up. Then, users can score based on their experience. In Experiment 2, crowd evaluation data and feedback opinions collected from experiment 1 are analyzed. Then, the administrator makes the corresponding improvements to the CyVOD platform and collects and analyses the evaluation data of users in the period after the launch of the new version. The collection time for the evaluation data ends as of the date of launching the subsequent version. A total of 140 pieces of crowd evaluation data have been collected. We realized the security and trustworthiness evaluation system, as illustrated by Figs. 1 and 2, based crowd computing to make the following experiments.

5.1. Experiment 1

Under the CyVOD V2.0 platform, seven signals are implemented with crowd evaluation, i.e., “C1 login dialog security for website”, “C4 limitation for website main contents and promotion contents”, “C7 update hint for platform”, “C8 friends visible/access control evaluation”, “C10 security warning for user information”, “C12 feedback of bad information” and “C13 graded copyright protection system”. Table 8 shows the FAHP trust value for each signal under the CyVOD V2.0 platform.

The FAHP trust value for each signal in the CyVOD platform is calculated and compared with the signal weight relative to layer A and weight of the maximum membership degree that are scientifically calculated after sorting and weighting, as shown in Fig. 3. In the CyVOD platform, the evaluation values are low for “C7 update hint for platform”, “C8 friends visible/access control evaluation” and “C10 security warning for user information” but high for “C13 graded copyright protection system”. The platform administrator will make the corresponding improvements according to the evaluation results, strengthen the access control strategy, and complete the platform with respect to the update hint and security warning. However, the evaluation value for “C13 graded copyright protection system” is the highest, which satisfies the theme of digital copyright protection for the CyVOD platform. The platform administrator determines the signals to be improved under the current version according to the sorting results for security and trustworthiness.

5.2. Experiment 2

From the previously presented results of data analysis, the CyVOD platform administrator has made improvements to the media platform, shown previous versions in the form of a static list in the individual center of registered users, sent an update of new version to users before the subsequent update, simplified the method of adding friends in the friend management center, added a

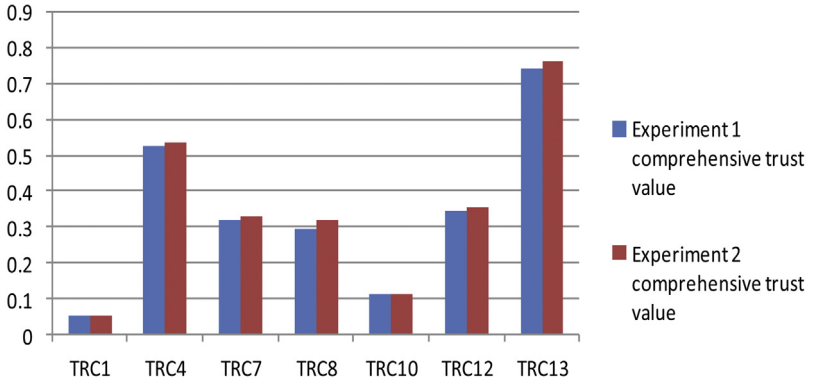


Fig. 4. Integrated evaluation value comparison chart between Experiment 1# and 2#.

new access control strategy, and designed the security hint for typing into individual information if necessary. One month after the launch of the new version, new crowd evaluation data were collected. After the calculation, we obtained the FAHP trust value of each signal under the CyVOD V2.0.1 platform and the comparison results with increment of trust value in experiment 1, as shown in Table 9.

When the FAHP trust value for each signal is sorted, weighted, and compared with the signal weight relative to layer A and the maximum membership weight, the results remain unchanged; thus, the security and trustworthiness of each signal does not changed significantly. From the horizontal comparison conducted for the comprehensive trust value of each signal under V2.0.1 and V2.0, the trust values for six signals (i.e., "C1 login dialog security for website", "C4 limitation for website main contents and promotion contents", "C7 update hint for platform", "C8 friends visible/access control evaluation", "C12 feedback of bad information" and "C13 graded copyright protection system") have been elevated, but the trust value for "C10 security warning for user information" slightly declines (see Fig. 4).

On one hand, this method is applied to perform qualitative analysis with respect to static attributes and dynamic behavior and to evaluate high-quality signals shown to users or not. On the other hand, combined with the security-related and security and trustworthiness-critical signals in this study, the FAHP method is applied to obtain the weight value for the rules. Moreover, quantitative evaluation is conducted for these signals based on the crowd evaluation results.

Formula (3) implements trust evaluation in the current stage for comprehensive signal evaluation values based on the survey results from users of major social media and the scientific calculation and application of crowd evaluation that can be referred to by users. Horizontal comparison of the results is conducted to analyze signals with low security and trustworthiness, whereas longitudinal comparison of the results is conducted to assess the trust increment of each signal. Formula (4) calculates the change rate for platform security and trustworthiness, and "m" is the quantity of signals for crowd evaluation. With the continuous improvement and increase in the number of users, the evaluation value of users for the platform changes, which is in direct proportion to platform security and trustworthiness, such that the comprehensive trust value will also change with the platform version. The change rate for platform security and trustworthiness describes the slow or fast change of security and trustworthiness within a certain period in the social network platform, which will also change after signal adjustment for the subsequent stage. This mathematical model is significant in that the user score may be increased under the new version only when signals with low user scores are improved within a short time and the version is updated. The short term for version update will result in better user experience, increase the score and security and trustworthiness, and elevate the change rate of security and trustworthiness, which effectively demonstrated that high-quality signals in signaling theory represent a high-quality platform.

6. Conclusions

The classification standard for platform signals in the social media platform has been proposed in this study, which applied ontology descriptive language and behavior sequential logic method to describe the static attributes and dynamic behavior, respectively. Moreover, the FAHP method has been used to calculate the weights of the corresponding signals, and weight sorting has also been performed in accordance with the maximum membership principles for 13 security-critical and trustworthiness-critical signals. Finally, a dynamic security and trust evaluation model has been proposed for the social media platform, and CyVOD is applied to calculate the evaluation results to conduct horizontal and longitudinal comparisons and analyses, which have provided references for the platform administrator to improve the version and improve the functions in the social media platform, with a result of avoiding low-quality and fraudulent services for social users. This comprehensive computational model is suitable for any generic OSN platform or application, by leveraging crowd big data to assessment a specific platform. which not only can be evaluated in trustworthiness, but also design a specific function for scoring and comprehensive assessment to evaluate and improve it. The future work of the paper is to explore a crowd assessment architecture and evaluation task recommender.

Acknowledgments

The work was sponsored by National Natural Science Foundation of China Grant No. 61370220, Plan For Scientific Innovation Talent of Henan Province Grant No. 174200510011, Program for Innovative Research Team (in Science and Technology) in University of Henan Province Grant No. 15IRTSTHN010, Program for Henan Province Science and Technology Grant No. 142102210425, Natural Science Foundation of Henan Province Grant No. 162300410094, Project of the Cultivation Fund of Science and Technology Achievements of Henan University of Science and

Technology Grant No. 2015BZCG01. We give thanks to Jie Wang, Cheng Li and Fangyun Liu for their technical assistance on CyVOD MSN prototype, and also would like to thank the reviewers and editor for their valuable comments, questions, and suggestions.

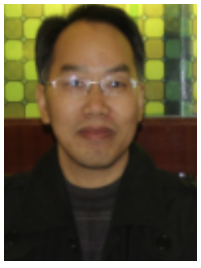
References

[1] A.M. French, An empirical analysis evaluating trust in social networking, Int. J. Web Based Commun. 11 (1) (2015) 4–24.
[2] S. Adali, R. Escriva, M.K. Goldberg, et al., Measuring behavioral trust in social networks, Proceedings of IEEE International Conference on Intelligence and Security Informatics (2010) 150–152, http://dx.doi.org/10.1109/ISI.2010.5484757.
[3] Z.Y. Zhang, K. Wang, A trust model for multimedia social networks, Soc. Netw. Anal. Min. 3 (4) (2013) 969–979.
[4] E.M. Clark, J.R. Williams, C.A. Jones, et al., Sifting robotic from organic text: a natural language approach for detecting automation on Twitter, J. Comput. Sci. 16 (2015) 1–7, http://dx.doi.org/10.1016/j.jocs.2015.11.002.
[5] S.P. Marsh, Formalising Trust as a Computational Concept, University of Stirling, 1994 (OAI:dspace.stir.ac.uk:1893/2010).
[6] J. Bao, J.J. Cheng, Group trust algorithm based on social network, Comp. Sci. 39 (2) (2012) 38–51.
[7] J. Huang, F.P. Nie, H. Huang, et al., Social trust prediction using heterogeneous networks, ACM Trans. Knowl. Discov. Data 7 (4) (2013) 1774–1778.
[8] C. Fernandez-Gago, I. Agudo, J. Lopez, Building trust from context similarity measures, Comp. Stand. Interfaces 36 (4) (2014) 792–800.
[9] Z.Y. Zhang, B.B. Gupta, Social media security and trustworthiness: overview and new direction, Future Gener. Comp. Syst. (2016), http://dx.doi.org/10.1016/j.future.2016.10.007.
[10] D.V. Medhane, A.K. Sangaiah, ESCAPE: effective scalable clustering approach for parallel execution of continuous position-based queries in position monitoring applications, IEEE Trans. Sustain. Comput. 99 (2017) 1, http://dx.doi.org/10.1109/TSUSC.2017.2690378.
[11] S. Agreste, M.P. De, E. Ferrara, et al., Trust networks: topology, dynamics and measurements, IEEE Internet Comput. 19 (6) (2015) 26–35.
[12] S. Kaur, S. Singh, S. Kaushal, et al., Comparative analysis of quality metrics for community detection in social networks using genetic algorithm, Neural Netw. World 26 (6) (2016) 625–641.
[13] X. Xiao, C. Chen, A.K. Sangaiah, et al., CenLocShare: a centralized privacy-preserving location-sharing system for mobile online social networks, Future Gen. Comp. Syst. (2017), http://dx.doi.org/10.1016/j.future.2017.01.035.
[14] M.P. De, E. Ferrara, D. Rosaci, et al., Trust and compactness in social network groups, IEEE Trans. Cybern. 45 (2) (2015) 205–216.
[15] Z.Y. Zhang, K.L. Wang, A trust model for multimedia social networks, Soc. Netw. Anal. Min. 3 (4) (2013) 969–979.
[16] Z.Y. Zhang, A formal analytic approach to credible potential path and mining algorithms for multimedia social networks, Comp. J. 58 (4) (2015) 668–678.
[17] S.H. Chen, G.J. Wang, W.J. Jia, Kappa-fuzzy trust: efficient trust computation for large-scale mobile social networks using a fuzzy implicit social graph, Inform. Sci. 318 (2015) 123–143, http://dx.doi.org/10.1016/j.ins.2014.09.058.
[18] B.L. Connelly, S.T. Certo, R.D. Ireland, et al., Signaling theory: a review and assessment, J. Manag. 37 (1) (2011) 39–67.
[19] A. Kirmani, A.R. Rao, No pain, no gain: a critical review of the literature on signaling unobservable product quality, J. Market. 64 (2) (2000) 66–79.
[20] W. Boulding, A. Kirmani, A consumer-side experimental examination of signaling theory: do consumers perceive warranties as signals of quality? J. Consum. Res. 20 (1) (1993) 111–123.
[21] V.A. Zeithaml, Consumer perceptions of price, quality, and value: a means-end model and synthesis of evidence, J. Market. 52 (3) (1988) 2–22.
[22] T. Mavlanova, R. Benbunan-Fich, M. Koufaris, Signaling theory and information asymmetry in online commerce, Inform. Manag. 49 (5) (2012) 240–247.
[23] N. Guarino, Formal ontology and information systems, in: Proceedings of FOIS '98, Trento, Italy, 6–8, June, 1998.
[24] M. Toahchoodee, I. Ray, On the formalization and analysis of a spatio-temporal role-based access control model, Proceedings of the 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security Springer-Verlag (2008) 17–32, http://dx.doi.org/10.1007/978-3-540-70567-3_2.
[25] M. Donick, C. Schonfeldt, A. Thomanek, et al., A model for assessing the degree of formalization and support of learning scenarios, International Conference on Interactive Collaborative Learning (2011) 290–295, http://dx.doi.org/10.1109/icl.2011.6059593.
[26] A.K. Sangaiah, J. Gopal, A. Basu, et al., An integrated fuzzy DEMATEL, TOPSIS, and ELECTRE approach for evaluating knowledge transfer effectiveness with reference to GSD project outcome, Neural Comput. Appl. 28 (1) (2015) 111–123.
[27] O.W. Samue, G.M. Asogbon, A.K. Sangaiah, et al., An integrated decision support system based on ANN and Fuzzy_AHP for heart failure risk prediction, Expert Syst. Appl. 68 (2017) 163–172.
[28] W.N. Feng, Z.Y. Zhang, J. Wang, et al., A novel authorization delegation scheme for multimedia social networks by using proxy re-encryption, Multimedia Tools Appl. 75 (21) (2016) 13995–14014.
[29] Z.Y. Zhang, Z. Wang, D.M. Niu, A novel approach to rights sharing-enabling digital rights management for mobile multimedia, Multimedia Tools Appl. 74 (16) (2015) 6255–6271.

Z. Zhang, born in October 1975, earned his Master, Ph.D. degrees in Computer Science from Dalian University of Technology and Xidian University, P. R. China, respectively. He was ever post-doctoral fellowship at School of Management, Xi'an Jiaotong University, China. Nowadays, he is a full-time Henan Province Distinguished Professor and Dean with Department of Computer Science, College of Information Engineering, Henan University of Science & Technology. He is also a Visiting Professor of Computer Science Department of Iowa State University. Prof. Zhang and research interests include multimedia social networks, digital rights management, trusted computing and usage control. Recent years, he has published over 80 scientific papers and edited 4 books in the above research fields, and also holds 8 authorized patents. He is IEEE Senior Member (06′M, 11′S), ACM Senior Member (08′M, 13′S), IEEE Systems, Man, Cybermetics Society Technical Committee on Soft Computing, World Federation on Soft Computing Young Researchers Committee, Membership for Digital Rights Management Technical Specialist Workgroup Attached to China National Audio, Video, Multimedia System and Device Standardization Technologies Committee. And also, he is editorial board member and associate editor of Multimedia Tools and Applications (Springer), Neural Network World, EURASIP Journal on Information Security (Springer), Social Network Analysis and Mining (Springer), Topic (DRM) Editor-in-Chief of International Journal of Digital Content Technology and Its Applications, leading guest editor or co-guest Editor of Applied Soft Computing (Elsevier), Computer Journal (Oxford) and Future Generation Computer Systems (Elsevier). And also, he is Chair/Co-Chair and TPC Member for numerous international conferences/workshops on digital rights management and cloud computing security.

J. Wen, born in March 1991, is currently a postgraduate majoring in computer science, College of Information Engineering, Henan University of Science & Technology. Her research interest focuses on multimedia social networks and applications.

X. Wang, born in June 1993, is currently a postgraduate majoring in computer science, College of Information Engineering, Henan University of Science & Technology. Her research interest focuses on crowd computing and crowdsocuring system.



C. Zhao, born in October 1972, received his Ph.D .degree in Computer Science at Xi'an Jiaotong University, P. R. China. He is an associate professor at College of Information Engineering, Henan University of Science & Technology. His research interests include machine learning and social network analytics.