Future Generation Computer Systems 86 (2018) 914–925

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Social media security and trustworthiness: Overview and new direction

Zhiyong Zhang[a,b,*], Brij B. Gupta[c]

[a] Information Engineering College, Henan University of Science and Technology, Luoyang 471023, People's Republic of China
[b] Department of Computer Science, Iowa State University, Ames 50010, USA
[c] National Institute of Technology, Kurukshetra, India

HIGHLIGHTS

- The survey investigates the state-of-the-art of social media security and trust.
- We propose a new research direction on crowd evaluations of social media platforms.
- Several key open problems and challenges are also presented in the survey.

ARTICLE INFO

Article history:
Received 25 August 2016
Received in revised form
23 September 2016
Accepted 6 October 2016
Available online 12 October 2016

Keywords:
Social media networks
Security
Trustworthiness
Measurement
Crowd computing

ABSTRACT

The emerging social media with inherent capabilities seems to be gaining edge over comprehensiveness, diversity and wisdom, nevertheless its security and trustworthiness issues have also become increasingly serious, which need to be addressed urgently. The available studies mainly aim at both social media content and user security, including model, protocol, mechanism and algorithm. Unfortunately, there is a lack of investigating on effective and efficient evaluations and measurements for security and trustworthiness of various social media tools, platforms and applications, thus has effect on their further improvement and evolution. To address the challenge, this paper firstly made a survey on the state-of-the-art of social media networks security and trustworthiness particularly for the increasingly growing sophistication and variety of attacks as well as related intelligence applications. And then, we highlighted a new direction on evaluating and measuring those fundamental and underlying platforms, meanwhile proposing a hierarchical architecture for crowd evaluations based on signaling theory and crowd computing, which is essential for social media ecosystem. Finally, we conclude our work with several open issues and cutting-edge challenges.

1. Introduction

The rapid development and daily perfection of modern communication networks technology and information technology have caused revolutionary changes to various industries, fields, and every facet of society across the world. Web 2.0 and Science 2.0 have now become critical network infrastructure and knowledge platform for all participating entities (man, machine, group, and even brain-like computer) in the "Global Village" for exchanging, sharing, contributing a great amount of data, information, knowledge and wisdom. The social media ecosystem focuses on social organization, content media and stakeholders, as well as their comprehensiveness, diversity and intelligence. Thus, it facilitates the emergence of new virtual societal network and organization forms.

In recent years, the use of social media is rapidly growing. Some social networks for instance, LinkedIn, Facebook and MySpace have been very prominent and are now the preferred way of communication for many people. The significance of these websites comes from the fact that the users spend a generous amount of time to update their information and interact with other users and surf other member's profile.

According to the global platform Statista.com, the total number of social media users worldwide will cross 2.13 billion by the year

[*] Corresponding author at: Information Engineering College, Henan University of Science and Technology, Luoyang 471023, People's Republic of China.
E-mail addresses: z.zhang@ieee.org (Z. Zhang), gupta.brij@gmail.com (B.B. Gupta).

http://dx.doi.org/10.1016/j.future.2016.10.007
0167-739X/© 2016 Published by Elsevier B.V.

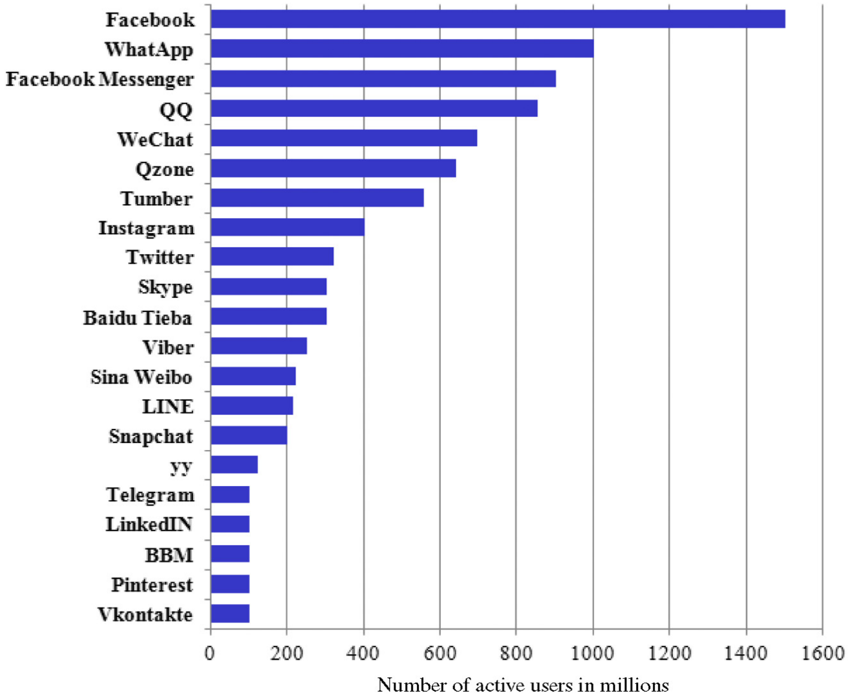

Fig. 1. Leading OSNs around the globe as of January 2016.

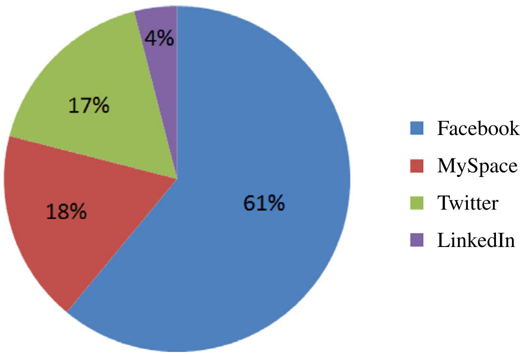

Fig. 2. Sophos security threat report- 2011.

of 2016, in 2010 it was about 970 million, which show that there was an increase in the users 2.2 times from 2010 to 2016. As of April 2016, Facebook is ranked first (as shown in Fig. 1) in the social media market, it has about 1.59 billion users. The number of users of Tencent QQ, which is ranked No. 4 in the world, has reached 899 million as of today. LinkedIn, which is ranked the twentieth in terms of number of users, has 100 million stable user groups. The latest "38th Statistical Report on Internet Development in China" released by official Chinese Internet Network Information Center (CNNIC) shows that by June 2016, the number of Internet users in China will reach 710 million and the popularization rate of Internet will reach 51.7%. These figures show that half of the population in China has be connected to the Internet, 656 million users mainly via mobile devices.

According to the threat security report given by Sophos in 2011, about 0.5 billion Internet users over the web has already used Facebook at that time. This report reveals that Facebook is the most popular social networking site, but it also face the highest security risks, which accounted for 61% (shown in Fig. 2). Unfortunately, the scenario continues until today.

With the exponential and explosive increase of social users, current (mobile) social media tools, services, and platforms try to maintain the number of both general users and platform-based (content) services providers, activity and liveliness by providing personalized services, recommended content/friends, together with upgrading user quality of experience [1,2]. Users have become much more addicted to share their personal ideas, sentiments and experiments to a wider range of friends as well as friends of friends by leveraging video, images and photos, etc. The user evolution of online communication enables a new user-created contents ecosystem [3].

Unfortunately, this type of social media ecosystem, which is "taken from the people and is used in the interests of the people", suffers from data interception, information fraudulence, privacy spying, and copyright infringement from disorganized social organizational forms and non-friendly participation bodies. In the past years, the rise of social media cybersecurity incidents has been explosive, and there are many reports and comments. For example, Delta Airlines' social media accounts were badly hijacked on February 10th, 2015, and the attackers posted annoying and questionable content. On July 20th of this year, SongTaste, one of social media platforms primarily focused on music sharing, was closed indefinitely due to unsolvable music copyrights issue. Besides, there is a report titled by "Social Media Plays Key Role in Bank Fraud" from an interview with American Bankers Association's Mrs. Jane Yao, and she argued how to cope with the increased fraud activity in social media sites Summarily speaking, it is clear that this embarrassment is caused by technology growth, responsibilities of organizational behavior, and platform monitoring. The (mobile) social media ecosystem urgently needs to establish security and trustworthiness. These two factors should be merged together to be addressed and interpreted. Otherwise, they can affect the dependence, attention, and service efficiency of the platforms (owners) by the individual users and content (information) service providers. Considering the mergence of trust and even risk into security issues, the investigation of social media security would be more sophisticated and challenging than ever before, as combined with explosive social users, as well as their various identifications, roles, groups and corresponding behaviors.

Therefore, the trustworthiness and security of the fundamental platforms is important to various aspects of social media ecosystem in order to establish a credible, safe, and lasting social platform [4]. Summarily speaking, the available studies on social media

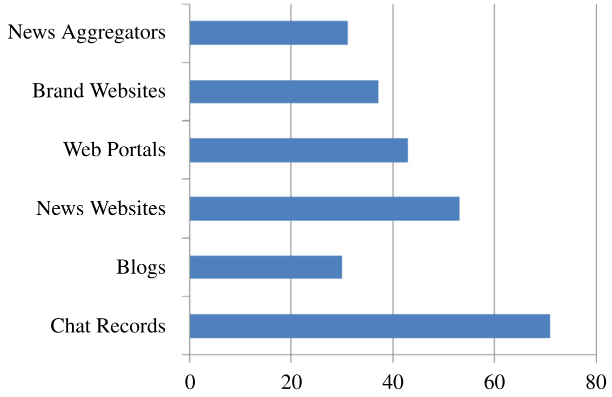

Fig. 3. Percentage level of trust users have on various social media domains [5].

technology mainly use traditional security techniques, cryptography, and image processing methods to address problems related to partial security, privacy protection, and copyright protection. Most studies are also conducted in terms of social media analysis, searching, exploration, assessment, and sentiment analysis on the basis of machine learning and deep learning.

In a report, Phil Mershon director of Social media examiner mentioned that social media users share the contents of blog with the least probability, however, if the information comes from an acquittance or family they are most likely to share it with others due higher trust level as shown in Fig. 3.

With regard to network and information security research, the National Science and Technology Council indicates in the "Federal Cybersecurity Research and Development Strategic Plan" released in February 2016 that "evidence-driven" network security research methods are urgently needed. Furthermore, the evidence can take forms like subject-matter-expert opinions, qualitative evidence, models of protection from defined threats, empirical evidence, and mathematical proofs. To cope with the serious challenge of increasingly insecure and untrusted social media systems and applications, we should explore the development, perfection and evolution of social medial ecosystem from the perspectives of information technology, information management and social behavior [6–8]. In particular, we need to innovate and develop breakthroughs in social media platforms which are the fundamental and key infrastructure. This paper mainly investigates the state-of-the-art of social media security and trustworthiness. Then, proposes a new direction on social media security and trustworthiness.

Remainder of the paper consists of following sections: Overview on social media security and trustworthiness is presented in Section 2. Section 3 describes a new direction of Social Media security and trustworthiness. Major open issues and challenges have been covered in Section 4. Finally, we concluded our work in Section 5.

2. Overview on social media security and trustworthiness

In the beginning of the section, a spectrum of the following research works is first summarized for more clearly presenting the main concerns and working directions of a few interesting and meaningful works. There are several aspects specifically categorized into model, mechanism, algorithm/protocol, mathematical/logic, engineering and survey, as illustrated by Table 1.

2.1. Various attacks on social media

The various types of Social media platforms invite a variety of attacks towards them, which tend to steal users' identity or threaten then privacy and trust over the network. In this section, we present the some attacks which are prominent over the social media these days. Table 2. represents a comparative analysis of these attacks [9,10].

- **Identity theft**

  This refers to the real time impersonation of legitimate user, the attacker takes control the target profile and is able to successfully other genuine user that the profile belongs to him. Here the attacker misuses the profile in any way possible which could have severe impact on the user whose identity it was once.
- **Spam attack**

  Here, the attacker somehow obtains communication details about the user and are able to send spam or junk data. The communication details are not that hard to obtain, they can be extracted by the profiles of the legitimate user. The spam emails send in bulk cause network congestion and cost of sending emails falls mostly upon the service providers and sometimes on the user.
- **Malware attacks**

  They are becoming very common among social networking sites these. The attackers send malware injected scripts to the legitimate user. On clicking the malicious URL a malware might be installed on the attackers devices or it can lead to a fake website which attempts to steal some personal information from the target user.
- **Sybil attacks**

  Fake profiles are the foundation for Sybil attacks, which can be harm the proper functioning of the social media platform, they can be used for the distribution of junk information or even malware over the network. To prevent these attacks the authentication mechanisms while user registration should be stronger.
- **Social phishing**

  It refers to the attack where the attacker aims to obtain sensitive information from a target user via some fake website which appears to be real or by impersonating someone the target is acquainted with. These attacks can be significantly reduced if the users are aware and should examine the data they receive carefully beforehand.
- **Impersonation**

  Here the aim of the attacker is to create fake profile in order to successfully impersonate a real-world person. This attack highly depend on the authentication techniques that are faced by the users while registration to make new account. These attacks can do serious damage to the target which is being impersonated.
- **Hijacking**

  It refers to acquiring control over someone else's profile. The attacker is successful in hijacking a legitimate profile if they are able to crack login password of the account. Weak passwords are thus a poor choice as they increase the threat of hijacking such passwords can be obtained by dictionary attacks. Strong passwords and changing them frequently is good practice.
- **Fake requests**

  The attacker sends fake request with their own profile, so as to enlarge their network. If the users accept fake request it gives the attacker more privileges and they are able to more information from the victim profiles. The prevention of fake requests is not possible, thus, the user should be more responsible over the social media.
- **Image retrieval and analysis**

  The attacker here uses various face and image recognition software to find more information about the target and its linked profiles. It not only affects the target but also his/her friends and family. This attacks aims to gather images videos etc. from the target.

Table 1
A collection of social media security, trust and related research works.

	Model	Mechanism	Algorithm/Protocol	Mathematics/Logic	Engineering	Survey
Security and privacy	Refs. [11–14]	Refs. [16,62]	Refs. [17,18,24,25]	Refs. [20–23,64]	Ref. [19]	Refs. [15,51,61,63]
Trust and evaluation	Refs. [39,42,43]	Ref. [38]	Refs. [36,37,41]	Ref. [44]	Ref. [40]	N/B
Intelligent applications	Ref. [1]	Ref. [55]	Ref. [54]	Ref. [53]	Refs. [49,65]	Refs. [48,50,52]

Table 2
Comparison of most popular attacks on online social networks.

Measure	Impact on user	Effectiveness of server side protection mechanism	Effectiveness of user side protection mechanism	Threat to data privacy	Threat to data integrity
Identity theft	Average to high	Poor	Poor	Yes	Yes
Spam attack	Small	Strong	Poor	No	No
Malware	High	Medium	Medium	Yes	Yes
Sybil attack	Average	Strong	Poor	No	Yes
Social phishing	High	Poor	Strong	Yes	Yes
Impersonation	High	Poor	Poor	Yes	Yes
Hijacking	High	Poor	Poor	Yes	Yes
Fake requests	Small	Poor	Strong	Yes	No
Image retrieval and analysis	Average to high	Medium	Medium	Yes	No

2.2. Motivations of the attacks on social media

Attackers, also known as hackers, carry out attacks on social media with wide range of motivations. These include revenge/emotions, financial gains, entertainment, hacktivism, espionage and cyber warfare.

- **Revenge/Emotions**
  Dissatisfied or displeased users or even an organization employee can attempt a cyber-attack on social media due to their anger, disagreement or any kind of revenge. These type of hackers aim to destroy the reputation of the victim organization by blocking their services and leaving the legitimate users disgruntled. Due to such kind of attacks victim organization may incur great financial loss.
- **Financial gains**
  This is the most important and common reason for attack on social media. Cyber criminals gain the sensitive information regarding the bank account of the users and maliciously access their account to acquire the financial gain. It may include stealing the business related information to gain the profit by another rival company.
- **Entertainment**
  Some hackers enjoy the thrilling experience of hacking on social media. They perform attack to gain recognition of their hacking abilities or notoriety among fellow hackers. They do it for their entertainment without expecting any financial or political gain. As some say, some men just want to watch the world burn.
- **Expertise for job**
  Most of the IT experts do not have cybersecurity and hacking background, thus there is a very high demand for expertise in these fields. The employment domain for these jobs is very fervent these days. Hiring hackers and cybersecurity specialists can help the organizations evaluate their security in a better way and tackle the cyber criminals easily, it is easy to beat a criminal if we have a person on our side, who can think and operate in the same way as him/her.
- **Hacktivism**
  Hacktivism is use of computers and computer networks to promote political ends, chiefly free speech, human rights and information ethics. This also includes the publishing aims and views of a political community or religion, to stage protests supporting their political/religious beliefs. It also includes vandalism of the various websites with political/religious messages.
- **Cyber espionage**
  This is also one of the important motivations that leads to the theft of confidential information on social media. It includes obtaining private information without permission of owner of the information from individuals, competitors, or even other country. These attacks are done with the help of various hacking techniques and malicious software.
- **Cyber warfare**
  These are politically motivated Internet-based attacks on information and information systems using social media. The target of these attacks mainly includes government websites to cripple down their communication, financial stability and many other things that mainly focus on improper functioning of the government of other country. It is basically a war that is fought by sitting inside the room, than going on the front.

2.3. Social media security and privacy

As a form of presentation and typical application of Web 2.0 technology, (mobile) social media has been constructed by the relations between users and bodies on the basis of modern (mobile) Internet technology and platform carriers. The original problems related to the confidentiality, completeness, and availability of Internet platforms still exist under social media platforms. With regard to new platforms, new scenes, and new applications of social media ecosystems, practical application problems have been derived that are related to security control mechanism, individual privacy protection, and digital copyright protection. For the access control problem of Online Social Networks (OSNs), Pang et al. [11] summarized and defined the new needs of OSN access control from the current access control schemes. This study focuses on the security of public information from the point of user adjustable resource access, proposed a new OSN model that includes users, the relations between users and public information, and described the major access control strategies with hybrid logic. What is more valuable is that they finally presented how to extend the proposed model and logic to cope with untrusted information and to realize collaborative access control in OSNs.

Ma et al. [12] indicated that the Pervasive Social Network (PSN) supports online/instant social activities and communications on the basis of heterogeneous networks and pervasive behaviors. Mobile users expect interaction with valuable information but face the distribution and sharing of unwanted and even malicious content, and the negative content of non-required information affects the practical and successful applications of PSN. Considering that current literature still lacks a robust and general malicious content control model, they proposed the design and realization of this model on the basis of trustworthiness management and PSN Controller. Under the circumstance of a large amount of invasion and attacks, they have further assessed the performance of the controller system, which is effective on essential aspects of accuracy, efficiency and robustness.

In earlier studies, Barbara et al. [13] pointed out that an enhanced access control system for social networks is the first step for addressing the security and privacy problems of online networking. In order to resolve the current limitations, they created an experimental and testable social network using synthetic data, which are used to test the efficacy of the previously proposed reasoning method based on semantics. And also, they proposed a scalable fine grain access control model for OSNs based on semantic web, and adopted OWL and SWRL for modeling. The model is involved with such main functions as authorization, management, and filtration. Related to the above work, Sachan et al. [14] proposed a fine grain multimedia access control model based on bit-vector transform domain under multimedia social networking. This model verified the security, as well as storage and execution efficiency by mathematics and analysis of simulation experiments.

With regard to the personal information disclosure and privacy protection of social media users, Fogues et al. [15] represented that given the explosive increase of users in the last few years, the current beneficial services of Social Networking Service (SNS), like Facebook and Twitter, are being overshadowed because of the existence of a privacy hazard while providing convenience and rich experiences to social users. Therefore, they listed all privacy hazards that may potentially affect the privacy threat of SNSs users, together with the requirements of privacy mechanism to realize the restraint of threats. They further described and analyzed the current solutions that can cover the range and degree of important needs. Viejo et al. [16] indicates that the big data released on social media platforms contains sensitive personal information that can be collected and utilized by external entities for profit. However, the current solutions mainly adopt strict access control means for protection, but do not support users to know which content are sensitive and confidential. Furthermore, current solutions require social media operators to participate to realize the control mechanism, therefore these solutions may not be practical. For this, they proposed a new idea to solve this appalling problem. This scheme can be applied to the privacy protection of current social media platforms by using a software component that is independent of platform. This solution can automatically test the sensitive data released by users to establish the privacy-clearing versions for data. Besides, it can read the security credentials provided by users to content release owners and only display a limited range of content and information to users, resulting to supporting transparent access to the sensitive content that need privacy protection. Finally, this solution has been successfully applied to two global social websites: Twitter and PatientsLikeMe.

As a typical application in the social media ecosystem, multimedia social networks (MSNs) mainly allow (mobile) users to interact with information at any time and any location to easily exchange, interact, and communicate multimedia content (images, photos, audio and video). However, given that the broad application of digitized content in the 1990s of the last century, the problem of Digital Rights Management (DRM) for multimedia content has already yield for long time. The major technical roadmap includes proactive methods for cryptography security protection, for instance encryption and decryption, provable cryptography protocols [17], as well as reactive approaches to forensics and copyright prosecution that can track and identify the digital content owner via digital watermarks and others [18]. However, with a variety of newly developed social media tools and a great number of MSNs community users, the DRM problem has become more and more prominent and complex. Only open DRM systems [19], proper limitation and customized DRM SaaS will stimulate the future DRM-related markets. To this end, more studies have been further conducted on multimedia content security and anti-piracy regarding the emerging MSNs.

We, at Multimedia Content Security Laboratory, have proposed the DRM utility analytics and adoption of security policies combination based on cooperation and non-cooperation game theory, plus DRM security risk assessment and soft computing method in a scenario of digital content sharing [20–23]. A mobile DRM solution for multimedia copyright under mobile social networking was proposed and realized for Android mobile terminals [24]. More recently, we have also designed a new delegation authorization mechanism on the basis of proxy re-encryption to completely solve the increasingly prominent problem of limitation and inefficacy of traditional access control list technology in the era of big data of social media [25].

Hossain et al. [26] try to predict where twitter users are when share their own experience or some others persons on drinking. They analyzed large population using their check-in locations throughout a day, and for result generation they used three layers of SVM (Support Vector Machines) which gives an F-score of 83%.

Davies et al. [27] examined the social media security with pervasive memory augmentation. They identified a number of threats to our data. Pervasive memory augmentation being a novel area for research provides various opportunities and applications in the field of social media security. Kang et al. [28] performed a study to gather information about user knowledge and their action against security risks. They concluded that there is no straight forward relationship between the technical knowledge of user to their ability to understand or mitigate attacks. However, they mentioned user's awareness is partly affected by experience and technical knowledge.

2.4. Social media security and user behavior

The never-ending security breaches over social media have entitled the organizations to safeguard the information that is shared over the network. Any violation to security hinders directly with economic growth of the organization. The social media can be analyzed by studying the behavior of its users, which might be an individual or group. The Internet users need to be well-informed about the threats that are faced by their personal and financial information. They should be able to behave securely and use reliable security measures at their aid. The behavior depends on their actual realization and their experience over the social media. For example, the users who are victims of identity theft or cyber bullying will have very different perspective of security and trust from those who have not [29].

Another factor that affects the users' perception is whether or not they consider and carefully go through the security notices and direction issued at various social networking sites. Although, now it seems that regular reports of privacy and security attacks on the news have made the users more considerate about their behavior. The business organizations are also making more efforts in protecting their consumers' private information because any harm will lead to loss of consumer trust.

In order to study social media trust and privacy formation is to investigate the perceived control from the users' point of view. Perceived control here can be defined as the users' realization of their own control over their information. It is considered to be an efficient tool for the prediction of user behavior, better than actual control. Gender also plays an important role in defining the perception vulnerabilities. The concept of perceived control stems from presumption that user has supremacy over the social network habitat. Perceived control can be: (i) behavioral, which refers to users' tendency to adapt according to circumstance; (ii) decisional, which refers to ability of the user to successfully obtain the desired outcome out of circumstances based on his/her actions and conclusion; (iii) cognitive, which notifies whether or not the user is able to understand the circumstances. We can also refer perceived control as the amount of control users assumes that he/she is having however, it is not actually there. Actual control however, is generally taken into consideration while performing hypothetical interpretations. It determines the degree of true hold that user possess over the network [30–32].

Perceived control is defined as an emissary of actual control. It plays a very prominent role in relieving the privacy and trust issues of the user. Hajli and Lin studied the role of perception control and risks on user behavior. They stated that the increase in the degree of perceived control affects the user behavior positively and leads to increased information sharing whereas any perceived privacy vulnerability have a negative effect on user behavior. Vladlena et al., analyzed user behavior over social media based on their attention to security notices and features. They stated that user who use social media more frequently are more likely to observe such notices. However, the users having previous experiences are less likely to observe these notices. Similarly, the victims of online fraud are more likely to pay attention to security notices [33–35] (see Fig. 4).

2.5. Social media trust and evaluations

When addressing social media security problems, the trustworthiness problem among social media users, content (service) providers, platform owners, and third-party supervisors is another concern and key factor of the stable existence and successful application of social media ecosystem. The problems of both security and trustworthiness are inseparably interconnected and have a range of overlap, and the security of social platforms can affect the trustworthiness considerations from stakeholders above mentioned. Building and strengthening trustworthiness will provide awareness and guarantee of safety to users.

Meo and Agreste et al. [36,37] indicate that social group formation and the dynamic characteristics of topology structure evolution should be understood, and those are in essence. However, in the process of user gathering and community formation, the trustworthiness relation between users is of vital importance. They proposed a measurable method for the degree of group compactness and considered the similarity and trustworthiness between users. Furthermore, they also proposed a novel algorithm to optimize the method. They provided an empirical research result based on real social networks, namely, Epinion, Ciao, and Prosper (a micro-lending site with implicit trust), by introducing centrality metrics to prove the advantage of this new method.

In addition, with regard to large-scale mobile social networking, users may belong to multiple communities or clusters, and overlapping users may play special roles in complex networks. Thereafter, the critical problem is how to assess or explain user trustworthiness. Under such a circumstance, trust inference plays an important role in the trusted social linkage between (mobile) users. To infer the fuzzy trust relation between users in the large-scale social networking of overlapping communities, Chen et al. [38] proposed an effective trust inference mechanism based on fuzzy community. This mechanism is called the Kappa-Fuzzy Trust. They, then proposed an algorithm to test the community structure of a complex network under fuzzy degree kappa, and created a fuzzy implicit social graph. Finally, they assessed the main functions of Kappa-Fuzzy Trust by simulation experiments.

As a killer application of social media and networking, recommendation systems based on social trust have been widely studied and applied. In this field, a personalized recommendation system can provide a good opportunity for the more efficient and wider interactions between the community members. The trust model based on user behavior has proved to be useful, and this kind of models generally use the interaction of a member with other members to calculate social trust value. However, Nepal et al. [39] indicate that these current models significantly neglect the interactions of those members with whom a member has interacted; this phenomenon is also named as the "friendship effect". The results of social research and behavioral science show that the behavior of community members has a significant effect on friends. Therefore, they described a trust communication model based on associations that combines individuals with the behavior of their friends, and focused on three key dependency factors in trust propagation: the density of interactions, the degree of separation, and the decay of friendship effect. The final goal of this model is to realize the accuracy of the recommendation system.

Recently, Wu et al. [40] developed a new social media recommendation framework GCCR for the reliable information source problem of social media recommendation. The current graph summarization, content-based method, clustering, and recommendation provide support to this framework. In addition, this framework divides users into small groups of different interest by developing a two-phase process by utilizing graph summarization and content-based clustering. This framework then uses the information of the interest groups for recommendation. Besides, Moradi et al. [41] also proposed the RTCF method to improve the accuracy of the trust recommendation system. This method provides a dynamic mechanism and constructs a user trust network on the basis of the proposed reliability method. Interestingly, Wang et al. [42] considered the context of the social environment of social media participants and the recommended target service and also proposed a context social networking model. This model considers the individual features of participants (e.g., the independent social environment, including hobbies and domain expertise) and mutual relations (e.g., the dependent social environment, including trust, social intimacy, and interactive conditions between two participants). Furthermore, they proposed a new probabilistic method called SocialTrust, which addresses the trust inference of social context awareness.

Being challenged by the trust issues faced by social media users, we first proposed a trust assessment model within and between the communities domains of multimedia social networking, conducted a simulation experiment of UCINET social networking, finally obtaining the change mode of trust strengthening and weakening of users in the sharing and communication of media content [43]. The proposed model combines the essential characteristics of MSNs small world feature and topological structure, and realized the potential path definition, inference and discovery of digital right communication between cross-community users in MSNs by using the binary-relation roughening method based on rough set. Second, on the basis of the discovered potential path, the proposed model measured the potential path trust by combining the trust assessment method to find the credible potential, i.e., the path within the pre-set trust threshold value. Finally, in order to verify the novel approach to trust path, we designed and realized the discovery algorithm for the potential path, the credible potential path. Our experiment was made by means of a social network simulation software UCINET and YouTube real data sets to construct a general virtual social communities in term of individual user-centric "150 Rule", so as to discover a complete and reliable potential path and to verify the efficacy and efficiency of the algorithm [44].

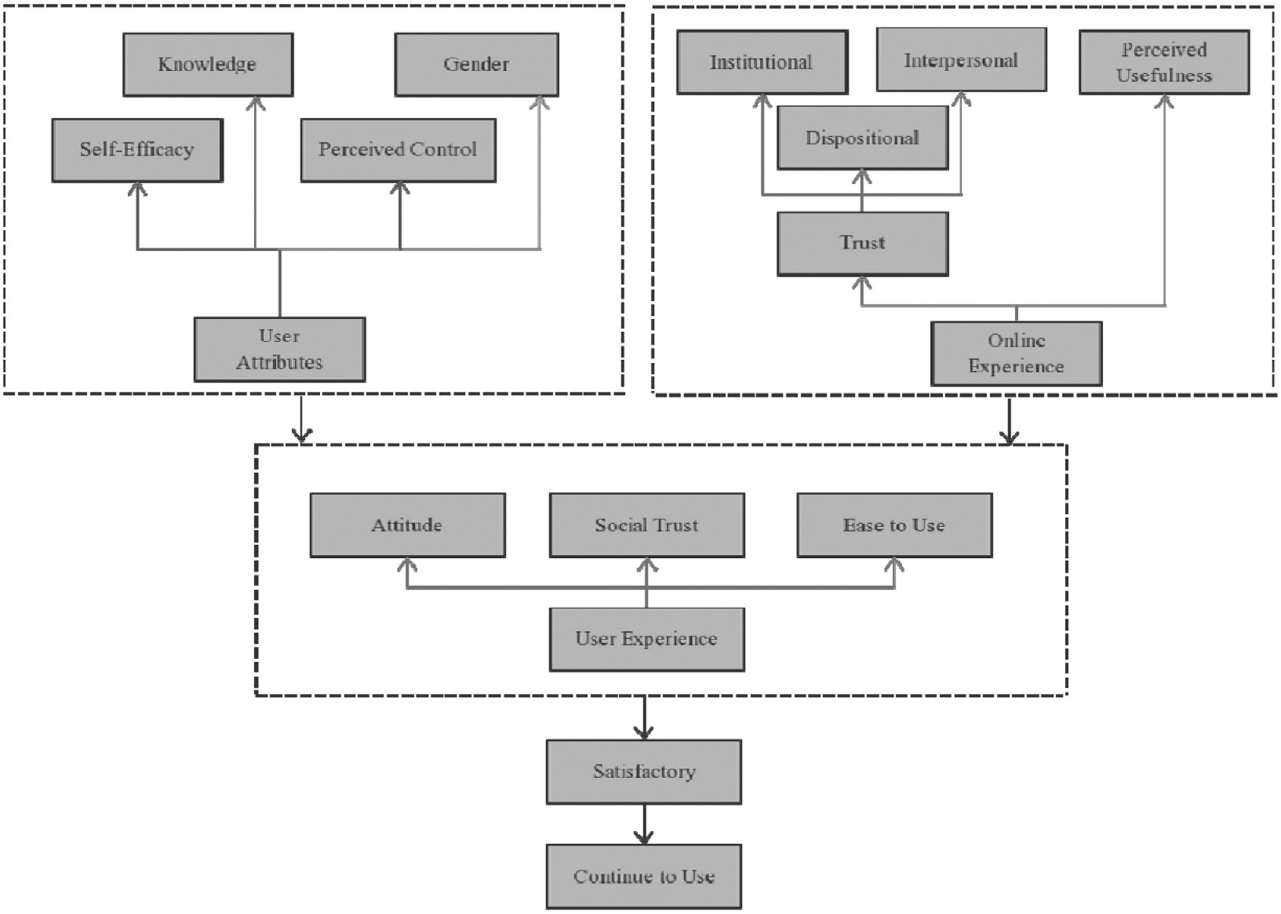

Fig. 4. Factors affecting user behavior on social media.

Wu et al. [45] presented a consensus based model for social networks. They estimated the trust score which was further used to calculate the preference values. To reach a consensus visual feedback process is used which is also able to give advice to the expert. Using the visual information, the experts can return to their evaluation of consensus can re perform it to achieve higher consensus. Lin et al. [46] highlighted the issues that are associated with trust over the social media. They determined that trust is affected by self-disclosure positively. Self-disclosure here refers to sharing personal details over social media to other who are able to comprehend the person sharing it. Uncertainty reduction affects self-disclosure positively.

Wu et al. [47] predicts the ranking to user information by exploiting information from multiple sources over the social media. The ranking was done with respect to user choice and trusted friends using Collaborative topic regression and probabilistic matrix factorization.

2.6. Social media intelligent applications and crowdsourcing

In recent years, the relighting of the artificial intelligence field and the emergence of crowdsourcing and crowd computing [48], and deep learning technology have not only stimulated and promoted the intelligent development direction and fast progress of social networking services, tools and applications, but also strengthened the analysis and computing in social media (content) recommendation, image analytics, and social video annotations.

In a recent study, Stantchev et al. [49] introduced a new collaborative learning service on the basis of cloud computing regarding the demand for online learning, which depends on advanced artificial intelligence mechanism and social network crowdsourcing to infer the knowledge and interest of users while considering the aggregated data from/to users of different social networks. Nepal et al. [1] proposed a novel social behavior model for two current major recommendation systems: user recommendation and content recommendation. These behavior-based recommendation methods have shown better performance than the standard friendship-based algorithms and link-prediction ones. Interestingly, Whitaker et al. [50] pointed out the new frontier direction of crowdsourcing, namely, the Extend Mind, and proposed the EMC concept. It indicates that people can extend their cognition to the environment by using smart phones and applications to express their mind activities. That is a new method of understanding and assessing human cognition embedded in data and devices for collective discoveries. This cutting-edge study is a cross-disciplinary and involved with the field of human computation, social computing and crowdsourcing.

Crowdsourcing refers to a method of solving big problems on the basis of how the crowd deals with sub-problems and sub-tasks. Mobile Crowdsourcing Network (MCN) has adopted the basic rules of crowdsourcing to execute user tasks supported by strong mobile equipment. This method is considered as a promising networking architecture in the future [51]. However, it also results into important security and privacy problems, which inhibit the applications of MCN. To cope with those challenge, Yu et al. made a detailed analysis and first proposed a generic architecture for a mobile crowdsourcing network involved with both crowdsourcing sensing and crowdsourcing computing.

Besides, there are the problems include data acquisition, management and analyses in crowdsourcing data. Ref. [52] is a valuable survey on data crowdsourcing. It not only provided the cases of problems that have been solved by the authors, but also presented the key design steps of executing the crowdsourcing scheme. And then, the study discussed some open problems that should be urgently solved, including data preparation and initialization, decomposition and aggregation, worker management, plus prior and external information. Finally, the article indicated that crowdsourcing, including the best computer data management and analytical technology with the powerful "natural intelligence", will become the valuable tool for increasing data quality and usefulness. With regard to the data collection and model generation of big data sets, Bongard et al. [53] introduced a new method of machine science to prove that non-domain experts can collectively formulate features and provide feature values such that they can predict the behavior results of interest. This method is realized by establishing an interactive questionnaire of users and online survey platform to help predict the result of a behavior and the related new problems possibly caused. Finally, the method conducts verification by generating experiments of two models: one model can predict users' power consumption per month, and the other model can analysis and predict users' body mass index.

Similarly interesting, Rudinac et al. [54] proposed an automatic image selection method to realize the selection of images that are suitable for visual effects. This method utilizes the essential factors such as image content, context, popularity, visual aesthetic appeal and sentiment analytics from comments relative to images, to conduct united analysis. And, they obtained a large amount of manually created visual summaries and hided criteria information of images from Amazon Mechanical Turk crowdsourcing platforms. Biel et al. [55] applied crowdsourcing technology to the annotation of individual and social features in online social videos or social media content.

Xu et al. [56] proposed the 5W (What, Where, When, Who, and Why) model to detect real time urban emergencies. The crowd sourcing target here are the social media users where information extracted and the emergency detection is done. Wang et al. [57] present a state-of-art to enable the understanding of crowdsourcing in ITS. Intelligent transport systems (ITS) is an application of crowdsourcing. The issues are identified by keyword co-occurrence and co-authorship. They also introduced geo spatial tagged data for real time traffic analysis. Simula et al. [58] studied business-to-business firm interaction methods using social media as their communication medium. The firms also interact with their consumers on the social media to generate feedback. They gave a model to integrate crowdsourcing with B2B interaction and the challenges faced in doing so.

Summarily speaking, existing studies on social media security mainly focus on the utilization of traditional security technologies, cryptography, and image processing to solve social media problems on security, privacy and anti-piracy. Besides, there are some intelligent applications of online social media platforms by the state-of-the-art of artificial intelligence techniques. However, existing studies have not explored how to evaluate and measure security and trustworthiness of social media fundamental platforms. With the rapid increase in active users of social media and networking, as well as the attendance of information (content) service providers to various social media services, social media platforms face severer security and trust problems. Both the trust between users and the trust between users and content service providers rely on the fundamental platforms. Therefore, there is a necessity of a new research on effective, measurable evaluation and measurement for trustworthiness and security of social media systems and applications, thus further improvement and evolution of social platforms would be possible and effective in the future.

3. A new direction of social media security and trustworthiness

The social media research still lacks sufficient quantitative and qualitative analysis of security and trustworthiness. They cannot deal well with the present security and privacy challenges. With regard to the fundamental and common features of the newly developed social media applications, this paper proposes a novel research direction, which is a measurable evaluation and measurement for trustworthiness and security of social fundamental platforms, by defining the availability, transparency, and quality assurance of platform as evidences-driven research. The study should focus on how to evaluate, measure, and increase (optimize) the trustworthiness and security to realize the goal of "constructing a trustworthy, security-preserving social media ecosystem". The research roadmap is illustrated by Fig. 5, and main research aspects are shown by Fig. 6.

In Fig. 5, we in detail represent a top-down research from evidence-driven signals of social media platform security and trustworthiness to the construction a trusted and security-persevering social media ecosystem. In the procedure, there are there main research areas (3rd Layer) and corresponding open issues (4th Layer) to finally realize model, algorithm and related experimental analyses and verifications (5th Layer) in the basis of the fundamental principles and key technologies including social media computing, crowd intelligence and crowdsourcing, multimedia communication security and trust, especially signaling theory rooted from the management science.

3.1. Crowd evaluation/measurement architecture

In the scenario of social media ecosystems, from the point of view of stakeholders, there are mainly involved with SMPO (Social Media Platform Owner), GU (General User), CISP (Content Information Services Provider), ISP, and SMM (Social Media Monitor). The paper proposed a multi-layer architecture for crowd evaluation and measurement based on signaling theory in economics and information management [59,60] and crowd computing, such as Featured Signals Layer, Evaluation/Measurement Layer and Enhancement/Optimization Layer, as well as two kinds of signals and their feedback loop. The multi-layer architecture is shown in Fig. 7, indicating the entities and their featured signal-based operation, as well as data flow between layers.

3.2. Three aspects of the hierarchical research

(1) **Expression of social media platform signaling and crowd computing framework**

This study could creatively introduce the signaling theory to crowd computing, as it is centered on the important features and common organizational modes of social media platform, and analyzes of social media platforms. Specifically, we would first generalizes three main aspects of featured signal sources, i. e, services availability, transparency and quality assurance. On the basis of that, those are further categorized into two kinds of static property and dynamic behavior signals. And then, there are ontology expression of static (dynamic) features, inheritance, generalization and aggregation to build the signals spectrum. We could utilize the crowd computing concept to study how to collect, analysis evaluate and measure those signals to construct a conceptual model and framework.

(2) **Crowd evaluation and modeling of social media platform trustworthiness**

In the evaluation procedure of trustworthiness of a social media platform, we can create and leverages the crowdsourcing marking method and empirical questionnaire to collect the static/dynamic

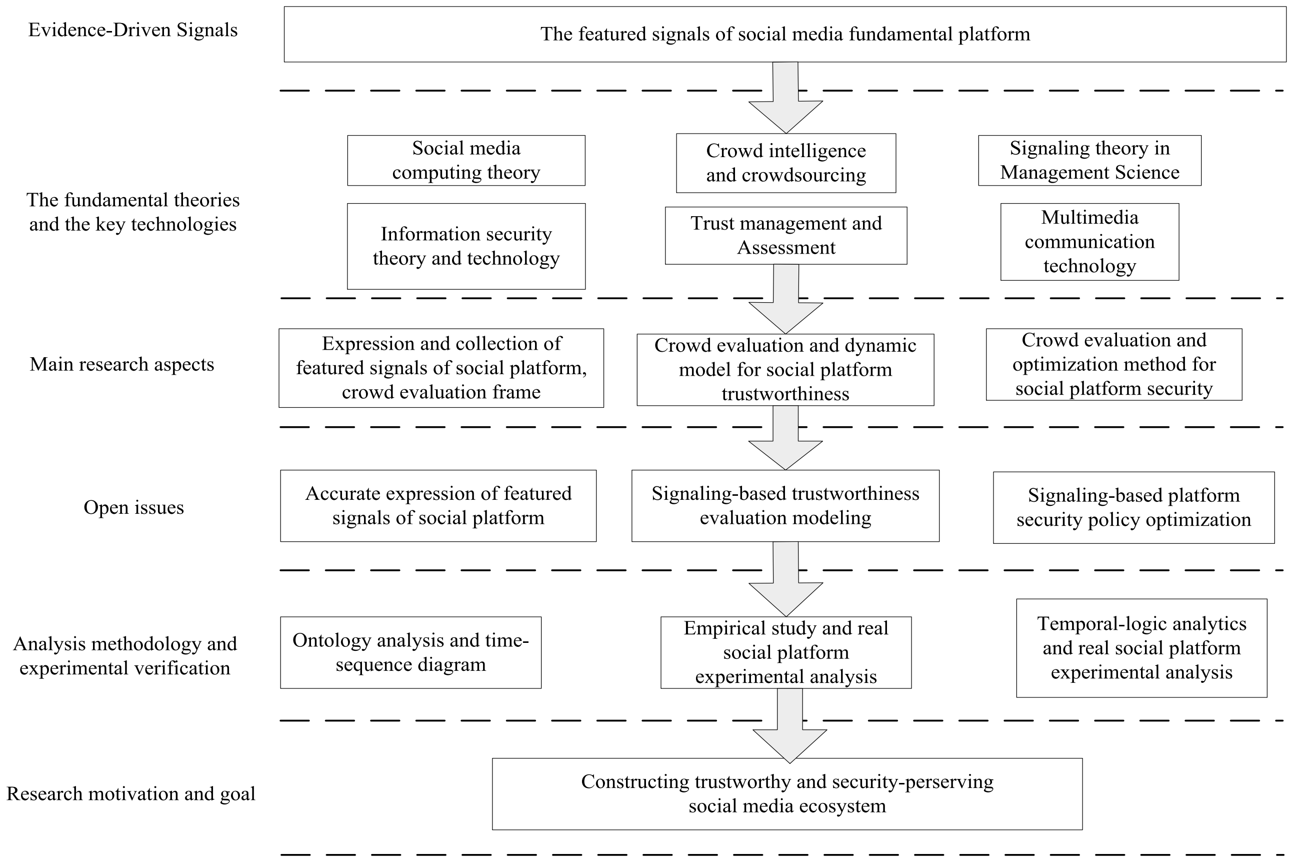
Evidence-Driven Signals
The featured signals of social media fundamental platform
The fundamental theories and the key technologies
Social media computing theory
Crowd intelligence and crowdsourcing
Signaling theory in Management Science
Information security theory and technology
Trust management and Assessment
Multimedia communication technology
Main research aspects
Expression and collection of featured signals of social platform, crowd evaluation frame
Crowd evaluation and dynamic model for social platform trustworthiness
Crowd evaluation and optimization method for social platform security
Open issues
Accurate expression of featured signals of social platform
Signaling-based trustworthiness evaluation modeling
Signaling-based platform security policy optimization
Analysis methodology and experimental verification
Ontology analysis and time-sequence diagram
Empirical study and real social platform experimental analysis
Temporal-logic analytics and real social platform experimental analysis
Research motivation and goal
Constructing trustworthy and security-perserving social media ecosystem

Fig. 5. The roadmap of the study on trustworthiness and security of social media.

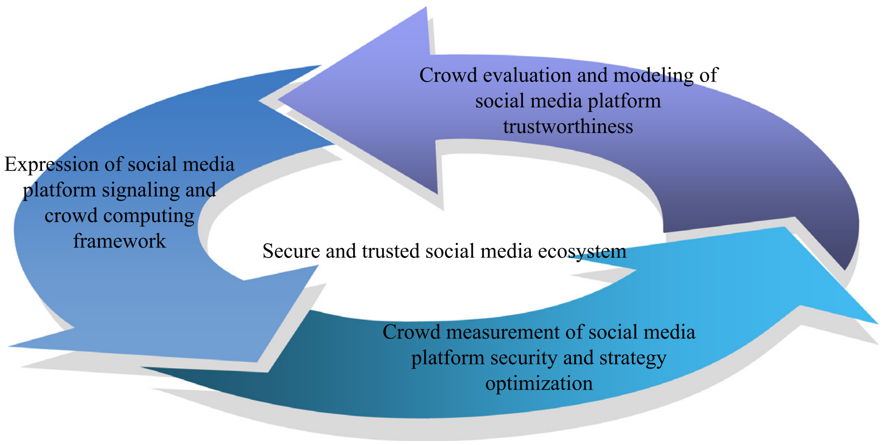
Crowd evaluation and modeling of social media platform trustworthiness
Expression of social media platform signaling and crowd computing framework
Secure and trusted social media ecosystem
Crowd measurement of social media platform security and strategy optimization

Fig. 6. Research motivation and surrounding main research aspects.

featured signals from three signal sources. And then, FAHP method could be adopted to compute the weight values of platform trustworthiness and security signals (including static and dynamic). In term of the values of key trustworthiness signals, this study need to further construct the trustworthiness evaluation mathematical model based on social platform version evolution. Combining with the case of CyVOD, a typical multimedia social media platform or others available, we analyze and compute the value of trustworthiness of real social media platforms in a scenario of multiple version migration. According to the evaluation results, a trustworthiness signal enhancement mechanism with a self-feedback is necessary to be established, in order to further improve and evolve social media platforms.

(3) **Crowd measurement of social media platform security and strategy optimization**

This layer study is the security of social media platform-centric, extracting key security signals according to the weight values of platform security signals (including static and dynamic) and adopting behavioral sequential logic to build the formal method and description of platform security rules. We can deploy the temporal logic reasoning and optimization methods to discover and address the potential implicit security rules' conflicts, and to optimize the parameters of the key signals in the security policy and finally establishing the optimized security strategy. By using CyVOD social media platform or others available, we can analyze and optimize the security signal parameters, and propose the self-enhancement security mechanism based on a feedback of the optimization results.

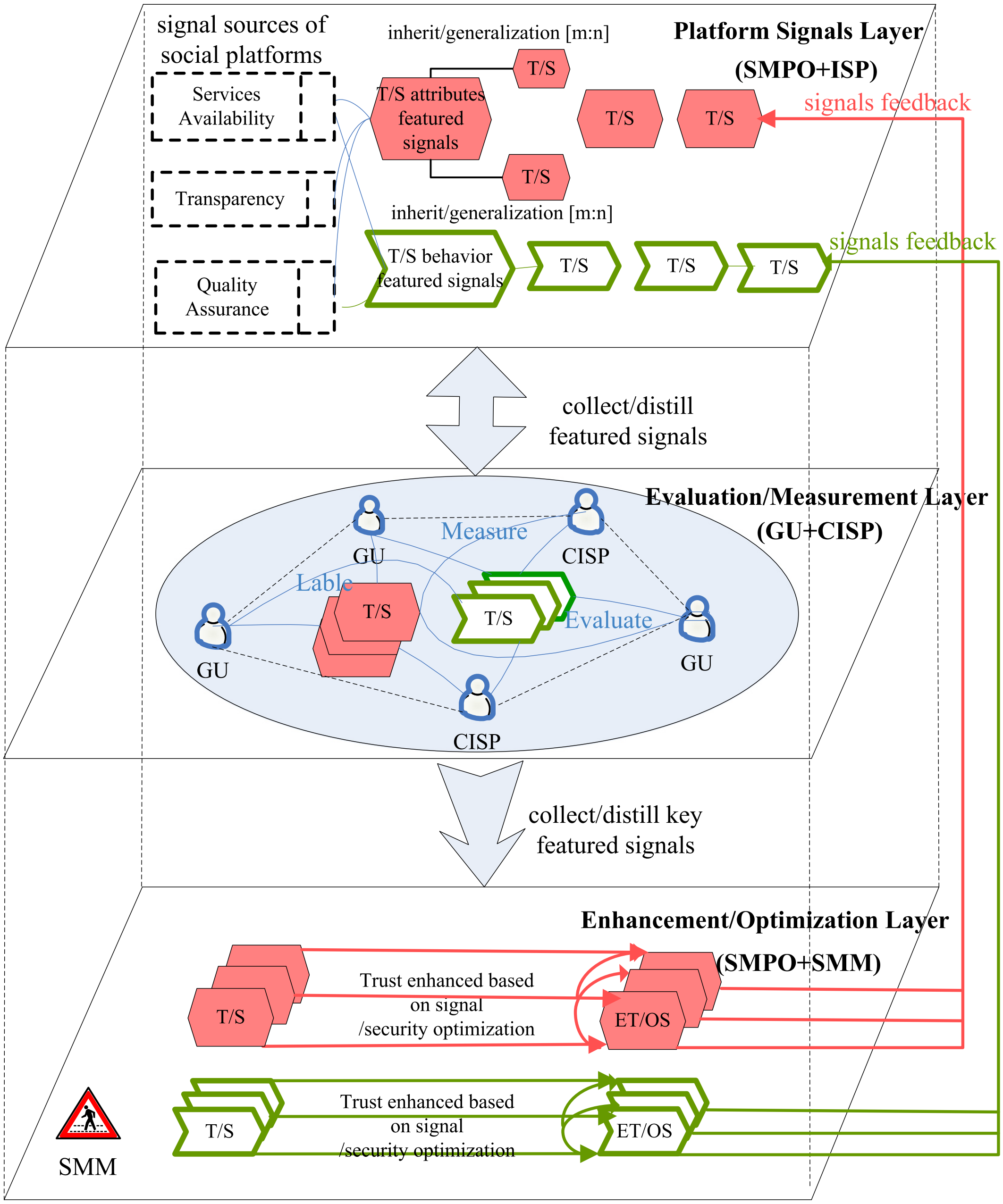
signal sources of social platforms
Services Availability
Transparency
Quality Assurance
inherit/generalization [m:n]
Platform Signals Layer (SMPO+ISP)
T/S attributes featured signals
T/S
T/S
T/S
T/S
signals feedback
inherit/generalization [m:n]
T/S behavior featured signals
T/S
T/S
T/S
signals feedback
collect/distill featured signals
Evaluation/Measurement Layer (GU+CISP)
GU
Measure
CISP
Lable
T/S
T/S
Evaluate
GU
GU
CISP
collect/distill key featured signals
Enhancement/Optimization Layer (SMPO+SMM)
Trust enhanced based on signal /security optimization
T/S
ET/OS
Trust enhanced based on signal /security optimization
T/S
ET/OS
SMM

Fig. 7. The framework of crow evaluation and measurement for trustworthiness and security of social media platform based on featured signals.

4. Major open issues and challenges

As of today, researchers and practitioners in the field of social media networks are still facing with various attacks from (or against) social network and social platforms [61], and endeavor to cope with those challenging security [62,63], privacy and measurement [64,65]. In light of three aspects of the hierarchical research above discussed, we mainly face the following several key open problems and challenges:

- Social media provides us the ability share our information with people all across the globe. But it gives the organizations that handle our information access control to our private information. People also use social media to spread fake news to cause chaos and fear among people. These issues need to address as user trust can only be gained by increasing the perceived user control and lowering such risks.
- As to the expression of social platform featured signals, it is an impassable step for further crowd evaluation and measurement because of the various, heterogeneous and dynamic features of social media platforms. We need to address how to correctly express the common features of the classified and extracted platform trustworthiness and security, particularly the construction of ontology formalism of platform behavioral features.
- To create the social platform trustworthiness evaluation model, we need first to find an effective method for constructing the complete dynamics (mathematical) model. This method should not only fully cover key factors of the platform key trustworthiness from the three featured signal sources of services availability, transparency and quality assurance of social platforms, but also consider the execution efficiency and computing complexity of the model.
- Social media users, including general users and information (content) service providers, have different needs of security

regarding different social media, time, location and scenario. The platforms themselves have fundamental and comparatively stable security and privacy protection requirements. Therefore, on the basis of the formalism of platform security crowd measurement and security rules' temporal logic, the optimization of social platform security policy has become an open problem for guaranteeing the fundamental social platform security and obtaining the generally optimized security policy that is common for two kinds of users. These objectives can be achieved by the conflict-free of security rules and by constructing the optimized method (model).

- The Real-time proxy based security solutions requires very quick software updating. Furthermore, the issue, an OSN user does not have any control on the information that other users expose about him, is yet not resolved.
- Most of the defensive techniques, we have studied which use encryption to protect user text form malicious users, however these techniques fail to achieve the image encryption properly.
- The security alertness should be improved among the OSN users by regularly providing recent news about OSN attacks, defensive solutions, responsibilities of user and prevention tools.
- The organizations that manage our personal and financial data, thus interaction between the organizations and the consumer is very important to ensure transparency and trust. Enabling the security notices and features easily accessible ensures liability and enhances public trust.

5. Conclusions

This paper mainly presents a survey on the state-of-the-art of social media security and trustworthiness, and then proposed a new direction on social media security and trustworthiness. The never-ending security breaches over social media have entitled the organizations to safeguard the information that is shared over the network. Any violation to security hinders directly with economic growth of the organization. The social media can be analyzed by studying the behavior of its' users, which might be an individual or group. The Internet users need to be well-informed about the threats that are faced by their personal and financial information. They should be able to behave securely and use reliable security measures at their aid. The direction is significantly theoretical meaningful for realizing secure interaction, sharing and digital rights management of social media content, continuously improving platform trust and security, as well as establishing trusted and security-preserving social media ecosystem. It has also better applicable vision and practical application value for healthy, normal and rapid development of digital media content industry. Building and strengthening trustworthiness will provide awareness and guarantee of safety to users.

Acknowledgments

We give thanks to the reviewers and editor for their valuable comments, questions, and suggestions. The work was sponsored by National Natural Science Foundation of China Grant No. 61370220, Program for Innovative Research Team (in Science and Technology) in University of Henan Province Grant No. 15IRTSTHN010, Training Foundation for Scientific Innovation Ability of Henan University of Science and Technology Grand No. 2013ZCX022, Program for Henan Province Science and Technology Grant No. 142102210425, Key Program for Basic Research of The Education Department of Henan Province Grant No. 13A520240 and No. 14A520048.

References

[1] S. Nepal, C. Paris, P.A. Pour, et al., Interaction-based recommendations for online communities, ACM Trans. Internet Technol. 15 (2) (2015) 1–21.
[2] H. Tobias, S. Michael, H. Matthias, et al. Quantification of youtube QoE via crowdsourcing, in: Proc. of 13th IEEE International Symposium on Multimedia, 2011, pp. 494–499. http://dx.doi.org/10.1109/ISM.2011.87.
[3] R. Yan, The rise of multimedia for online communication startups, IEEE Comput. Edge 2 (2) (2016) 50–54.
[4] Z.Y. Zhang, Security, trust and risk in multimedia social networks, Comput. J. 58 (4) (2015) 515–517.
[5] P. Mershon, Reasons to Rethink Your Blogging Strategy: New Research, 2011, Available at: http://www.socialmediaexaminer.com/7-reasons-to-rethink-your-blogging-strategy-new-research/ (Last accessed August 2016).
[6] X. Ruan, Z. Wu, H. Wang, Profiling online social behaviors for compromised account detection, IEEE Trans. Inf. Forensics Secur. 11 (1) (2016) 176–187.
[7] K. Pelechrinis, V. Zadorozhny, V. Kounev, et al., Automatic evaluation of information provider reliability and expertise, World Wide Web 18 (1) (2015) 33–72.
[8] C.Y. Chin, H.P. Lu, C.M. Wu, Facebook users' motivation for clicking the like button, Soc. Behav. Pers. 43 (4) (2015) 579–592.
[9] P. Joshi, C.C. Kuo, Security and privacy in online social networks: A survey, in: Proceedings of 2011 IEEE International Conference on Multimedia and Expo, ICME, Barcelona, Spain, 2011, pp. 1–6.
[10] L.A. Cutillo, M. Manulis, T. Strufe, Security and privacy in online social networks, in: Handbook of Social Network, Technologies and Applications, Springer, ISBN: 978-1-4419-7141-8, 2010, (Chapter book of).
[11] J. Pang, Y. Zhang, A new access control scheme for facebook-style social networks, Comput. Secur. 54 (44) (2015) 44–59.
[12] S. Ma, Z. Yan, PSNController: An unwanted content control system in pervasive social networking based on trust management, ACM Trans. Multimedia Comput. Commun. Appl. 12 (1s) (2015) 1–23.
[13] C. Barbara, F. Elena, H. Raymond, et al., Semantic web-based social network access control, Comput. Secur. 30 (2) (2011) 108–115.
[14] A. Sachan, S. Emmanuel, M. Kankanhalli, An efficient access control method for multimedia social networks, in: Proceedings of the 2nd ACM SIGMM Workshop on Social Media, Firenze, Italy, 2010, pp. 33–38.
[15] R. Fogues, J.M. Such, A. Espinosa, et al., Open challenges in relationship-based privacy mechanisms for social network services, Int. J. Hum.-Comput. Interact. 31 (5) (2015) 350–370.
[16] A. Viejo, D. Sánchez, Enforcing transparent access to private content in social networks by means of automatic sanitization, Expert Syst. Appl. 42 (23) (2015) 9366–9378.
[17] F. Koushanfar, Provably secure active IC metering techniques for piracy avoidance and digital rights management, IEEE Trans. Inf. Forensics Secur. 7 (1) (2012) 51–63.
[18] T. Thomas, S. Emmanuel, A.V. Subramanyam, et al., Joint watermarking scheme for multiparty multilevel DRM architecture, IEEE Trans. Inf. Forensics Secur. 4 (4) (2009) 758–767.
[19] V. Torres, C. Serrão, M.S. Dias, et al., Open DRM and the future of media, IEEE Multimedia 15 (2) (2008) 28–36.
[20] Z.Y. Zhang, Q.Q. Pei, J.F. Ma, et al. Cooperative and non-cooperative game-theoretic analyses of adoptions of security policies for DRM, in: Proc. of 5th IEEE International Workshop on Digital Rights Management Impact on Consumer Communications, Satellite Workshop of 6th IEEE Consumer Communications & Networking Conference, Las Vegas, Nevada, USA, 2009.
[21] Z.Y. Zhang, Q.Q. Pei, L. Yang, et al., Establishing multi-party trust architecture for DRM by using game-theoretic analysis of security policies, Chin. J. Electron. 18 (3) (2009) 519–524.
[22] Z.Y. Zhang, S.G. Lian, Q.Q. Pei, et al., Fuzzy risk assessments on security policies for digital rights management, Neural Netw. World 20 (3) (2010) 265–284.
[23] Z.Y. Zhang, Q.Q. Pei, L. Yang, et al., Game-theoretic analyses and simulations of adoptions of security policies for DRM in contents sharing scenario, Intell. Autom. Soft Comput. 17 (2) (2011) 191–203.
[24] 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.
[25] W.N. Feng, Z.Y. Zhang, J. Wang, et al., A novel authorization delegation for multimedia social networks by using proxy re-encryption, Multimedia Tools Appl. (2015) http://dx.doi.org/10.1007/s11042-015-2929-2.
[26] H. Nabil, T. Hu, R. Feizi, et al. Inferring fine-grained details on user activities and home location from social media: Detecting drinking-while-tweeting patterns in communities, 2016. ArXiv Preprint arXiv:1603.03181.
[27] N. Davies, A. Friday, S. Clinch, Security and privacy implications of pervasive memory augmentation, IEEE Pervasive Comput. 14 (1) (2015) 44–53.
[28] R. Kang, L. Dabbish, N. Fruchter, et al. My data just goes everywhere: User mental models of the Internet and implications for privacy and security, in: Eleventh Symposium On Usable Privacy and Security. 2015, pp. 39–52.
[29] B.G. Scott, C.F. Weems, Patterns of actual and perceived control: are control profiles differentially related to internalizing and externalizing problems in youth? Anxiety Stress Coping 23 (2010) 515–528.
[30] C.M. Hoadley, H. Xu, J.J. Lee, et al., Privacy as information access and illusory control: The case of the facebook news feed privacy outcry, Electron. Commer. Res. Appl. 9 (2010) 50–60.
[31] N. Hajli, A study of the impact of social media on consumers, Int. J. Mark. Res. 56 (2014) 95–113.

[32] J. Lee, Components of medical service users' dissatisfaction: A perceived control perspective, Int. J. Manag. Mark. Res. 5 (2012) 53–63.
[33] B. Vladlena, G. Saridakis, H. Tennakoon, et al., The role of security notices and online consumer behaviour: An empirical study of social networking users, Int. J. Hum. Comput. Stud. 80 (2015) 36–44.
[34] N. Hajli, X. Lin, Exploring the security of information sharing on social networking sites: The role of perceived control of information, J. Bus. Ethics 133 (1) (2016) 111–123.
[35] N. Mohamed, I.H. Ahmad, Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia, Comput. Hum. Behav. 28 (6) (2012) 2366–2375.
[36] P.D. Meo, E. Ferrara, D. Rosaci, et al., Trust and compactness in social network groups, IEEE Trans. Cybern. 45 (2) (2015) 205–216.
[37] S. Agreste, P.D. Meo, E. Ferrara, et al., Trust networks topology, dynamics, and measurements, IEEE Internet Comput. 19 (6) (2015) 26–35.
[38] S.H. Chen, G.J. Wang, W.J. Jia, Kappa-fuzzytrust: Efficient trust computation for large-scale mobile social networks using a fuzzy implicit social graph, Inform. Sci. 318 (2015) 123–143.
[39] S. Nepal, S.K. Bista, C. Paris, Behavior-based propagation of trust in social networks with restricted and anonymous participation, Comput. Intelligence 31 (4) (2015) 642–668.
[40] J. Wu, L. Chen, Q. Yu, et al., Trust-aware media recommendation in heterogeneous social networks, World Wide Web 18 (1) (2015) 139–157.
[41] P. Moradi, S. Ahmadian, A reliability-based recommendation method to improve trust-aware recommender systems, Expert Syst. Appl. 42 (21) (2015) 7386–7398.
[42] Y. Wang, L. Li, G.F. Liu, Social context-aware trust inference for trust enhancement in social network based recommendations on service providers, World Wide Web 18 (1) (2015) 159–184.
[43] Z.Y. Zhang, K.L. Wang, A trust model for multimedia social networks, Soc. Netw. Anal. Min. 3 (4) (2013) 969–979.
[44] Z.Y. Zhang, K.L. Wang, A formal analytic approach to credible potential path and mining algorithms for multimedia social networks, Comput. J. 58 (4) (2015) 668–678.
[45] J. Wu, F. Chiclana, E. Herrera-Viedma, Trust based consensus model for social network in an incomplete linguistic information context, Appl. Soft Comput. 35 (2015) 827–839.
[46] W. Lin, X. Zhang, H. Song, et al., Health information seeking in the Web 2.0 age: Trust in social media, uncertainty reduction, and self-disclosure, Comput. Hum. Behav. 56 (2016) 289–294. http://dx.doi.org/10.1016/j.chb.2015.11.055.
[47] H. Wu, K. Yue, Y. Pei, et al., Collaborative topic regression with social trust ensemble for recommendation in social media systems, Knowl.-Based Syst. 97 (2016) 111–122.
[48] T. Milo, Enlisting the power of the crowd, Commun. ACM 59 (1) (2016) 117.
[49] V. Stantchev, L. Prieto-G, Tamm G., Cloud computing service for knowledge assessment and studies recommendation in crowdsourcing and collaborative learning environments based on social network analysis, Comput. Hum. Behav. 51 (2015) 762–770.
[50] R.M. Whitaker, M. Chorley, S.M. Allen, New frontiers for crowdsourcing: the extended mind, in: Proc. of 2015 48th Hawaii International Conference on System Sciences, Jan 5-8, Grand Hyatt, HI, USA, 2015, pp. 1–10.
[51] K. Yang, K. Zhang, J. Ren, et al., Security and privacy in mobile crowdsourcing networks: Challenges and opportunities, IEEE Commun. Mag. 8 (2015) 75–81.
[52] H. Garcia-Molina, M. Joglekar, A. Marcus, et al., Challenges in data crowdsourcing, IEEE Trans. Knowl. Data Eng. (2015) http://dx.doi.org/10.1109/TKDE.2016.2518669.
[53] J.C. Bongard, P.D.-H. Hines, D. Conger, et al., Crowdsourcing predictors of behavioral outcomes, IEEE Trans. Syst. Man Cybern.-Syst. 43 (1) (2013) 176–185.
[54] S. Rudinac, M. Larson, A. Hanjalic, Learning crowdsourced user preferences for visual summarization of image collection, IEEE Trans. Multimedia 15 (6) (2013) 1231–1243.
[55] J.I. Biel, D. Gatica-Perez, Mining crowdsourced first impressions in online social video, IEEE Trans. Multimedia 16 (7) (2014) 2016–2074.
[56] Z. Xu, Y. Liu, N. Yen, et al., Crowdsourcing based description of urban emergency events using social media big data, IEEE Trans. Cloud Comput. 99 (2016) 1.
[57] X. Wang, X. Zheng, Q. Zhang, et al., Crowdsourcing in ITS: The state of the work and the networking, IEEE Trans. Intell. Transp. Syst. 17 (6) (2016) 1596–1605.
[58] H. Simula, A. Töllinen, H. Karjaluoto, Facilitating innovations and value cocreation in industrial B2B firms by combining digital marketing, social media and crowdsourcing, in: Proceedings of the 23th ISPIM Conference. Barcelona, 2012.
[59] T. Mavlanova, R. Benbunan-Fich, M. Koufaris, Signaling theory and information asymmetry in online commerce, Inf. Manage. 49 (2012) 240–247.
[60] B.L. Connelly, S.T. Certo, R.D. Ireland, et al., Signaling theory: A review and assessment, J. Manage. (2011) http://dx.doi.org/10.1177/0149206310388419.
[61] G. NaliniPriya, M. Asswini, A survey on vulnerable attacks in online social networks, in: Proceedings of 2015 International Conference on Innovation Information in Computing Technologies, ICIICT, 2015, pp. 1–6.
[62] M. Guerar, M. Migliardi, A. Merlo, et al., Using screen brightness to improve security in mobile social network access, IEEE Trans. Dependable Secure Comput. (99) (2016) 1545–5971.
[63] Z. Dhouioui, A.A. Ali, J. Akaichi, Social networks security policies, in: Proceedings of 9th KES International Conference on Intelligent Interactive Multimedia Systems and Services, Canary Islands, Spain, 2016, pp. 395–403.
[64] M. Sarkar, S. Banerjee, Exploring social network privacy measurement using fuzzy vector commitment, Intell. Decis. Technol. 10 (3) (2016) 285–297.
[65] S. Alduaij, Z. Chen, A. Gangopadhyay, Using crowd sourcing to analyze consumers' response to privacy policies of online social network and financial institutions at micro level, Int. J. Inf. Secur. Privacy 10 (2) (2016) 41–63.

Zhiyong 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, Cybernetics 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.

Brij B. Gupta received Ph.D. degree from Indian Institute of Technology Roorkee, India in the area of Information and Cybersecurity. In 2009, he was selected for Canadian Commonwealth Scholarship and awarded by Government of Canada Award ($10,000). He spent more than six months in University of Saskatchewan (UofS), Canada to complete a portion of his research work. He has published more than 80 research papers (including 02 book and 14 chapters) in International Journals and Conferences of high repute including IEEE, Elsevier, ACM, Springer, Wiley Inderscience, etc. He has visited several countries, i.e. Canada, Japan, China, Malaysia, Hong-Kong, etc. to present his research work. His biography was selected and publishes in the 30th Edition of Marquis Who's Who in the World, 2012. He is also serving as guest editor of various Journals. He was also visiting researcher with Yamaguchi University, Japan in 2015 and with Guangzhou University, China in 2016, respectively. At present, Dr. Gupta is working as Assistant Professor in the Department of Computer Engineering, National Institute of Technology Kurukshetra, India. His research interest includes Information security, Cybersecurity, Mobile/Smartphone, Cloud Computing, Web security, Intrusion detection, Computer networks and Phishing.