Future Generation Computer Systems 86 (2018) 851–854

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Editorial

Recent research in computational intelligence paradigms into security and privacy for online social networks (OSNs)

B.B. Gupta [a], A.K. Sangaiah [b], Nadia Nedjah [c], Shingo Yamaguchi [d], Zhiyong Zhang [e], Michael Sheng [f]

[a] National Institute of Technology Kurukshetra, India
[b] VIT University, Vellore, India
[c] State University of Rio de Janeiro, Brazil
[d] Yamaguchi University, Japan
[e] Henan University of Science & Technology, China
[f] University of Adelaide, Adelaide, Australia

A B S T R A C T

Today, with the fast changing technology and life-style, online social networks (OSNs) play an important role in everybody's life. Online social networking has made a drastic change in the way we pursue our social life. At the same time, various security problems like fake profiles, online impersonation, socialbots, clickjacking, identity clone attacks, publish spam messages, etc have also grown. Moreover, the concept of applying a computational intelligence (CI) approaches in social network analysis is feasible and sound. Therefore, the papers of this special issue address variety of security and privacy issues in online social networks including, social network modelling and security issues, information revelation and privacy, mining and analyzing social data, social networking data analysis tools and services and security of other aspects of online social networks.

© 2018 Published by Elsevier B.V.

1. Introduction

In recent years, the use of online social networks (OSNs) is growing rapidly. Some online social networks (Linkdn, Facebook, Twitter, MySpace, Google+, Sina Weibo, VKontakte, Mixi, etc.) are becoming very famous and considered as one the preferred way of communication for many people [1–3]. The significance of these websites comes from the fact that the users spend high amount of time to up-to-date their information, interact with other users and surf other member's profile. OSN can be very beneficial for the users because it eliminates the geographical and economical borders. In addition, OSN can be utilized for achieving the targeted goals such as educational, entertainment, job searching, etc. In nutshell, we can say that the popularity of OSN Websites has grown enormously and playing a significant role among the Internet community [4–7]. However despite its benefits, in recent years, security and privacy concerns with online social networks (OSNs) have becoming a key research area. Accordingly to Sophos security threat report, threats affected to the Facebook are more as comparison to the other social networking websites. Likewise, Twitter and LinkedIn is the next target of the attacker [8]. Similarly, according to Nexgate's report [9], approximate 355% escalation of spam on social media websites were observed during the first half of 2013. The concept of applying a computational intelligence (CI) approaches in social network analysisis feasible and sound. Moreover, CI and its associated learning paradigms play vital characteristics in huge number of application areas related to security and privacy in information systems. CI paradigm consists of various branches that are not limited to expert systems, artificial immune system, swarm intelligence, fuzzy system, neural network, evolutionary computing and various hybrid systems, which are combinations of two or more of the branches.

These considerations have led to this special issue and security solutions from CI perspective have evolved to detect and prevent attacks, and are also able to perform forensic analysis that have significantly complicated user authentication, access control and system security. Specifically, this special issue addresses various security and privacy aspects from CI perspective, with a focus on simulations of social networks, representation, applications/tools and analysis of social networks, particularly on advances computing technologies and related areas [10–12]. Papers were invited for this special issue considering aspects of this problem, including:

- Social networking security and privacy concepts and applications
- Social network modelling and security issues
- Information revelation and privacy in online social networks
- Social networking data analysis tools and services
- Machine learning to gain novel insights on social network security analysis

E-mail address: bbgupta@nitkkr.ac.in (B.B. Gupta).

https://doi.org/10.1016/j.future.2018.05.017
0167-739X/© 2018 Published by Elsevier B.V.

- Evolutionary algorithms for learning the behaviour and privacy analysis in social networks
- Evolutionary algorithms for mining social networks for decision support
- Mining and analyzing social data for decision support & optimization
- Optimization of dynamic processes in social networks
- Computational Intelligence Solutions to security and privacy issues in mobile social networking
- Large-scale graph algorithms for social network analysis
- Chaos theory and chaotic systems for social media content security
- Soft computing technologies for both quantitative and qualitative security assessment and privacy management in online social networks
- Artificial neural network and neural system applied to social media and mitigating the privacy risks of social networking

This special issue contains nine papers which were selected after rigorous review process to deal with different aspects of security and privacy issues in online social networks and other related areas [13–15].

2. Contributions

The first article entitled, "Collaborative analysis model for trending images on social networks" authored by M Shamim Hossain, et al. presents a collaborative analysis model to identify if any trending image is altered or modified, and whether the content used to describe it is actually accurate [16]. It is a challenge to provide the desired trending media content in a short time from the vast amount of trending images on the social networks. Online social network environment is heterogeneous in nature, which demands computational Intelligent (CI) techniques to deliver the required media content in an acceptable time to the users. To this end, a collaborative search algorithm is used to utilize the descriptive tags, and user interaction history. The collaboration of tags powers the investigation of a trending images. Accordingly, authors demonstrate the potential of the proposed model by performing experiments on the online collected data set using a proposed collaborative analysis model.

The second paper entitled, "CenLocShare: A centralized privacy-preserving location-sharing system for mobile online social networks", authored by Xi Xiao, et al. presents a centralized privacy-preserving location-sharing system, named CenLocShare [17]. It integrates SNS and LBS into one server, i.e., Location-storing Social Network Server (LSSNS), and uses the dummy locations and the dedicated mapping protocols between LSSNS and Cellular Tower (CT) to share privacy-preserving locations. Its safety is validated by the security analysis. Furthermore, authors implemented the prototype of CenLocShare and do some comparisons with other systems. The thorough experiments indicate that the proposed system decreases the query time for friends' locations and the storage space. CenLocShare is more suitable and effective in the context of mOSNs.

The third paper entitled, "Attribute-based handshake protocol for mobile healthcare social networks" authored by Yi Liu, et al. presents a comprehensive study of the privacy protection problem of handshake protocol for mobile healthcare social network, and introduces the concept of attribute-based handshake (ABH) protocol [18]. Using ABH, users in mobile healthcare social network can make a handshake to authenticate each other and obtain a common session key without exposing their privacy when their attributes meet the social needs of each other. Then, authors provide the formal definition and security model of ABH protocol with a specific construction proving its security in the standard model. Finally, authors introduce how to deploy proposed ABH protocol in the mobile healthcare social network.

The fourth paper entitled, "Enhancing privacy through uniform grid and caching in location-based services" is authored by Shaobo Zhang, et al. [19]. In this paper, authors propose a solution designed to enhance location privacy in LBSs. Proposed scheme is based on the uniform grid, and adopts both order-preserving symmetric encryption (OPSE) and k-anonymity technique. Thus, the anonymizer knows nothing about a user's real location, and it can only implement simple matching and comparison operations. In the proposed approach, authors also employ an entity (hereafter referred to as the converter) to transform the user-defined grid structure into the uniform grid structure. This combined with the caching mechanism, allow to avoid repeated queries from different users on the same query spatial region and consequently, reduce the overhead of the LBS server. The analysis and simulation results demonstrate that proposed approach can effectively preserve a user's location privacy, with reduced overheads at the anonymizer and the LBS server.

The fifth paper entitled, "Social networking data analysis tools & challenges" authored by A. Sapountzi, et al. presents a sophisticated classification of state-of the-art frameworks for social data networking analysis considering the diversity of practices, methods and techniques [20]. Authors claim that this is the first attempt that illustrated the entire spectrum of social data networking analysis and their associated frameworks. The survey demonstrates challenges and future directions with a focus on text mining and the promising avenue of computational intelligence.

The sixth paper entitled, "Social media security and trustworthiness: overview and new direction" authored by Zhiyong Zhang, et al. presents a comprehensive 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. Furthermore, authors highlighted a new direction on evaluating and measuring those fundamental and underlying platforms [21]. Moreover, authors proposed a hierarchical architecture for crowd evaluations based on signaling theory and crowd computing, which is essential for social media ecosystem. Finally, authors conclude the paper with several open issues and cutting-edge challenges.

The seventh paper entitled, "Multiple watermarking technique for securing online social network contents using back propagation neural network" authored by A. Singh, et al. proposes a robust and secure DWT, DCT and SVD based multiple watermarking techniques for protecting digital contents over unsecure social networks [22]. The proposed technique initially decomposes the host image into third level DWT where the vertical frequency band (LH2) at second level and low frequency band (LL3) at the third level DWT is selected for embedding image and text watermark respectively. Further, the proposed method addresses the issue of ownership identity authentication, multiple watermarks are embedded instead of single watermark into the same multimedia objects simultaneously, which offer the extra level of security and reduced storage and bandwidth requirements in the important applications areas such as E-health, secure multimedia contents on online social network, secured E-Voting systems, digital cinema, education and insurance companies, driver's license/passport. Further, to enhance the security of the host and watermarks, the selective encryption is applied on watermarked image, where only the important multimedia data is encrypted. The proposed method has been extensively tested and analyzed against known attacks. Finally, authors have evaluated the image quality of the watermarked image by subjective method.

The eighth paper entitled, "Experimental and quantitative analysis of server power model for Cloud data centers" authored by Wei-Wei Lin, et al. presents an I/O-mode aware disk power model

based on the observation of disk power behavior [23]. Experimentally, authors first analyze the accuracy of different CPU power models by looking into a SPECpower_ssj2008 dataset. Furthermore, authors also carried out experiments on a physical server to evaluate memory power models and disk power models. The experimental results indicate the advantage of polynomial CPU model, LLCM-based memory model and the proposed disk model. The ideology of component-level power modeling presented in this paper helps realize fine-grained power control. Moreover, the evaluation and comparison results provide CSPs with useful guidance on optimizing energy management of cloud data centers.

The ninth paper entitled, "Image steganography using uncorrelated color space and its application for security of visual contents in online social networks" authored by K. Muhammad, et al. proposes an adaptive LSB substitution method using uncorrelated color space, increasing the property of imperceptibility results in minimizing the chances of detection by the human vision system [24]. In the proposed scheme, the input image is passed through an image scrambler, resulting in an encrypted image, preserving the privacy of image contents, and then converted to HSV color space. The secret contents are encrypted using an iterative magic matrix encryption algorithm (IMMEA) for better security, producing the cipher contents. An adaptive LSB substitution method is then used to embed the encrypted data inside the Vplane of HSV color model based on secret key-directed block magic LSB mechanism. Morever, the quantitative and qualitative experimental results of the proposed framework and its application for addressing the security and privacy of visual contents in online social networks (OSNs), confirm its effectiveness in contrast to state-of-the-art methods.

And, finally, this editorial would not be complete without brief mention of some other papers [25–28] related to this special edition which have been published as regular papers. In [25], authors presented a prediction system of Sybil attack in social network using deep-regression model. Moreover, in [26], authors proposed a privacy-preserving multi-hop profile-matching protocol for proximity mobile social networks. An approach for anonymizing popularity in online social networks with full utility is presented in [27]. An approach for flexible data access control in D2D communications is presented in [28]. Similarly, authors presented privacy-protected statistics publication over social media user trajectory streams in [29].

3. Conclusion

This special issue presented some selected papers in touching important aspects of security and privacy issues in online social networks including, social network modelling and security issues, information revelation and privacy, mining and analyzing social data, social networking data analysis tools and services and security of other aspects of online social networks and also emphasizes many open questions. Moreover, the wide spread use and importance of OSNs encourage various researchers to look at different security and privacy issues which need to be addressed urgently by developing efficient defense solutions and a lot more work need to be done before it is widely accepted by the user community. We hope the papers covered in this special issue will provide relevant insights into the emerging trends in Computational Intelligence paradigms into Security and Privacy for online social networks (OSNs).

Acknowledgment

We would like to express our special thanks to Prof. Peter Sloot, the Editor-in-Chief of Future Generation Computer Systems, for his great support and efforts throughout the whole publication process of this special issue. Moreover, this special issue is due to the encouragement of Ms. Hilda Xu, who is instrumental in the organization process, and to the Elsevier Journal Editorial Office for their continuous support to publish this special issue. Many individuals have contributed toward the success of this issue. Special thanks are due to dedicated reviewers who found time from their busy schedule to review the articles submitted in this special issue. In addition, we are also grateful to all the authors for submitting and improving their papers.

References

[1] Muhammad Al-Qurishi, Sk Md Mizanur Rahman, M. Shamim Hossain, Ahmad Almogren, Majed Alrubaian, Atif Alamri, Mabrook Al-Rakhami, B.B. Gupta, An efficient key agreement protocol for Sybil-precaution in online social networks, Future Gener. Comput. Syst. (2017). http://dx.doi.org/10.1016/j.future.2017.07.055.

[2] L.A. Cutillo, R. Molva, T. Strufe, Safebook: A privacy-preserving online social network leveraging on real-life trust, IEEE Commun. Mag. 47 (12) (2009).

[3] P. Chaudhary, B.B. Gupta, S. Yamaguchi, XSS detection with automatic view isolation on online social network, in: 2016 IEEE 5th Global Conference on Consumer Electronics, Kyoto, 2016, pp. 1–5. http://dx.doi.org/10.1109/GCCE.2016.7800354.

[4] B.B. Gupta, D.P. Agrawal, Shingo Yamaguchi, Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, IGI Global, 2016, p. 589.

[5] P. Chaudhary, B.B. Gupta, A novel framework to alleviate dissemination of XSS worms in online social network (OSN) using view segregation, Neural Netw. World 27 (1) (2017) 5–25.

[6] Mouna Jouini, et al., A security framework for secure cloud computing environments, Int. J. Cloud Appl. Comput. (IJCAC) 6 (3) (2016) 32–44.

[7] M. Al-Ayyoub, A. Rabab'ah, Y. Jararweh, M.N. Al-Kabi, B.B. Gupta, Studying the controversy in online crowds' interactions, Appl. Soft Comput. (2017).

[8] Sophos: Two third of business fear that social networking endangers corporate security, Sophos research reveals, 2009. Available at: http://www.sophos.com/en-us/press-office-releasees/2009/04-nnetworking.aspx.

[9] Nexgate (2013) State of social media spam. Available at: http://nexgate.com/wp-content/uploads/2013/09/Nexgate-2013-State-of-Social-Media-Spam-Research-Report.pdf.

[10] Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, B. Gupta, Secure integration of IoT and cloud computing, Future Gener. Comput. Syst. (2016). http://dx.doi.org/10.1016/j.future.2016.11.031.

[11] Zhiyong Zhang, et al., CyVOD: A novel trinity multimedia social network scheme, Multimedia Tools Appl. 76 (18) (2017) 18513–18529.

[12] Mamdouh Alenezi, et al., Evolution impact on architecture stability in open-source projects, Int. J. Cloud Appl. Comput. (IJCAC) 5 (4) (2015) 24–35.

[13] Long Jin, et al., Understanding user behavior in online social networks: A survey, IEEE Commun. Mag. 51 (9) (2013) 144–150.

[14] Michael Fire, Roy Goldschmidt, Yuval Elovici, Online social networks: Threats and solutions, IEEE Commun. Surveys Tutor. 16 (4) (2014) 2019–2036.

[15] Kaihe Xu, et al., My privacy my decision: Control of photo sharing on online social networks, IEEE Trans. Dependable Secure Comput. 14 (2) (2017) 199–210.

[16] M. Shamim Hossain, Mohammed F. Alhamid, Ghulam Muhammad, Collaborative analysis model for trending images on social networks, Future Gener. Comput. Syst. 86 (2018) 855–862.

[17] Xi Xiao, et al., CenLocShare: A centralized privacy-preserving location-sharing system for mobile online social networks, Future Gener. Comput. Syst. 86 (2018) 863–872.

[18] Yi Liu, et al., Attribute-based handshake protocol for mobile healthcare social networks, Future Gener. Comput. Syst. 86 (2018) 873–880.

[19] Shaobo Zhang, et al., Enhancing privacy through uniform grid and caching in location-based services, Future Gener. Comput. Syst. 86 (2018) 881–892.

[20] Androniki Sapountzi, Kostas E. Psannis, Social networking data analysis tools & challenges, Future Gener. Comput. Syst. 86 (2018) 893–913.

[21] Zhiyong Zhang, Brij B. Gupta, Social media security and trustworthiness: Overview and new direction, Future Gener. Comput. Syst. 86 (2018) 914–925.

[22] Amit Kumar Singh, et al., Multiple watermarking technique for securing online social network contents using back propagation neural network, Future Gener. Comput. Syst. 86 (2018) 926–939.

[23] Weiwei Lin, et al., Experimental and quantitative analysis of server power model for cloud data centers, Future Gener. Comput. Syst. 86 (2018) 940–950.

[24] Khan Muhammad, et al., Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Gener. Comput. Syst. 86 (2018) 951–960.

[25] Muhammad Al-Qurishi, et al., A prediction system of sybil attack in social network using deep-regression model, Future Gener. Comput. Syst. (2017). http://dx.doi.org/10.1016/j.future.2017.08.030.

[26] Entao Luo, et al., Privacy-preserving multi-hop profile-matching protocol for proximity mobile social networks, Future Gener. Comput. Syst. 68 (2017) 222–233. http://dx.doi.org/10.1016/j.future.2016.09.013.
[27] Shiwen Zhang, Qin Liu, Yaping Lin, Anonymizing popularity in online social networks with full utility, Future Gener. Comput. Syst. 72 (2017) 227–238. http://dx.doi.org/10.1016/j.future.2016.05.007.
[28] Zheng Yan, et al., Flexible data access control in D2D communications, Future Gener. Comput. Syst. (2017). http://dx.doi.org/10.1016/j.future.2017.08.052.
[29] Shuo Wang, Richard Sinnott, Surya Nepal, Privacy-protected statistics publication over social media user trajectory streams, Future Gener. Comput. Syst. (2017). http://dx.doi.org/10.1016/j.future.2017.08.002.