Guest Editorial
Trustworthiness in Social Multimedia Analytics and Delivery

RECENTLY, social multimedia content is being delivered to users with a high quality of experience (QoE) with the advance of multimedia technologies and social networks. However, as a huge amount of social users have various demands to exchange and share multimedia content with each other, it becomes a new challenge for the current social multimedia analytics and delivery to deal with the various attacks perpetrated by malicious users or through spam contents. Therefore, the trust and risk management for social multimedia content based on the social tie of users become of prime importance to face the unpredicted threats and subsequent damage.

This Special Section aims to provide a premier forum for researchers working on the trust-based social multimedia analytics and delivery. It also provides the opportunity for both academic and industrial researchers to discuss recent results and provide solutions to the above-mentioned challenges. It is a great honor for us to have 10 research groups to share their latest research works from North America, Europe, Australia, and Asia. These papers cover multiple aspects of trustworthiness in social multimedia analytics and delivery including the related models, technologies, and applications.

In the paper "Differentially-Private and Trustworthy Online Social Multimedia Big Data Retrieval in Edge Computing," the authors present an online learning protocol to enable collaborate multimedia services of edge nodes to mobile users with differentially-private and trustworthy schemes. Edge nodes can collaborate to learn the preferences based on contexts and previous social behaviors. A multimedia content cluster tree is established from top to the bottom to support the big data analytics. This paper considers the security and privacy issues for distributed machine learning-based service recommendations in MEC with increasing big datasets.

The paper "Enhancing the Robustness of Neural Collaborative Filtering Systems under Malicious Attacks" presents a robust training strategy for neural collaborative filtering systems with robustness to adversarial perturbations. With multiple hints from the teacher model, in the student model, multiple students are trained with noise layers to obtain robust units. The proposed defensive method can be used to reduce the success rate of malicious user attacks and keep the prediction accuracy better than the standard neural recommendation systems.

In the paper "Hybrid Deep Learning-based Anomaly Detection Scheme for Suspicious Flow Detection in SDN: A Social Multimedia Perspective," the authors propose a hybrid deep learning-based anomaly detection scheme for suspicious flow detection to enhance the reliability of SDN. An anomaly detection module is presented to detect the abnormal activities and an end-to-end data delivery module is shown to satisfy the strict quality-of-service (QoS) requirements of SDN. With both real-time and benchmark datasets, experimental results prove the efficiency in terms of data delivery and anomaly detection.

The paper "Enabling Trusted and Privacy-Preserving Healthcare Services in Social Media Health Networks" proposes a trusted and privacy preserving framework to enable the trusted healthcare services between patients and caregivers. The proposed scheme combines bloom filter and collaborative filtering to recommend suitable doctors for patients and preserve the patient's health information privacy simultaneously. Furthermore, the proposed scheme integrates the identity signature to detect sibyl attacks from malicious patients who intend to provide fake ratings and reviews towards doctors in the system, to guarantee the trust between patients and doctors.

In the paper "Trust-Based Privacy-Preserving Photo Sharing in Online Social Networks," the authors propose a photo-sharing mechanism that uses the trust relationship between users to decide how to publish a photo in a privacy-preserving way. When a user wants to share a photo that involves multiple users, the service provider of the online social network will utilize the trust values to predict the privacy loss of each related user, and then delete some users' information from the photo via image processing techniques. After the photo is shared, the trust of a related user in the publisher will decrease if he or she does suffer a privacy loss. The paper has made a pioneering contribution to the collaborative privacy management issue caused by the data sharing.

In the paper "Trust-based Video Management Framework for Social Multimedia Networks," the authors present a new framework that allows the collaboration between human and machine in order to implement a trustworthy social multimedia network (SMN). The main component of the framework explores the historical behavior of the SMN users', and feeds the mined data to another component that uses an infinite Discrete Markov Decision Process (DMDP) to decide if newly uploaded content should be published to the network or not. By doing so, the framework ensures that only trusted data are exchanged in the network and that efficient Capital Expenditures (CAPEX) and Operational Expenditures (OPEX) can be achieved.

Digital Object Identifier 10.1109/TMM.2019.2899279

In the paper "Emotion-aware Multimedia System Security," the authors present an identity authentication and access control policy for the emotion-aware robot systems. The authors design an identity information privacy protection where the computational overhead is low to support the collaborative authentication of an edge cloud node. The universal access control scheme can meet the security requirement and support the edge cloud node. Based on the results with the actual testbed, it shows that the performance of the collaborative identity authentication mechanism outperforms the traditional approaches.

The paper "Socially Aware Trust Framework for Multimedia Delivery in D2D Cooperative Communication," proposes a socially aware trust framework for multimedia delivery to choose the trustworthy D2D cooperative users from D2D relay users. The proposed approach considers capability trust mainly from base station (BS) to relay users and social trust from sender to relay users. Furthermore, this paper uses a three-way decision algorithm based on naive Bayesian to pick up the reliable user set from the relay users. The effectiveness of the proposed framework is validated by numerical results.

The paper "Differential Privacy Oriented Distributed Online Learning for Mobile Social Video Prefetching" focuses on privacy-oriented user cooperative video prefetching over mobile networks. It enables optimal prefetching in terms of preference, popularity, and social interactions by solving an online convex optimization problem. The performance bound includes optimality convergence and differential privacy are proved theoretically. Experimental results provide well prefetching performance, such as access delay and a caching hit ratio, over a high dynamic mobile environment while maintaining reasonable communication overhead.

In the paper "Trust Assessment in Vehicular Social Network based on Three-Valued Subjective Logic", the authors present a solution accounting for both static and dynamic trust computational mechanisms to deal with the trust assessment problem in vehicular social networks. The trust computation mechanisms use a previously proposed logic-based model, called three-valued subjective logic (3VSL), to compute the trust propagation and fusion in a vehicular social network. The proposed approach leverages the data exchange, which can be regarded as a social connection, to account for the trust relations between vehicular networks. Furthermore, this paper categorizes the trust computation in vehicular social networks as static trust and dynamic trust.

Acknowledgment

The guest editorial team of this Special Section would like to show our thanks to all of the authors who submitted their fine work to this Special Section. We also thank all of the reviewers for their hard work and expert reviews which greatly improve the quality of the final papers. We thank Prof. Wenwu Zhu, the Editor-in-Chief, for his great support and direction throughout the process. We would also like to thank Ms. Adrienne Fisher from the Coordinator Society Publications office for her effort and help during the processing of this Special Section.

Zhou Su, *Guest Editor*
Shanghai University
Shanghai 2000444, China

Qing Fang, *Guest Editor*
Yamagata University
Yamagata-shi 990-8560, Japan

Honggang Wang, *Guest Editor*
University of Massachusetts Dartmouth
Dartmouth, MA 02747 USA

Sanjeev Mehrotra, *Guest Editor*
Microsoft Research
Redmond, WA 98052 USA

Ali C. Begen, *Guest Editor*
Ozyegin University
Istanbul 34794, Turkey

Qiang Ye, *Guest Editor*
Dalhousie University
Halifax, NS B3H 4R2, Canada

Andrea Cavallaro, *Guest Editor*
Queen Mary University of London
London E1 4NS, U.K.