Editorial Preface

Special Issue on Data Security, Privacy, and Trust in Networked Environments

Anabela Mesquita, Politécnico do Porto, Porto, Portugal
Paula Peres, Politécnico do Porto, Porto, Portugal
Fatos Xhafa, Technical University of Catalonia, Catalonia, Spain
Xu An Wang, Engineering University of Chinese Armed Police Force, Xi'an, China

With the rapid development of internet technologies, especially with advances in wireless communication technologies, mobile smart devices and cloud computing in the 21st century, Social Networking Services (SNS), Short Message Service (SMS), Instant Messaging (IM), e-business, e-government, cloud computing networks etc. have provided rich and efficient platforms for human. However, these platforms are continuously facing severe challenges in data security, trust and privacy in networked environments. These issues in such an environment have gained great attention recently from both academia and industry in recent years. The accepted papers in this special issue are devoted to present the recent developments and research achievements. They are closely related to theoretical and practical aspects on data security, trust and privacy in networked environments. The mainly contents are based on modeling algorithms and experimental analysis, involving 3D watermarking, secure scheme, privacy-preserving, trust detection scheme, security analysis of cipher, encryption scheme, SMS Spam Filtering.

The papers in this special issue are arranged as follows:

Liu, et al. in the first paper "An Improved Security 3D Watermarking Method Using Computational Integral Imaging Cryptosystem" proposed a new improved security 3D digital watermarking method based on computational integrated imaging cryptosystem. The new method is able to meet the requirements of robustness and security. The quality of image can meet these criterions of the human visual model.

The new method has some advantages of optical imaging systems such as multi-dimension, high design freedom, and high robustness. The feasibility and effectiveness of the proposed method is demonstrated by experiment.

In the second paper by Wang, et al. "Design and analysis of the secure scheme for quantum positioning based on entangled photon pair", the scheme of quantum positioning with entangled photon pair was proposed, which was consisted of ground unit, satellite and the user three parts. The new scheme can improve the accuracy of measurement and synchronization.

The third paper by Li, et al. "An Exact and Efficient Privacy-preserving Spatiotemporal Matching in Mobile Social Networks", they proposed an exact and efficient privacy-preserving spatiotemporal matching scheme in mobile social networks is proposed. The overlapping grid system is introduced into the scheme to improve the accuracy of spatiotemporal matching, and many repetitive records in a user's spatiotemporal profile are counted as one item so as to cut down the compute overhead.

The new scheme decreases the spatiotemporal matching error, and promotes the efficiency of private matchmaking simultaneously.

Yang, et al. in the fourth paper "D-S Evidence Theory Based Trust Detection Scheme in Wireless Sensor Networks" present a novel detection scheme based on Dempster-Shafer (D-S) evidence theory in Wireless sensor networks (WSNs) to detect and isolate misbehavior sensors. They focus on to solve counter- intuitive results which appear frequently when the scheme is operated. They improve the original DS evidence theory, which defines a new variable to modify the collected evidence before combination and then combines these evidences according to Dempster combination rule. Simulation results show that this scheme can detect and isolate misbehavior sensors effectively and accurately, suppress nodes collusion and improve network performance. Compared with other existing detection scheme, this scheme has more security, robustness and accuracy.

In the fifth paper "Security Analysis of Cipher ICEBERG against Bit-pattern Based Integral Attack", bit-pattern based integral attack is applied to ICEBERG—a lightweight block cipher efficient in reconfigurable hard-ware. By tracing the propagation of the plaintext structure at bit- level, the balance property is obtained and then key guesses are verified. They find that bit-pattern based integral attack is more available to ICEBERG since it traces every bit of the texts. In their research, a 2.5- round distinguisher is discovered. Using this distinguisher, they attack the 3-round ICEBERG and extend the attack to 5-round. It is the first analysis on integral attack the most effective analysis of all cryptanalysis on ICEBERG.

The sixth paper "A Pairing-based multi-user homomorphic encryption scheme" by Zhang Wei, presented a new method to privately outsource computation of different users, which is a significant cryptographic primitive in cloud computing, homomorphic encryption (HE) can evaluate on ciphertext directly without decryption, thus avoid information leakage. Because most of the available HE schemes are single user, they provide a pairing-based multiuser homomorphic encryption scheme. The scheme is a somewhat homomorphic one, which can do infinite additions and one multiplication operation.

Finally, Ma, et al. in the final paper "A Message Topic Model for Multi-grain SMS Spam Filtering" propose a message topic model (MTM) for multi-grain SMS spam filtering. They focus on overcome the sparse data problem and noise data in the SMS message. The theory of probability topic model is used by them to learn features in the SMS spam corpus. The MTM not only identify SMS spam effectively, but also can offer multi-grain classes, which is more selective for customers or mobile operators to filter the SMS messages according to their needs.

We would like to thank all the authors for their valuable contributions and the reviewers for their time and constructive feedback during several rounds of review and revision. The support by the Journal's Editorial Board is highly appreciated.

Fatos Xhafa's work has been partially supported by Research Project of the Spanish Ministry for Economy and Competitiveness (MINECO) and the European Union (FEDER funds) under grant COMMAS (ref. TIN201346181C21R).

Anabela Mesquita
Editor-in-Chief
Paula Peres
Fatos Xhafa
Xu An Wang
Guest Editors
IJTHI