Editorial

Eldon Y. Li

School of Economics and Management,
Tongji University,
1500, Siping Road, Shanghai 200092, China
and
College of Management,
National Chung Cheng University,
168, Sec. 1, University Rd.,
Minhsiung, Chiayi 621301, Taiwan
Email: eli@calpoly.edu

Today's electronic business environment is inundated with security threats over the internet. In this regular issue, we collected five articles related to security controls in electronic business. In the first article, 'AD-C: a new node anomaly detection based on community detection in social networks', Mohammad Reza Keyvanpour, Mehrnoush Barani Shirzad and Maryam Ghaderi propose a method to identify anomaly based on community detection (AD-C) for the social network graph using Facebook and Flickr datasets. The results indicate that applying the proposed method leads to increased accuracy of the community detection methods. The second article, 'Hiding critical transactions using a modified un-realisation approach', is co-authored by T. Satyanarayana Murthy, N.P. Gopalan and T.R. Athira. Hiding association rules in critical transactions is vital to hospitals, social media sites, and online departmental stores that possess sensitive data. The authors propose an algorithm based on the maximum association rule to hide the sensitive association rules by minimising the ghost rules and lost rules. The performance of this MAR algorithm is assessed on eight parameters and it outperforms the traditional algorithm on the transactional datasets.

The third article, 'Providing a public auditing cryptographic approach in cloud computing' by R. Ashalatha, Jayashree Agarkhed and Siddarama R. Patil, describes an auditing system for secure cloud storage systems using a privacy preservation scheme. The data auditability technique allows the user to make the data integrity check using a third party. The public auditability system permits the TPA to check the cloud information without downloading the original data from the user. This process involves profiling the data and evaluating the impact of inadequate quality data which results in the performance of the organisation. The fourth article, 'Enhance the security properties and information flow control' co-authored by Nadya El Moussaid and Maryam El Azhari, implements a security policy which the main role is to create a template in order to guarantee the security properties namely the confidentiality, integrity, and availability (CIA). The main purpose is to enhance the security properties by dynamically formulating them through analysing the behaviour of entities and associate them with a trust level and security class. The experimental results show the efficiency of the approach in terms of the classification and the real-time detection rate which reaches up to 95%. Finally, the fifth article, 'Hardening web browser security

configuration using machine learning technique' by Harshad Wadkar and Arun Mishra, implements a novel framework using a machine-learning algorithm to bridge the gap between default and recommended configuration. Since browser configuration states are voluminous, they need to be classified into different security levels. As such, the authors develop a prototype browser add-on using the framework to assess browser security level and modify it to increase security level if required.

For this issue of the journal, we thank the authors and reviewers for their time and effort to prepare and review the articles. Special thanks are given to the editorial staff in the home office of Inderscience Publishers for their assistance in making the publication of this issue possible. Please note that the views in these articles are those of the authors and not of the institutions and individuals of editors, editorial board, *IJEB*, and the publishers. We hope these articles are interesting to read and useful to your future research. On behalf of the editorial board, we thank you, the readers, very much for your continuous support.