Editorial

B.B. Gupta*

National Institute of Technology Kurukshetra,
Kurukshetra-136119, Haryana, India
Email: bbgupta@nitkkr.ac.in
*Corresponding author

Xiaojun Chang

Monash University,
Wellington Rd, Clayton VIC 3800, Australia
Email: Xiaojun.Chang@monash.edu

Shingo Yamaguchi

Yamaguchi University,
1677-1 Yoshida, Yamaguchi, 753-8511, Japan
Email: shingo@yamaguchi-u.ac.jp

Biographical notes: B.B. Gupta received his PhD degree from Indian Institute of Technology Roorkee, India in the area of Information and Cyber Security. He has published more than 250 research papers in international journals and conferences of high repute including IEEE, Elsevier, ACM, Springer, Wiley, Taylor & Francis, Inderscience, etc. He has visited several countries, i.e., USA, Canada, Japan, Malaysia, Thailand, Australia, UK, Macau, China, Hong-Kong, etc. to present his research work. At present, he is working as an Assistant Professor in the Department of Computer Engineering, National Institute of Technology Kurukshetra India. His research interest includes Information security, cyber security, mobile/smartphone, cloud computing, web security, intrusion detection, computer networks and phishing.

Xiaojun Chang received his PhD degree from University of Technology Sydney in 2016. From March 2014 to August 2016, he was a visiting student at Language Technologies Institute, Carnegie Mellon University. His research interests include machine learning, computer vision and multimedia. He is now working as an Assistant Professor in Monash University, Australia. He has published more than 30 peer-reviewed publications, most of them appear in top-tier journals/conferences. His publications appear in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *IEEE Transactions on Neural Networks and Learning Systems*, *International Conference on Machine Learning*, *International Joint Conference on Artificial Intelligence*, etc.

Shingo Yamaguchi is currently a Full Professor in the Graduate School of Science and Engineering, Yamaguchi University, Japan. He received his BE, ME and DE degrees from Yamaguchi University, Japan in 1992, 1994 and 2002, respectively. He was an Assistant Professor (Research Associate) in the Faculty of Engineering, Yamaguchi University, from 1997 to 2007. He was also a Visiting Scholar in the Department of Computer Science at University of Illinois at Chicago, USA in 2007. His research interest is in the area of

theoretical computer science, software engineering, including their application to consumer electronics, cyber security and cloud computing. He has published 80 transaction papers and proceeding papers of IEEE, IEICE, IPSJ, and so on. He is also a senior member of IEEE and IEICE. He also plays many important roles. He is a Conference Chair of *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE 2014)*. He was a TPC Vice-Chair of GCCE 2013. Currently, he is an Area Editor of *IEICE Transactions on Fundamentals*. And he is also TPC members of five international conferences. He is also a Secretary of IEEE Consumer Electronics Society West Japan Joint Chapter.

Cybersecurity and privacy are essential needs for modern society where information technology and services pervade every aspect of our lives. More specifically, security and privacy in the internet of things which is an essential part of daily life for accessing different systems, services and applications is a serious issue (Rahman et al., 2018; Kumari et al., 2018; Gupta, 2018). However, it is challenging to achieve while technology changes at rapid speed and our systems turn become ever more complex. The explosion of multimedia big data has created unprecedented opportunities and fundamental security challenges, since the data is not just big in volume, but also unstructured and multimodal (Huang et al., 2019; Alieyan et al., 2019; Din et al., 2018).

Specifically, this special issue addresses various security and privacy issues of multimedia big data in the internet of things, particularly on advances in IoT technologies and related areas. This special issue contains five papers dealing with different aspects of security and privacy issues of multimedia big data in the internet of things and other related areas (Stergiou et al., 2018; Jiang et al., 2018).

The first article entitled 'An improved spatial-temporal correlation algorithm combined with compressed sensing and LEACH protocol in WSNs' co-authored by Xin Xie et al. presents a compressed sensing method based on the spatial-temporal correlation of nodes to save the energy consumption of the sensor nodes. The LEACH algorithm is used to cluster the network nodes and select the cluster head. Then, the cluster head node is sampled by the compressed sensing theory. The sampled data is passed to the remote sink node through multi-hop routing. Finally, at the sink node, the OMP algorithm can be used to recover the original signal from a small amount of data transmitted by the cluster head nodes. The simulation results show that the method can effectively reduce the amount of data transmission, and save the energy consumption of nodes and prolong the lifetime of the wireless sensor network.

The second paper entitled 'An activity theory model for dynamic evolution of attack graph based on improved least square genetic algorithm' authored by Chundong Wang et al. presents an activity theory model to analyse the contradictions in the attack behaviour. In order to assess the maximum probability path of an attacker, and dynamically remain in control for the overall situation, a definition of attacker's benefit (loss/gain) value calculated by contradictory vector is proposed. Loss/gain value is used as the objective function of the genetic algorithm to produce different optimal solutions in the presence of different evidence. Taking into account the constraints of the attacker budget, an improved genetic algorithm is proposed in this paper. The benefit of each path will vary with the coming evidence and the attacker's budget. The budget is applied as an unbiased amount in the least square genetic algorithm, optimises the fitness function of the genetic algorithm. It turns constrained optimisation problem into unconstrained optimisation problem, makes the fitting curve more accurate by the principle of structural risk minimisation. Experimental results reveal that the improved least square genetic algorithm with unbiased estimator effectuate higher gains owing to the high fit degree of fitness function. The changes in the different paths with different attacker's budgets help to select the optimal attacker's budget in the experiment. The generation of the maximum probability paths for an attacker is obtained by the improved genetic algorithm. With the coming evidence, the evidence based Bayesian is used in maximum probability attack paths to get a more accurate risk assessment of the situation, and shows the dynamic evolution of attack graphs.

The third paper entitled 'Data protection and provenance in cloud of things environment: research challenges' authored by Chundong Wang et al. proposes a data privacy protection and provenance model (DDPM) based on CoT. It can protect the privacy data of the users and trace the source of leaked data. In detail, security encryption and watermarking algorithms are proposed. Meanwhile, authors used the improved k-anonymity data masking algorithm and pseudo-row watermarking algorithm in this scheme. Those algorithms can carry out security control over the whole process of data publishing, especially in data encryption, data masking and provenance verification. Finally, the experimental results show that proposed scheme has good efficiency. It is proved that the data masking time is proportional to the parameters k and L, the results also show good robustness to the common database watermarking attacks.

The fourth paper entitled 'Advanced security of two-factor authentication system using stego QR code' authored by Yacouba Kouraogo et al. In this paper, authors present a two-factor authentication communication channel based on steganography in the QR-Code. The purpose of this proposal is to better secure the mTAN of a 2FA system by using the steganography technique to hide it in the QR-Code. In other words, when authenticating, the user sends the login and password to the server that returns a stego QR-Code containing the hidden mTAN in addition to public information. Thus, the mTAN can only be read by a specific scanner that implements the technique of extracting the hidden information while having the shared key and the public information in the QR-Code is readable by the standard scanners. Finally, authors implemented the proposed method and then do the test by simulating a line banking service.

The fifth paper entitled 'New chaotic cryptosystem for the image encryption' authored by Assia Merzoug et al. presents a new image encryption scheme. The idea is to associate the Hénon attractor and the logistics map, for the construction of a new secret key cryptosystem. Authors generate values through of the logistics map that will be added to the pixels of the plaintext image. This result modulo 256 will be permuted to another position of the encrypted image. The calculation of this permutation is deducted from the Hénon attractor, which is 2-dimensional, in order to have a significantly increasing the resistance to attacks. The proposed system has the advantage of bigger key space (about 180 bits); high security analysis such as key space analysis, statistical analysis and sensitivity analysis were carried out. The results demonstrate that the proposed system is highly efficient and a robust system.

This special issue is due to encouragement of Dr. Eldon Y. Li and Dr. Raylin Tso who are instrumental in the organisation process. Many individuals have contributed for 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. This special issue presents some selected papers in touching important aspects of security and privacy issues of multimedia big data in the internet of things, particularly on advances in IoT technologies and related areas and also emphasises many open questions.

References

Alieyan, K., Almomani, A., Anbar, M., Alauthman, M., Abdullah, R. et al. (2019) 'DNS rule-based schema to botnet detection', *Enterprise Information Systems*, pp.1–20, DOI: https://doi.org/10.1080/17517575.2019.1644673.

Din, S., Paul, A., Ahmad, A. et al. (2018) 'Service orchestration of optimizing continuous features in industrial surveillance using big data based fog-enabled internet of things', *IEEE Access*, Vol. 6, pp.21582–21591, DOI: 10.1109/ACCESS.2018.2800758.

Gupta, B.B. (Ed.) (2018) *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives*, CRC Press, Taylor & Francis, UK.

Huang, Y., Li, B., Liu, Z., Li, J. et al. (2019) 'ThinORAM: towards practical oblivious data access in fog computing environment', *IEEE Transactions on Services Computing*, DOI: 10.1109/TSC.2019.2962110.

Jiang, F., Fu, Y., Gupta, B. B., Lou, F., Rho, S., Meng, F. and Tian, Z. (2018) 'Deep learning based multi-channel intelligent attack detection for data security', *IEEE Transactions on Sustainable Computing*, DOI: 10.1109/TSUSC.2018.2793284.

Kumari, A., Tanwar, S., Tyagi, S., Kumar, N., Maasberg, M. and Choo, K.K.R. (2018) 'Multimedia big data computing and internet of things applications: a taxonomy and process model', *Journal of Network and Computer Applications*, Vol. 124, pp.169–195, DOI: https://doi.org/10.1016/j.jnca.2018.09.014.

Rahman, M.A., Hossain, M.S., Hassanain, E. and Muhammad, G. (2018) 'Semantic multimedia fog computing and IoT environment: sustainability perspective', *IEEE Communications Magazine*, Vol. 56, No. 5, pp.80–87.

Stergiou, C., Psannis, K. E., Gupta, B.B. and Ishibashi, Y. (2018) 'Security, privacy & efficiency of sustainable cloud computing for big data & IoT', *Sustainable Computing: Informatics and Systems*, Vol. 19, pp.174–184.