Editorial

B.B. Gupta*

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

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 in the area of Information and Cyber Security from the Indian Institute of Technology Roorkee, India. He published more than 200 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., Canada, Japan, Malaysia, China, Hong Kong, etc. to present his research work. 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, cloud computing, web security, intrusion detection and phishing.

Shingo Yamaguchi is a Professor in the Graduate School of Science and Engineering, Yamaguchi University, Japan. He received his BE, ME and DE degrees from the Yamaguchi University, Japan, in 1992, 1994 and 2002, respectively. He has published almost 100 transactions, proceedings and survey papers of IEEE, IEICE, etc. He was the Conference Chair of the IEEE international conferences, such as GCCE 2014 and GCCE 2015. He is currently the Chapter Chair of the IEEE Consumer Electronics Society, West Japan Joint Chapter. He is an area editor of *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*. He is a senior member of the IEEE and IEICE.

Information security and privacy are essential needs for our modern society in which information technology and services pervade every aspect of our lives (Jiang et al., 2018; Gupta et al., 2016). Particularly, security and privacy of multimedia big data, which is becoming a part of daily life for accessing different systems, services and applications is a serious issue (Stergiou et al., 2018a; Gupta et al., 2018a). However, it is challenging to address as technology develops at rapid speed and our systems become ever more complex. The explosion of multimedia big data in internet of things (IoT) systems has created unprecedented opportunities and fundamental security and privacy challenges, as it is not just big in volume, but also unstructured and multi-modal (Adat et al., 2018). This special issue intends to bring together state-of-art research and developments in security and privacy of IoT and secure IoT services, novel attacks on IoT services, novel defences for IoT service attacks, and forensics and IoT security analysis. Topics for this

special issue include, but are not limited to (Gupta et al., 2015; Zhang et al., 2014; Tewari et al., 2018; Din et al., 2018; Wang et al., 2018):

- security and privacy of big data in IoT
- security and privacy management of multimedia big data in IoT
- intrusion detection systems in IoT
- security and privacy of pricing and billing for IoT services
- cryptography, authentication, authorisation and usage control for IoT systems
- security of mobile, peer-to-peer and pervasive services in IoT
- security of big data in mobile commerce and mobile IoT
- big data-enabling social networks on mobile clouds and in IoT
- security protocols in IoT
- privacy protocols in IoT
- forensics in IoT
- social engineering, insider threats, advanced spear phishing in IoT
- multi-modal information retrieval for big data in IoT systems
- security and privacy of big data in MCC and cloud.

This special issue contains five papers focuses on information security, privacy and forensics of multimedia big data in the IoT and other related areas (Gupta and Quamara, 2018; Stergiou et al., 2018b; Gupta and Sheng, 2019; Psannis et al., 2018; Joshi and Gupta, 2019; Gupta et al., 2018b) which were selected after rigorous review process. The first article entitled, 'Botnet detection based on DNS traffic similarity' authored by Ahmad Manasrah et al. presents a scalable approach for detecting a group of bot hosts from their DNS traffic is proposed. The proposed approach leverages a signal processing technique, power spectral density (PSD) analysis, to discover the significant frequencies (i.e., periods) of the botnets periodic DNS queries. The proposed approach processes the timing information of the generated DNS queries, regardless of the number of queries or domain names. Measuring the level of similarity between hosts demonstrating periodic DNS queries should reveal the group of bot hosts in the monitored network. Finally, authors evaluated the proposed approach using multiple DNS traces collected from different sources along with a real world botnet deployed under controlled environment. The evaluation result shows that the proposed approach was able to detect the group of bot hosts that demonstrates similar periodic DNS pattern with high accuracy and minimum false positives rates.

The second article entitled, 'Fingerprinting violating machines with in-memory protocol artefacts' authored by Mohammed I. Al-Saleh and Yaser Jararweh discusses that tracking the IP address of the attacker to its origin is indispensable. However, apart from finding the attacker's (possible) machine, it is inevitable to provide supportive proofs to bind the attack to the attacker's machine, rather than depending solely on the IP address of the attacker, which can be dynamic. This paper proposes to implant such supportive proofs by utilising the internals of three well-known internet protocols: IP, TCP and

ICMP. Authors claim that their results show that there can be potential proofs in the structures of these protocols. In addition, because a violator is unaware of (and has no control over) the involved protocols, the investigation process is empowered with stealth. Authors also claim that they are the first to utilise protocol remnants in fingerprinting violating machines.

In the third article entitled, 'Enhancement of 3D-Playfair algorithm using dual key' authored by Arnab Kumar Das and Nabanita Das proposed an extended 3D-Playfair cipher working with 256 (4 × 8 × 8) characters. It selected 52 alphabets (upper case and lower case), ten numerals and 194 most commonly used special characters of ASCII character set. Authors used the 3D version of the Playfair cipher but use the digraph concept. The restrictions of existing 2D-Playfair ciphers and 3D-Playfair cipher using 4 × 4 × 4 matrices, 6 × 4 × 4 matrices are overcome in the proposed work. As per authors claim, the proposed algorithm can accumulate more characters than the existing 3D-Playfair ciphers.

The fourth article entitled, 'A knowledgebase insider threat mitigation model in the cloud: a proactive approach' authored by Qutaibah Althebyan et al. presents a proactive insider threat model using a knowledgebase approach. Proactive in a sense that proposed model tries to detect (in advance) any deliberate deviation of the legal accesses an insider might try to perform so that the individual's private data will be protected and secured. At the same time, the cloud resources will be insured to be secured as well as consistent at all times. Knowledgebase models were used earlier in preventing insider threats in both the system level and the database level. This knowledgebase work will be extended to cloud computing systems. The proposed model insures an in advance mitigation in the form of detection (and hence, a chance for prevention) of possible insider breaches. This mitigation correlates system insider's admins' knowledge who may grant undesired privileges to insiders of the underlying cloud data centre. The proposed model handles the insider threat in a cloud data centre at its several levels: the host level and the network level where insiders are categorised several levels of privileges according to their locations within the cloud data centre. Simulation results show that the proposed model works well in predicting malicious acts of insiders of the cloud data centre. It also shows that although proposed model is effective in predicting insiders' threats, it still performs well with minimum overhead to its performance. This fact has been concluded by showing that the number of blocked insiders is reduced to the minimum.

The aim of this paper entitled, 'Digital video forensics: a comprehensive survey' authored by Mohammad Alsmirat et al. is to collect and provide the definitions of the main concepts related to media forensics. Also, this paper aims to give an overview of the different techniques used in media forensics concentrating on video forensics. Furthermore, this paper classifies the work done in the field according to the main technique used in the proposed solution approach.

We would like to express our special thanks to Prof. Valentina E. Balas and Prof. Anca Ralescu, the Editors-in-Chief of *International Journal of Advanced Intelligence Paradigms* (*IJAIP*), for their great support and efforts throughout the whole publication process of this special issue. Moreover, this special issue is due to the encouragement of *IJAIP* 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

Adat, V. et al. (2018) 'Security in internet of things: issues, challenges, taxonomy, and architecture', *Telecommunication Systems*, Vol. 67, No. 3, pp.423–441.

Din, S. 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.

Gupta, B.B. and Quamara, M. (2018) 'An overview of internet of things (IoT): architectural aspects, challenges, and protocols', *Concurrency and Computation: Practice and Experience*, e4946, DOI: 10.1109/ACCESS.2018.2800758.

Gupta, B.B. and Sheng, Q.Z. (2019) *Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices*, p.352, CRC Press, Taylor & Francis [online] DOI: https://doi.org/10.1002/cpe.4946.

Gupta, B.B., Agrawal, D.P. and Wang, H. (2018a) *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives*, p.666, CRC Press, Taylor & Francis, UK.

Gupta, B.B., Yamaguchi, S. and Agrawal, D.P. (2018b) 'Advances in security and privacy of multimedia big data in mobile and cloud computing', *Multimedia Tools and Applications*, Vol. 77, No. 7, pp.9203–9208.

Gupta, B.B., Agrawal, D.P. and Yamaguchi, S. (2016) *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*, IGI Global Publisher, USA.

Gupta, S. et al. (2015) 'BDS: browser dependent XSS sanitizer', *Handbook of Research on Securing Cloud-based Databases with Biometric Applications*, pp.174–191, IGI Global, UK.

Jiang, F. et al. (2018) 'Deep learning based multi-channel intelligent attack detection for data security', *IEEE Transactions on Sustainable Computing*, USA.

Joshi, R.C. and Gupta, B.B. (2019) *Security, Privacy, and Forensics Issues in Big Data*, p.452, IGI Global Publisher, USA.

Psannis, K., Stergiou, C. et al. (2018) 'Advanced media-based smart big data on intelligent cloud systems', *IEEE Transactions on Sustainable Computing*, pp.1–11, DOI: 10.1109/TSUSC.2018.2793284.

Stergiou, C. et al. (2018a) 'Security, privacy & efficiency of sustainable cloud computing for big data & IoT', *Sustainable Computing: Informatics and Systems*, Vol. 19, pp.174–184.

Stergiou, C. et al. (2018b) 'Secure integration of IoT and cloud computing', *Future Generation Computer Systems*, Vol. 78, No. 3, pp.964–975 [online] DOI: https://doi.org/10.1016/j.future.2016.11.031.

Tewari, A. et al. (2018) 'Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework', *Future Generation Computer Systems* [online] DOI is: https://doi.org/10.1016/j.future.2018.04.027.

Wang, L. et al. (2018) 'Compressive sensing of medical images with confidentially homomorphic aggregations', *IEEE Internet of Things Journal*, Vol. 6, No. 2, pp.1402–1409.

Zhang, Z-K. et al. (2014) 'IoT security: ongoing challenges and research opportunities', *2014 IEEE 7th International Conference on Service-oriented Computing and Applications*, IEEE.