# Editorial

B.B. Gupta*

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

Dharma P. Agrawal

Department of Electrical Engineering and Computing Systems,
University of Cincinnati,
Cincinnati, OH 45221-0030, USA
Email: dpa@cs.uc.edu

**Biographical notes:** B.B. Gupta received his PhD from Indian Institute of Technology Roorkee, India in the area of information security. He has published more than 90 research papers in international journals and conferences of high repute. He has visited several countries to present his research work. His biography has published in the Marquis Who's Who in the World, 2012. Currently, 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, computer networks and phishing.

Dharma P. Agrawal is the OBR Distinguished Professor and the Founding Director for the Center for Distributed and Mobile Computing in the Department of ECECS, University of Cincinnati, USA. His current research interests include energy efficient routing, information retrieval, and secured communication in ad hoc and sensor networks, effective handoff handling and multicasting in integrated wireless networks, etc. He has served as an editor of the *IEEE Transactions on Computers*. He has received numerous certificates and awards from the IEEE Computer Society, including a 'Third Millennium Medal' for outstanding contributions. He is a fellow of the IEEE, ACM and AAAS.

Recent advances in wireless and VLSI technologies have led to smart devices both at home and work place that can be connected to form internet of things (IoT). Thus, IoT consists of smart connected devices that have embedded electronics, software, sensors, actuators, and network, which enable these objects to collect and exchange data among themselves. Such a heterogeneous system has components with varying data formats, diverse functionalities and altogether different expectations (Gralla, 2007; Gupta et al., 2016; Agrawal and Zeng, 2016). Some of the elements are static while others are mobile in nature, creating an accurate mobile cloud environment. The diversity in functionalities and diverse range of resources make some easily vulnerable to hackers, while others stay strong against security threats. Given the lax behaviour of users towards device security

Copyright © 2017 Inderscience Enterprises Ltd.

and having simple channels for data transfer, malware is expected to grow exponentially. These considerations have led to this special issue and security solutions have evolved to detect and prevent attacks, and are able to perform forensic analysis that have significantly complicated user authentication, access control and system security. Specifically, this special issue addresses various security issues in mobile cloud computing and the IoT, particularly on advances in mobile computing technologies and related areas (Tewari and Gupta, 2016; Alsmirat et al., 2016; Abolfazli et al., 2016). This special issue contains eight papers dealing with different aspects of security issues in mobile cloud computing, IoT and other related areas (Gupta and Gupta, 2016; Zhang and Gupta, 2016; Li et al., 2015; Whitmore et al., 2015).

The first article entitled 'Dynamic weighted VM load balancing for cloud-analyst' authored by Ahmad Manasrah presents an analysis of the various VM load balancing algorithms. Further, author proposed a new VM load balancing algorithm for an IaaS framework and implemented in virtual machine (VM) environment of cloud-analyst in order to achieve better performance in terms of response and processing time.

The second paper entitled 'Robust watermarking technique using back propagation neural network: a security protection mechanism for social applications' authored by Aditi Zear et al. presents an algorithm for digital watermarking based on discrete wavelet transforms (DWT) and singular value decomposition (SVD). In the embedding process, authors decomposed the host colour image into third-level DWT. Moreover, authors have used back propagation neural network (BPNN) to enhance the robustness performance of the image watermark. Various experiments are performed and results indicate that the proposed method is able to withstand a variety of signal processing attacks and provide superior performance for robustness and imperceptibility compared to existing methods.

The third paper entitled 'Trust delegation-based secure mobile cloud computing framework' authored by Lo'ai Tawalbeh et al. presents the main issues associated with mobile cloud computing models that include: security, performance, and quality of service. Afterwards, authors present secure implementation of the cloudlet-based mobile cloud computing framework with its prototype that uses trust delegation technique to provide better security and performance tradeoffs.

The fourth paper entitled 'Virtual machine security' is authored by Arif Khan. In this paper, authors present the security of the VM. Author mentioned that the various features of the virtual platform originate from the possibilities of threats. Author depicted how those threats affect the deployment of a VM in the cloud computing. Moreover, authors also discussed the proper techniques to construct a novel defence mechanism for virtualisation.

The fifth paper entitled 'Hierarchical detection of insider attacks in cloud computing systems' authored by Omar Al-Jarrah et al. presents the use artificial intelligent (AI) techniques to detect insider attacks in cloud computing. Authors have used a hierarchical detection system to insure a detection accuracy and speed. CloudExp simulator is used to simulate the proposed hierarchical detection approach. Various experiments are performed to evaluate the performance of the overall system using detection rate, precision, recall rates, and false positives ratio and better results are obtained.

The sixth paper entitled 'A secure mobile commerce framework based on community cloud' authored by Hisham Alsaghier presents a secure mobile commerce framework which overcomes all the flaws in the existing literature by making use of wireless public key infrastructure (WPKI), universal integrated circuit card (UICC) and banking

community cloud (BCC). Author claims that end to end security is ensured thereby ensuring authentication, integrity, confidentiality, and non-repudiation properties.

The seventh paper entitled 'Evaluation of puzzle-enabled proxy-assisted denial-of-service protection for web services' authored by Jothi Rangasamy et al. investigates the efficacy of a cryptographic DoS countermeasure, such as, client puzzles which can be used to achieve a weak authentication as it forces the client to solve a somewhat-difficult computational problem in order to get serviced. Authors claim that they integrate puzzles into reverse proxy and demonstrate that the proposed approach is indeed effective and advantageous in protecting the web servers from both flooding and semantic type attacks.

The eighth paper entitled, 'Mitigating selfish, blackhole and wormhole attacks in DTN in a secure, cooperative way' authored by Amit Kumar Gupta et al. presents cooperative approach to mitigate the destructive effects posed by selfish, blackhole and wormhole attacks in DTN scenario. Authors claim that with nominal overhead, proposed method provides good improvement on the overall performance. Performance of the proposed method is evaluated by implementing it over an existing DTN routing strategy, namely the spray and wait protocol, in the ONE simulator. It is observed that our proposed strategy is able to avoid the three types of malicious nodes in the message transmission process effectively and increases the trustworthiness of communication process.

This special issue is due to encouragement of Dr. Eldon Y. Li and Dr. Xin (Robert) Luo 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 in the mobile cloud computing and IoT, particularly on advances in mobile computing technologies and related areas and also emphasises many open questions. The wide spread use of mobile cloud computing and IoT is encouraging researchers to look at various open questions and a lot more work need to be done before it becomes a reality and widely accepted by the user community.

## References

Abolfazli, S. et al. (2016) 'Mobile cloud computing', *Encyclopedia of Cloud Computing*, pp.29–40.

Agrawal, D.P. and Zeng, Q-A. (2016) *Introduction to Wireless and Mobile Systems*, 4th ed., Cengage Learning, USA.

Alsmirat, M.A., Jararweh, Y., Obidat, I. and Gupta, B.B. (2016) 'Internet of surveillance: a cloud supported large scale wireless surveillance system', *The Journal of Supercomputing*, Springer, DOI: 10.1007/s11227-016-1857-x.

Gralla, P. (2007) *How the Internet Works*, Que Pub., Indianapolis, ISBN: 0-7897-2132-5.

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. and Gupta, B.B. (2016) 'XSS-secure as a service for the platforms of online social network-based multimedia web applications in cloud', *Multimedia Tools and Applications*, Springer, DOI: 10.1007/s11042-016-3735-1.

Li, J., Li, J., Chen, X., Jia, C. and Lou, W. (2015) 'Identity-based encryption with outsourced revocation in cloud computing', *IEEE Transactions on Computers*, Vol. 64, No. 2, pp.425–437.

Tewari, A. and Gupta, B.B. (2016) 'Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags', *Journal of Supercomputing*, Springer, DOI: 10.1007/s11227-016-1849-x.

Whitmore, A., Agarwal, A. and Xu, L.D. (2015) 'The internet of things – a survey of topics and trends', *Information Systems Frontiers*, Vol. 17, No. 2, pp.261–274.

Zhang, Z. and Gupta, B.B. (2016) 'Social media security and trustworthiness: overview and new direction', *Future Generation Computer Systems*, Elsevier, DOI: 10.1016/j.future.2016.10.007.