Editorial

B.B. Gupta

Department of Computer Engineering,
National Institute of Technology Kurukshetra,
Haryana, 136119, India
Email: bbgupta@nitkkr.ac.in
Email: gupta.brij@gmail.com

Biographical notes: B.B. Gupta received his PhD from the Indian Institute of Technology Roorkee, India in the area of information and cyber security. He has published more than 175 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 from 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.

Nowadays, cloud computing has developed a lot and been accepted by an increasing number of people. More and more companies and individuals prefer to outsource their data in the cloud to relief their local burden. Note that some of the client data is private, such as enterprise management data, individual photos and so on. Once the private data is leaked out, the consequence is horrible. It makes the design of data storage and verification directed at the cloud be in an urgent need. Hence, to create a safe and harmonious atmosphere of cloud computing is of particular importance. Although lots of researches in the field of cloud computing have been studied, there are still many open research issues to be further explored. To meet the requirements of data security in cloud computing and improve the user experience of cloud clients, innovative and secure data storage and verification protocols should be further studied (Yu et al., 2010; Stergiou et al., 2018; Subashini and Kavitha, 2011; Psannis et al., 2018; Li et al., 2017). This special issue mainly focuses to address challenges and present effective solutions for secure cloud storage and serves as a venue for the researchers around the world to share their state-of-the art research and technological solutions. Topics for this special issue include, but are not limited to (Bhushan and Gupta, 2017; Gupta et al., 2016; Alsmirat et al., 2017; Gupta and Badve, 2017; Muhammad et al., 2018):

- secure cloud storage protocol
- secure auditing protocols for cloud storage
- data dynamics support in cloud data verification
- outsourced data verification for multi-user in multi-cloud
- cloud storage supporting malicious user revocation
- privacy preserving in cloud storage
- storage QoS in a multi-tenant cloud
- replication and consistency in cloud storage
- backup and archival in cloud storage.

This special issue contains six papers focuses on secure data storage in cloud computing and other related areas (Hossain et al., 2017; Manasrah and Gupta, 2018; Gupta et al., 2018; Jararweh et al., 2017; Rong et al., 2013) which were selected after rigorous review process. The first article entitled, 'An access control framework for multi-level security in cloud environments' authored by Hongbin Zhang, et al. presents an access control framework which provides rigorous multilevel security in single domain and a multilevel mapping method between domains. In each domain, a policy processing method is designed to handle the multilevel policies and creates a DAG model that describes the access control relationship between all entities in the domain. The DAG model can be converted to a hierarchical access control structures that ensure rigorous multilevel security in intra domains. Moreover, between domains, the mapping method based on quantised subject attributes is proposed to determine the subject's security level in its target domain. Credibility is used in the framework to adjust the mapping value in order to achieve flexible multilevel inter-domain access control. Experimental results from simulations show that proposal can realise accurate inter-domain mapping and achieve multilevel security access control in inter-domain. The second article entitled, 'Improve the robustness of data mining algorithm against adversarial evasion attack' authored by Ning Cao et al. presents a novel approach that introduces uncertainty to the model behaviour, in order to obfuscate the decision process of the attacking strategy and improve the robustness of security system against attacks that try to evade the detection. Proposed approach addresses three problems. First, authors build a pool of mining models

to improve robustness of a variety of mining algorithms, similar to ensemble learning but focusing on the optimisation the trade-off between off-line accuracy and robustness. Second, authors randomly select a subset of models at run time (when the model is used for detection) to further boost the robustness. Third, authors propose a theoretical framework that bounds the minimal number of features an attacker needs to modify given a set of selected models. In the third article entitled, 'Formal analysis of a private access control protocol to a cloud storage' authored by Mouhebeddine Berrima et al., authors enhance the security of cloud storage systems through a formal analysis of a cloud storage protocol based on ABS and ABE schemes. Authors clarify several ambiguities in the design of this protocol and model the protocol and its security properties with ProVerif an automatic tool for the verification of cryptographic protocols. Authors discover an unknown attack against user privacy in the Ruj et al. protocol. Moreover, authors propose a correction, and automatically prove the security of the corrected protocol with ProVerif.

The fourth article entitled, 'Scalable video coding algorithm and rate-distortion optimisation based on cloud computing' authored by Yuejin Zhang et al. presents an adaptive multi-path video stream scalable video coding algorithm based on the cloud computing for H264/AVC extension, with the path of diversity provided by based on the cloud computing video distribution network. The method of using scalable video coding is finally adapted to the various end users. Moreover, it adapts to network bandwidth fluctuation by observing the changes of the available bandwidth over the multiple overlay paths. And performing rate-distortion optimisation in the basis of the end-to-end distortion estimation has given a method of reducing complexity. Experimental results show that the optimisation algorithm based on the cloud computing video distribution network is more effective to reduce video packet loss rate and network latency, rate-distortion optimisation performance gain outperforms the current redundancy coding scheme and traditional recursive optimal per-pixel estimation, ensure the quality of the video network transmission. The fifth article entitled, 'A blue noise pattern sampling method based on cloud computing to prevent aliasing' authored by Aiyun Zhan et al. presents an object-order algorithm in order to meet the results of theoretical complexity of O (n^2). Experimental results show that the low sampling rate model based on cloud computing can effectively prevent aliasing structure, in a high sampling rate model based on cloud computing also perform equally well. Simulation results employing H.264's redundant slice mechanism show significant performance gains over conventional error-resilient encoding methods and native redundant encoding methods. The sixth article entitled, 'An empirical study of cloud computing and big data analytics' authored by Emad Al-Shawakfa and Hiba Alsghaier presents some aspects of utilising big data and cloud computing with their effects on an organisation's business performance in many sectors. Furthermore, some issues of using big data and cloud computing in various environments are also addressed. The usage of cloud computing for internet of things and issues about it are also covered in this paper.

We would like to express our special thanks to Prof. Nadia Nedjah, the Editor-in-Chief of *International Journal of Innovative Computing and Applications* (*IJICA*), for his great support and efforts throughout the whole publication process of this special issue. Moreover, this special issue is due to the encouragement of *IJICA* 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

Alsmirat, M.A., Jararweh, Y., Obaidat, I. et al. (2017) 'Internet of surveillance: a cloud supported large-scale wireless surveillance system', *The Journal of Supercomputing*, Vol. 73, No. 3, pp.973–992.

Bhushan, K. and Gupta, B.B. (2017) 'Security challenges in cloud computing: state-of-art', *International Journal of Big Data Intelligence*, Vol. 4, No. 2, pp.81–107.

Gupta, B.B. and Badve, O.P. (2017) 'Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment', *Neural Computing and Applications*, Vol. 28, No. 12, pp.3655–3682.

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, B.B., Yamaguchi, S. and Agrawal, D.P. (2018) '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.

Hossain, M.S. and Muhammad, G. et al. (2017) 'Cloud-assisted secure video transmission and sharing framework for smart cities', *Future Generation Computer Systems*, June, Vol. 83, pp.596–606.

Jararweh, Y. et al. (2017) 'Software-defined system support for enabling ubiquitous mobile edge computing', *The Computer Journal*, Vol. 60, No. 10, pp.1443–1457.

Li, T. et al. (2017) 'Socially-conforming cooperative computation in cloud networks', *Journal of Parallel and Distributed Computing*, July, Vol. 117, pp.274–280.

Manasrah, A.M. and Gupta, B.B. (2018) 'An optimized service broker routing policy based on differential evolution algorithm in fog/cloud environment', *Cluster Computing*, pp.1–15, DOI: https://doi.org/10.1007/s10586-017-1559-z.

Muhammad, G., Alhamid, M.F. et al. (2018) 'Edge computing with cloud for voice disorder assessment and treatment', *IEEE Communications Magazine*, Vol. 56, No. 4, pp.60–65.

Psannis, K., Stergiou, C. et al. (2018) 'Advanced media-based smart big data on intelligent cloud systems', *IEEE Transactions on Sustainable Computing*, DOI: 10.1109/TSUSC.2018.2817043

Rong, C., Nguyen, S.T. and Jaatun, M.G. (2013) 'Beyond lightning: a survey on security challenges in cloud computing', *Computers & Electrical Engineering*, Vol. 39, No. 1, pp.47–54.

Stergiou, C. et al. (2018) 'Secure integration of IoT and cloud computing', *Future Generation Computer Systems*, January, Vol. 78, Part 3, pp.964–975.

Subashini, S. and Kavitha, V. (2011) 'A survey on security issues in service delivery models of cloud computing', *Journal of Network and Computer Applications*, Vol. 34, No. 1, pp.1–11.

Yu, S., Wang, C., Ren, K. and Lou, W. (2010) 'Achieving secure, scalable, and fine-grained data access control in cloud computing', in *2010 Proceedings IEEE, Infocom*, pp.1–9.