Editorial

B.B. Gupta*

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

Dharma P. Agrawal

University of Cincinnati,
Cincinnati, 45220, USA
Email: dpa@cs.uc.edu

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 300 research papers in international journals and conferences of high repute including the 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.

Dharma P. Agrawal is an OBR distinguished Professor in Department of Electrical Engineering and Computing Systems. His current research interests include applications of sensor networks in monitoring Parkinson's disease patients and neurosis, applications of sensor networks in monitoring fitness of athletes' personnel wellness, applications of sensor networks in monitoring firefighters physical condition in action, efficient secured communication in sensor networks, secured group communication in vehicular networks, use of Femto cells in LTE technology and interference issues, heterogeneous wireless networks, and resource allocation and security in mesh networks for 4G technology.

Computational intelligence is the theory, design, application and development of biologically and linguistically motivated computational paradigms. The application with the state-of-art the CI-based technologies fuzzy systems, evolutionary computation, genetic programming, neural networks and artificial immune systems, and highlight how CI-based technologies play critical roles in various security and privacy of cloud and IoT-based consumer data. The technology cloud and IoT already become a backbone for our daily communication in the society. Sharing the resources and information via these technologies is important for communication and touched almost every field such as education, finance, agriculture, healthcare, etc. (Jiang et al., 2018; Pasupuleti, 2019; Gou et al., 2017), however at the same time, the issues and concern about security and privacy about consumers data has been raised (Gou et al., 2017; Stergiou et al., 2020; Adat et al., 2018; Gupta et al., 2015). However, as technology advances at a breakneck pace and our processes become increasingly complex, it is difficult to solve (Zhang et al., 2014; Al-Qerem et al., 2020; Din et al., 2018). Since multimedia big data is not only large in volume, but also unstructured and multi-modal, it has generated unparalleled opportunities as well as fundamental security and privacy challenges in (IoT) systems. This special issue intends to bring together state-of-art research and developments in security and privacy of cloud and IoT services, novel attacks over the users of IoT-cloud, novel defences for protecting our data, and forensics security analysis. Topics for this special issue include, but are not limited to (Gupta and Gupta, 2015; Gupta and Quamara, 2018; Esposito et al., 2021; Gupta et al., 2012; Psannis et al., 2018):

- security and privacy of cloud and IoT
- security and privacy of big data in IoT
- security and privacy of IoT-enabled services
- intrusion detection systems in IoT-cloud
- security and privacy of pricing and billing for IoT services
- cryptography, authentication, authorisation and usage control for cloud-IoT systems
- security of mobile, peer-to-peer and pervasive services
- security and privacy protocols
- forensics in IoT-cloud.

This special issue contains six papers focuses on security and privacy in cloud and IoT-based consumer data and other related areas (Chhabra et al., 2013; Gupta et al., 2018; Zhang et al., 2017; Gupta and Quamara, 2020; Hossain et al., 2019; Stergiou et al., 2018) which were selected after rigorous review process. The first article entitled, ‘Research on privacy protection system of RFID personal consumption data based on internet of things and cloud computing’ authored by Ningning Du and Chongxu Chen presents the traditional ideas in sociology, law, and ethics have been subverted as a result of the internet of things and cloud computing. In order to increase the privacy protection standard of personal consumption data, the internet of things and cloud computing are being used to create a privacy protection model. In this paper, the first step is to conduct a legal interpretation of personal privacy data protection in RFID. Second, a privacy protection model based on cloud computing is developed, as well as the algorithm that goes with it. Finally, the RFID personal consumption data privacy security authentication protocol is developed. At last, simulation analysis is used to compare the protocol search time-consuming comparison based on conventional and proposed privacy security schemes. Authors presented the results which show that the proposed model can efficiently protect personal usage data.

The second article entitled, ‘Research on network security defence based on big data clustering algorithms’ by Jianchao Zhao presents the enhanced clustering algorithm which is used to carry out network security protection in the big data age to improve network security. In this paper, the use of large data clustering algorithms in network security protection is first investigated. Second, the network security defence model is investigated, and a mathematical model is proposed. The authors developed the proposed model by analysing text requirements and data characteristics. The proposed work is simulated and the results of the theory review indicate that the proposed model may provide a theoretical foundation for developing network information systems.

In the third article entitled, 'Information protection of end users on the web: privacy issues and measures' authored by Nooh Bany Muhammad and Aya Kandil discussed about cyber security and how the online scammers are increasing day by day with the advancement of the technology as well. End users must ensure that their data is secured in order to protect private information. End users are expected to use methods to secure data from online hackers in order to keep their files protected. In the paper, the authors discussed that what security measures do websites employ? What is the safest way to secure our data and what is the best behaviour? And then, how the end users becomes the victims over web-based end-user.

The fourth article entitled, 'E-commerce process reengineering for customer privacy protection', by Fengming Ma et al. focused and concerned about the privacy of the customers. In the paper, e-commerce has evolved into a modern catalyst for economic growth, injecting new energy into economic development and fundamentally altering the way people function and live. However, in the e-commerce process, a privacy security measure for consumer information is not in effect, resulting in privacy leakage in various ties and varying degrees of impact on the customer. Theft of personal information is a huge hidden threat to the safe and orderly growth of e-commerce. The fact that customer information is stored and presented in plaintext in the e-commerce process is the primary cause of customer information privacy leakage. It is incredibly simple for lawless elements to obtain customer details. In this paper, a consumer privacy security platform is presented based on an overview of the key explanation for privacy leakage, with technological steps such as information segmentation, data encryption, and access authorisation taken for customer privacy information, according to the characteristics of e-commerce. The standard e-commerce process has been altered, and consumer information is now used on demand. Traceability aids in the prevention of customer data leakage and misuse to the greatest extent possible.

The fifth article entitled 'The prediction of network security situation based on deep learning method' by Zhixing Lin et al. uses the deep learning technology, which is used to analyse and learn network data, generate counter networks for sample amplification using classification, use sparse noise reduction auto encoder for feature selection, and then use LSTM for deep learning model of security situation prediction in this paper. The authors proposed the network security situation prediction model and after the experiments, it is proved that the proposed LSTM network security situation prediction model based on sparse noise reduction since the encoder can solve different levels of attack against small numbers, not balanced, using the model prediction results more accurate, and in predicting in predicting regional security situation has the advantage for a long time in order to solve the problems.

The aim of the paper entitled 'A hybrid approach for preserving privacy for real estate data' by Parmod Kalia et al. is to discuss the use of increasingly reliant on cloud-based applications, which include online services such as e-banking, e-commerce and e-payment, among others, in the digital era. On such a forum, the disclosure of personal and confidential information becomes a potential attack target. It is critical to protect personal and sensitive information from an unwanted adversary while also ensuring that the necessary data can be accessed for the particular purpose for which it was obtained without revealing sensitive information. Researchers used randomised data distortion techniques to mask sensitive information by converting the data and adding random noise to the original dataset. This form of perturbation technique is useful for numerical datasets, but its application to other types of data is restricted. Authors suggested a hybrid model of two phases encoding with additive random noise value to address the limitations of randomised data distortion techniques while maintaining efficient data privacy and usefulness. To sensitise the data structure, this paper introduces a predefined classification of attributes based on sensitivity. The proposed method of encoding original data with additive noise value guarantees non-disclosure of private and confidential data while maintaining an efficient balance between data privacy and data utility. The results of using the proposed technique on various data sizes in the real estate industry in terms of efficiency and effectiveness in protecting privacy and data usefulness are presented in this paper. The proposed approach's retrieval algorithm was tested in terms of privacy level and information loss, and it proved to be efficient in comparison to other privacy-preserving strategies such as perturbation and encryption in terms of performance, spatial efficiency and information loss.

We would like to express our special thanks to Prof. Associate Prof. Biju Issac, the Editor-in-Chief of *International Journal of Information and Computer Security* (*IJICS*), for his great support and efforts throughout the whole publication process of 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.

Al-Qerem, A., Alauthman, M., Almomani, A. et al. (2020) 'IoT transaction processing through cooperative concurrency control on fog-cloud computing environment', *Soft Computing*, Vol. 24, No. 8, pp.5695–5711.

Chhabra, M., Gupta, B. and Almomani, A. (2013) 'A novel solution to handle DDOS attack in MANET', *Journal of Information Security*, Vol. 4, No. 3, Article ID: 34631, DOI: 10.4236/jis.2013.43019.

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, DOI: 10.1109/ACCESS.2018.2800758.

Esposito, C., Ficco, M. et al. (2021) 'Blockchain-based authentication and authorization for smart city applications', *Information Processing & Management*, Vol. 58, No. 2, p.102468.

Gou, Z., Yamaguchi, S. et al. (2017) 'Analysis of various security issues and challenges in cloud computing environment: a survey', in *Identity Theft: Breakthroughs in Research and Practice*, pp.221–247, IGI Global, USA.

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*, p.e4946, DOI: 10.1002/cpe.4946.

Gupta, B.B. and Quamara, M. (2020) 'An overview of internet of things (IoT): architectural aspects, challenges, and protocols', *Concurrency and Computation: Practice and Experience*, Vol. 32, No. 21, p.e4946.

Gupta, B.B., Joshi, R.C. and Misra, M. (2012) 'ANN based scheme to predict number of zombies in a DDoS attack', *IJ Network Security*, Vol. 14, No. 2, pp.61–70.

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.

Gupta, S. and Gupta, B.B. (2015) 'PHP-sensor: a prototype method to discover workflow violation and XSS vulnerabilities in PHP web applications', in *Proceedings of the 12th ACM International Conference on Computing Frontiers*, May, pp.1–8.

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, USA.

Hossain, K., Rahman, M. and Roy, S. (2019) 'IoT data compression and optimization techniques in cloud storage: current prospects and future directions', *International Journal of Cloud Applications and Computing (IJCAC)*, Vol. 9, No. 2, pp.43–59.

Jiang, F., Fu, Y. et al. (2018) 'Deep learning based multi-channel intelligent attack detection for data security', *IEEE transactions on Sustainable Computing*, Vol. 5, No. 2, pp.204–212.

Pasupuleti, S.K. (2019) 'Privacy-preserving public auditing and data dynamics for secure cloud storage based on exact regenerated code', *International Journal of Cloud Applications and Computing (IJCAC)*, Vol. 9, No. 4, pp.1–20.

Psannis, K., Stergiou, C. et al. (2018) 'Advanced media-based smart big data on intelligent cloud systems', *IEEE Transactions on Sustainable Computing*, Vol. 4, No. 1, pp.77–87.

Stergiou, C. et al. (2018) 'Security, privacy & efficiency of sustainable cloud computing for big data & IoT', *Sustainable Computing: Informatics and Systems*, Vol. 19, pp.174–184, DOI: 10.1016/j.suscom.2018.06.003.

Stergiou, C.L., Psannis, K.E. et al. (2020) 'IoT-based big data secure management in the fog over a 6G wireless network', *IEEE Internet of Things Journal*, Vol. 8, No. 7, pp.5164–5171.

Zhang, Z., Sun, R., Zhao, C., Wang, J., Chang, C.K. et al. (2017) 'CyVOD: a novel trinity multimedia social network scheme', *Multimedia Tools and Applications*, Vol. 76, No. 18, pp.18513–18529.

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.