# Editorial

## Gulshan Shrivastava*

Department of Computer Science and Engineering,
National Institute of Technology Patna,
Ashok Rajpath Rd., Patna, Bihar 800005, India
Email: gulshanstv@gmail.com
*Corresponding author

## Sheng-Lung Peng

Department of Computer Science and Information Engineering,
National Dong Hwa University,
Hualien County, 974, Taiwan
Email: slpeng@ndhu.edu.tw

## Mitsunori Makino

Department of Information and System Engineering,
Chuo University,
Kasuga 1-13-27, Tokyo 112-8551, Japan
Email: makino.fme7@g.chuo-u.ac.jp

## Nguyen Gia Nhu

Department of Computer Science and Engineering,
Duy Tan University,
254 Nguyen Van Linh, Thanh Khe District, Danang, Vietnam
Email: nguyengianhu@duytan.edu.vn

**Biographical notes:** Gulshan Shrivastava received his BE in CSE from the MDU, India. He also earned his MTech in Information Security from AIT, GGSIPU Delhi, India and MBA in IT and Finance from PTU. He is currently pursuing PhD in CSE from NIT Patna, India. He is an editor/author of more than six books, ten book chapters and 35 articles in international journals and conferences of high repute including Elsevier, Inderscience, etc. He is also serving many repute journals as a guest editor, editorial board member, international advisory board, and reviewer board. His research interest includes information security, Android, data analytics, and computer networks.

Sheng-Lung Peng is a Professor at National Dong Hwa University, Hualien, Taiwan. He received his BS in Mathematics from the NTHU, and MS and PhD in Computer Science from National Chung Cheng University and National Tsing Hua University, Taiwan, respectively. He is now the Dean of the Library and Information Services Office of NDHU, an Honorary Professor of Beijing Information Science and Technology University of China, and a Visiting Professor of Ningxia Institute of Science and Technology of China. His research interests are in designing and analysing algorithms for bioinformatics, data mining and networks. He published over 100 international conferences and journal papers.

Mitsunori Makino is a Professor of the Department of Information and System Engineering, Chuo University, Japan. He received his BE, ME and DrE from the Waseda University, in 1987, 1989 and 1992, respectively. His major research interests are study on technology and system in computer graphics, virtual reality, augmented reality and visualisation. He has actively and globally been engaging in research, educational and social activities, such as the Editor-in-Chief of *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* in 2011–2013.

Nguyen Gia Nhu received his PhD in Mathematical for Computer Science from the Ha Noi University of Science, Vietnam National University, Vietnam. Currently, he is the Dean of the Graduate School – Duy Tan University, Vietnam. He has a total academic teaching experience of 19 years with more than 60 publications in reputed international conferences, journals and online

book chapter contributions (indexed by: SCI, SCIE, SSCI, Scopus, ACM DL and DBLP). His area of research includes healthcare informatics, network performance analysis and simulation, computational intelligence. Presently, he is an associate editor of the IGI Global: *International Journal of Synthetic Emotions (IJSE)*.

In the past decade, innovative computing services open a number of security and privacy issues and challenges that are becoming a key research area. The rapid advances in presence of information technologies, such as cloud computing, sensors, and internet of things (IoT), have played a significant role in the smart city context (Sinha et al., 2017; Gupta et al., 2018; Shrivastava and Kumar, 2017). The smart city contributes to enhancing the life services and process a large amount of data stream, which in turn raise the security and privacy concerns. However, handling security and privacy challenges are essential for a smart city that leads to the organisations to realise the new computing paradigms. Recently, we have been witnessing the numerous literature of security and privacy that includes end-to-end security, trustable data acquisition, transmission, processing, legitimate service provisioning, and privacy of personal data as well as the role of bio-inspired computing approaches in achieving system design and operations availability (Beng et al., 2018; Shrivastava, 2017; Miglani et al., 2017; Shrivastava et al., 2016). Furthermore, the use of bio-inspired computing techniques [evolutionary computation, particle swarm optimisation (PSO), ant colony optimisation, etc.] for intelligent decision support has been exploited to originate effectual computing systems. The concept of applying computational intelligence (CI) approaches in innovative computing analysis is feasible and sound. Moreover, CI and its associated learning paradigms have played vital roles in a large number of application areas related to security and privacy in information systems. CI paradigm consists of various branches that are not limited to expert systems, artificial immune system, swarm intelligence, fuzzy system, neural network, evolutionary computing and various hybrid systems, which are combinations of two or more of the branches. The goal of this special issue is to bring together the state-of-art research and development on CI approaches for security and privacy of innovative computing and secure innovative computing services, novel attacks on innovative computing services, and novel defences for innovative computing services attacks and innovative computing security analysis. We invite researchers to contribute original research articles as well as comprehensive review articles that will seek to understand the CI techniques leading to real-world innovative computing challenges and future improvements for security and privacy for fog and mobile edge computing services. In this special issue, we expect the original contributions focused on addressing the latest research, innovative ideas, challenges, and bio-inspired computing solutions in security and privacy aspects in the context of the smart city (Shrivastava et al., 2018; Sharma and Gupta, 2018).

The focal objective of the special issue on 'Recent advances in bio-inspired computing paradigms for security and privacy of innovative computing' is to provide insight mechanisms while handling innovative computing; provide conceptual understanding of machine to machine security issues, challenges and mechanisms; develop basic skills of bio-inspired secure innovative computing architecture and explain the theory behind the security of fog computing, IoT and different cryptographic algorithms. It also provides a forum for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns, practical challenges encountered and the solutions adopted in these fields.

The article 'An out-of-band mobile authenticating mechanism for controlling access to data outsourced in the mobile cloud environment' by Sumit Kumar Yadav, Nisha Saroha and Kavita Sharma identified the drawbacks of the current frameworks of mobile cloud computing (MCC), such as overloaded computations in key distribution, reduced flexibility, and scalability, are unable to achieve fine-graininess and confidentiality. Moreover, some are not even compatible with MCC environment due to their static nature. Thus, proposed an 'access control mechanism' which is lightweight with minimal computational overhead and provides fine-grained access control for sharing data using out-of-band (OOB) mobile authentication. In this, performed client-side encryption and decryption using simple hash functions and concatenation operator and achieve dynamic scalability.

In the article 'Parkinson's diagnosis using ant-lion optimisation algorithm' by Prerna Sharma, Rishabh Jain, Moolchand Sharma and Deepak Gupta proposed a novel approach, i.e., modified ant-lion optimisation (ALO) algorithm for detecting and diagnosing patients for Parkinson's disease at early stages. ALO is a recently proposed bio-inspired algorithm, which imitates the hunting patterns of ant-lions or doodlebugs proposed algorithm is used to find a minimum number of features that result in higher accuracy using machine learning classifiers. The algorithm has been used on Parkinson's speech dataset and Parkinson's voice dataset and results have been calculated on different classifiers. After the experiment analysis, the maximum accuracy achieved by the classifiers after optimal feature selection is 95.91%. Further, the modified binary ALO algorithm can be applied to other classification problems to predict the results with better accuracy with fewer computations than the other machine learning algorithms.

The article 'An improved chaotic-based African buffalo optimisation algorithm' by Chinwe Peace Igiri, Yudhveer Singh and Ramesh Chandra Poonia address the study enhances search mechanism of the African buffalo

optimisation (ABO) algorithm using a suitable chaotic function. The ABO is a metaheuristic algorithm that belongs to the swarm intelligence class of the bio-inspired algorithms. The foraging and defending characteristics of the African buffaloes that reside in the sub-Saharan of South and East Africa inspire the algorithm. The ABO algorithm has demonstrated significantly better performance than some well-known metaheuristics algorithm in the literature in N-P hard problems such as travelling salesman's problems. The proposed study reviews the weaknesses of the standard ABO algorithm and mitigates it using the chaotic logistic map. The chaotic improved ant-lion optimisation (CABO) is evaluated with nonlinear benchmark functions and compared with the standard ABO, PSO, and chaotic PSO algorithms. The CABO outperformed the three algorithms with 92% performance ratio. Two conclusive remarks are drawn from this research. First, the logistic map is the best chaotic strategy for the ABO algorithm. Second, CABO is recommended for real-world optimisation problems such as scheduling, supply chain management, and many more.

In the article 'Image integrity verification via reversible predictive hiding and elliptic curve Diffie-Hellman' by Siddharth Agarwal and J. Jennifer Ranjani explained that digital revolution has created a tremendous impact in almost every field including healthcare. Electronic patient records form the basis of e-healthcare systems and it enables medical practitioners from anywhere around the world to access a wide range of medical cases and its diagnosis. The World Wide Web facilitates faster distribution of data. At the same time, it paves the way for hackers to alter or modify crucial information. Hence, it is necessary to have a mechanism that ensures the authenticity or integrity of the data. Digital signatures are commonly utilised for integrity verification. In the proposed work, hash signatures are computed on the medical image to ensure its integrity. Transmission of digital signatures within the e-healthcare framework is error prone as there is no definite link established between the transmitting and receiving ends. This problem can be solved by embedding the digital signatures on the medical image. Reversible data hiding technique is used for hiding the signatures as the medical images cannot be discarded once the signatures are extracted. To ensure additional security, the data is hidden within the image blocks of uneven size which is randomly chosen. The seed of the pseudo random generator is communicated using the Diffie-Hellman key exchange algorithm. The digital signatures can be extracted at the receiving end and the integrity of the medical images can be easily verified.

The article 'Bio-inspired algorithms for diagnosis of breast cancer' by Moolchand Sharma, Shubbham Gupta, Prerna Sharma and Deepak Gupta discusses the most widely recognisable of all cancers found in women is breast cancer. It also happens to be the second most fatal among women with a growth rate of 12%. It is extremely important that breast cancer is diagnosed early, to ensure proper medication and survival of the patient. Various algorithms have been introduced so that accurate diagnosis can be made. However, all of them have failed to achieve the desired efficiency. This paper aims to present a comparison between different bio-inspired algorithms for breast cancer diagnosis. The algorithms have been used on Wisconsin Diagnostic Breast Cancer UCI Dataset and results have been calculated on different classifiers. After experiment analysis, we can observe that among these four optimisation methods, i.e., (BABCO, BACO, BFA and BPSO), binary PSO has shown maximum accuracy of 96.45% with random forest classifiers.

The article 'A robust approach to detect video-based attacks to enhance security' by Shefali Arora and M.P.S. Bhatia explained that face authentication has become an important part of real-world applications these days. In unconstrained environments, especially during video surveillance, it is important to ensure that such systems are secure. Spoofing attacks are common when it comes to authentication of individuals in video-based applications and surveillance activities. Replay attacks are one such kind of attacks, in which an attacker can intercept the data being transmitted and impersonate an individual to get unauthorised access to a system. This paper proposed an approach which involves the use of convolutional neural networks as well as long short-term memory networks to capture temporal information from video frames. This information is further used while extracting features from faces of individuals and the trained model can be further used to predict whether the system is under replay attack or not. Thus, only authentic users will get access to a system in activities that involve video surveillance or involve a video-based entry mechanism.

Ifra I. Khan, Khaleel Ahmad, M.A. Rizvi and Khairol Amali Bin Ahmad presented a new technique of image security is proposed using digital watermarking which is more efficient and robust than the existing technique of discrete wavelet transformation (DWT) through the article 'Increased PSNR with improved DWT digital watermarking technique'. It is focused on achieving a fast and secure system for transferring confidential information by embedding it in an image. The digital watermarking techniques used were DWT and least significant bit. Both techniques were utilised for their robustness and rapidity of image transformation. After applying the devised algorithm to program an interface was created that applied watermark and calculated PSNR. In order to prove its efficiency, the PSNR of several image transformations was created then its average was calculated. This proposed technique finds its application in various fields like medical imaging, forensic and data obfuscation. It helps in maintaining the confidentiality of the information stored in the image, also it is safe from any intersection or attack while the image is being transferred or on the network. Only intended users hold the key algorithm that reveals the hidden information to the receiver. This feature of the proposed technique helps in securing patient's data from being leaked to unsecured networks as the only key can make the information visible. So, the data security is

achieved in most vulnerable places where forensics and medical history of patients need to be confidential. Thereby, making the host image the safest way to securely carry and store the data in the system. Its use can be further extended in hiding information in other kinds of file formats and multimedia data like audio and video files.

The article 'Secure provenance-based communication using visual encryption' by Kukatlapalli Pradeep Kumar and Ravindranath C. Cherukuri consider the area of information security, protecting and safeguarding integrity and confidentiality of information is crucial. Tracking and storing the life cycle aspects of a data item is also an important factor. In this regard, a concept is proposed where security is provided through visual encryption. Tracking and storing the pedigree of data is seen through data provenance. Results are related to an implementation scenario where the information is communicated between two nodes in which the same is secured using visual encryption. Issues in communication are traced and recorded using data provenance related to troubleshooting issues. The outcome of the combination of concepts viz. visual encryption and data provenance gives an indigenous solution. The proposal of securing communication in the lines of visual cryptography associated with provenance is novel in this regard. Contributing to this approach, simulations, appropriate results and comparisons are made in the article. In connection with the two aspects, an extensive literature is also drafted with identified research gaps related to the approach on provenance and approaches on visual encryption mechanism. Use case model on the developed application is described using unified modelling language (UML). Provenance as a fundamental aspect could be seen in two ways: first is securing the provenance data, i.e., the sensitive data or to be specific the genesis data. Second is tracking the pedigree of life cycle events of a data item which can be used for troubleshooting in communication issues. In order to provide security, secret sharing mechanism (visual cryptography) is chosen instead of regular security algorithms.

Finally, as editors of this special issue, we would like to thank all the reviewers for their excellent work and the authors for their contribution. We expect that *IJICA* will provide the best platform for the authors and the readers, with a comprehensive overview of the most recent developments for security in network analytics and IoT research.

## References

Beng, T.C., Hijazi, M.H.A., Lim, Y. and Gani, A. (2018) 'A survey on proof of retrievability for cloud data integrity and availability: cloud storage state-of-the-art, issues, solutions and future trends', *Journal of Network and Computer Applications*, Vol. 110, pp.75–86, DOI: 10.1016/j.jnca.2018.03.017.

Gupta, R., Shrivastava, G., Anand, R. and Tomažič, T. (2018) 'IoT-based privacy control system through android', in *Handbook of E-business Security*, pp.341–363, Auerbach Publications, UK.

Miglani, A., Bhatia, T., Sharma, G. and Shrivastava, G. (2017) 'An energy efficient and trust aware framework for secure routing in LEACH for wireless sensor networks', *Scalable Computing: Practice and Experience*, Vol. 18, No. 3, pp.207–218.

Sharma, K. and Gupta, B.B. (2018) 'Taxonomy of distributed denial of service (DDoS) attacks and defense mechanisms in present era of smartphone devices', *International Journal of E-services and Mobile Applications (IJESMA)*, Vol. 10, No. 2, pp.58–74.

Shrivastava, G. (2017) 'Approaches of network forensic model for investigation', *International Journal of Forensic Engineering*, Vol. 3, No. 3, pp.195–215.

Shrivastava, G. and Kumar, P. (2017) 'Privacy analysis of android applications: state-of-art and literary assessment', *Scalable Computing: Practice and Experience*, Vol. 18, No. 3, pp.243–252.

Shrivastava, G., Sharma, K. and Kumari, R. (2016) 'Network forensics: today and tomorrow', *in 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, IEEE, March, pp.2234–2238.

Shrivastava, G., Sharma, K., Khari, M. and Zohora, S.E. (2018) 'Role of cyber security and cyber forensics in India', in *Handbook of Research on Network Forensics and Analysis Techniques*, pp.143–161, IGI Global, USA.

Sinha, A., Kumar, P., Rana, N.P., Islam, R. and Dwivedi, Y.K. (2017) 'Impact of internet of things (IoT) in disaster management: a task-technology fit perspective', *Annals of Operations Research*, pp.1–36, DOI : 10.1007/s10479-017-2658-1.