Editorial

Gulshan Shrivastava and Prabhat Kumar*

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

Manju Khari

Department of Computer Science and Engineering,
Ambedkar Institute of Advanced Communication
Technology and Research,
Geeta Colony, New Delhi, Delhi 110031, India
Email: manjukhari@yahoo.co.in

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 his PhD in CSE from NIT Patna, India. He is an editor/author of more than four books, nine book chapters and 30 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.

Prabhat Kumar is currently the Head of the department and Associate Professor in CSE at the NIT Patna, India. He was awarded with a PhD in the area of wireless sensor networks. He has published more than 60 research papers in international journals and conferences of high repute including IEEE, Elsevier, Inderscience, etc. He was also the Co-Chief Investigator of Project sponsored by the Ministry of Communication and IT, Govt. of India. Apart from the academic responsibilities, he is also the Professor-in-Charge of the IT services at the NIT Patna. His research area includes WSN, IoT, software engineering, e-governance, etc.

Manju Khari is an Assistant Professor from the Ambedkar Institute of Advanced Communication Technology and Research, under the Govt. of NCT Delhi, India. She is also the Professor-in-charge of the IT services of the institute. She obtained her PhD in CSE from the NIT Patna and MTech in Information Security from the AIT, GGSIPU Delhi, India. She has 70 published papers and six book chapters in refereed journals and conferences (viz. IEEE, ACM, and Elsevier, etc.). She is also the co-author of 2 books published by NCERT. Her research interest includes software testing, information security and nature-inspired algorithm.

In the past decade, the regular modernisation of business model has lead to increased dependence of organisations on information and communication technologies (Hazır et al., 2018). The revolutionary transformation in information management is making the organisations more realistic towards their objectives and hence, increasingly more strategically advanced. The data and information management in the antecedent business model was confined to a particular location and it was relatively easy to protect. The changing scope of information processing at independent locations has made it more difficult to maintain confidentiality, integrity and availability (Beng et al., 2018; Shrivastava, 2017; Miglani et al., 2017; Shrivastava et al., 2016). Even, the recent trends in global scenario necessitate an additional sense of responsibilities such as non-repudiation, authorisation and provenance. There is an imminent and increasing demand for internet of things (IoT) (Sinha et al., 2017; Gupta et al., 2018; Shrivastava and Kumar, 2017). Leveraging this blooming technology, one can envisage many changes in the internet world. Big data-based ICT penetration creates an ample number of job opportunities in the industrial sectors, especially for rural people. To describe common network vulnerabilities and attacks, defense mechanisms against network attacks and cryptographic protection mechanisms is also the need of hour (Shrivastava et al., 2018; Sharma and Gupta, 2018). Exploration of the requirements of real-time communication security and issues related to the security of web services is essential. This all relates to the exploration and exposition of the technologies and tools for enabling the extraction of timely and actionable insights from IoT data.

This special issue aims to provide insight mechanisms while handling data; provide a conceptual understanding of network security issues, challenges and mechanisms; develop basic skills of secure network architecture; and explain the theory behind the security of wireless networks, antennas, IoT and different cryptographic algorithms.

The article ‘A novel encryption compression scheme using Julia sets’ by Bhagwati Prasad and Kunti Mishra proposed a novel combined encryption with a lossless compression scheme and implemented it on some medical images. To deal with medical images and documents, lossless compression is necessary because in such type of cases loss of a single bit of information may be harmful. A novel technique for combined encryption and lossless compression of data is proposed in the present paper. The proposed method utilises the concept of a logistic map and Julia sets for image encryption and a number theoretic approach for lossless image compression. It provides excellent security with reasonable lossless compression ratio. This paper has implemented the proposed technique on some medical images, some of the images are depicted in the paper. Average compression ratio obtained for the medical images is reasonable. Moreover, key space for the given scheme is large enough to resist all type of brute force searches.

In the article ‘Perplexed Bayes classifier-based secure and intelligent approach for aspect level sentiment analysis’ by Sumit Kumar Yadav, Devendra K. Tayal and Shiv Naresh Shivhare reviews of an entity may be analysed based upon its various attributes. Machine learning techniques are commonly used for analysing such opinions. In this research work, first Naïve Bayes classifier is used to perform ABSA and dependence incapability of the classifier is predicted. Hence, it has been concluded that the Naïve Bayes classifier outperforms to classify such reviews. Naïve Bayes classifier is not ideal for predicting reviews when the features are correlated.

Further perplexed Bayes classifier has been explained and used. It is a novel mathematical model to correctly classify the input reviews which has no assumptions for

class conditional independence. Based upon testing of the perplexed Bayes classifier on a small set of data it is found that this classifier predicts correct sentiments of the reviews. Thus, it provides more assurance for the prediction over the Naïve Bayes classifier. In future, this tool can be used for various social media companies like Twitter, Facebook, etc. for opinion mining.

Med Karim Abdmouleh, Hedi Amri, Ali Khalfallah and Med Salim Bouhlel by the article 'An efficient crypto-compression scheme for medical images by selective encryption using DCT' present a new method of partial or selective encryption for medical images. The principle of this method is to combine the image encryption and compression. The new crypto-compression algorithm that significantly reduces the encryption and decryption time can assure a secure and an authentic transmission in medical image communication. It is based on the encryption of some quantified discrete cosine transform (DCT) coefficients in low and high frequencies. The results of several experiments show that the proposed scheme provides a significant reduction of the processing time during the encryption and decryption, without tampering the high compression rate of the compression algorithm.

The article 'Hybrid approach to enhance contrast of image for forensic investigation using segmented histogram' by Sachin Dube and Kavita Sharma addresses the problem of visual image analysis for forensic investigation. An image often needs enhancement to make it suitable for forensic analysis and highlight minute details which are not visible otherwise. For this purpose, various techniques have been suggested; histogram equalisation (HE) is one such technique that uses information from the image histogram for contrast enhancement. However, HE fails badly in the presence of spikes and gives noisy output. Presence of large areas having pixel values in a small range leads to spike generation in the histogram. To deal with spikes; location of significant valleys and peaks is calculated to further segment image histogram. Segmented histograms are then equalised individually and combined to give a complete and equalised histogram. Using this enhanced histogram resultant image is generated. Apart from equalisation authors have performed black and white stretching to increase dynamic range further. They performed a subjective and objective assessment to show the superiority of the proposed method. For objective assessment performance measures like peak signal to noise ratio (PSNR), absolute mean brightness error (AMBE), entropy and standard deviation were used. Experiments were conducted on standard images like Lena, Cameramen, Max, etc.

In the article 'Use of 'A light weight secure image encryption scheme based on chaos and DNA computing' for encrypted audio watermarking' by Bhaskar Mondal, Tarni Mandal, Tanupriya Choudhury and Danish Ali Khan presented encryption algorithm that based on the chaotic map and DNA computation. The complexity of the chaotic map and DNA computation are very low which makes the encryption scheme a lightweight process, but the test results show that the encryption scheme has a powerful encryption effect. In the proposed scheme the watermark data is encrypted first using the encryption algorithm and then embedded on to the cover media that is audio. For this purpose, the cover audio is divided into frames using DCT and the frames are shuffled randomly. Next, discrete wavelet transformation (DWT) is applied to the randomly shuffled frames and then the pre-encrypted watermark data is embedded on to it. In this technique, it's become harder for the unauthenticated users to read the watermark data and reveal the correct source of the media as the watermark data is encrypted. Therefore, this scheme helps the sender to hide his or her identity from the unintended users. On the

other hand, an authenticated user can reveal the watermark data to authenticate the source. The experimental results show that the scheme is secure and effective.

Ekta Gandotra, Divya Bansal and Sanjeev Sofat focus on the increasing complexity and severity of malware through article 'Malware intelligence: beyond malware analysis'; it is essential for security organisations to change their approach from reactive to proactive. It can be achieved by extending security models to provide real-time intelligence by trends in historical and current malware behaviours. This paper performs a comprehensive statistical analysis of static and dynamic attributes of about 0.1 million historical malware specimens over the years 2004 to 2015. These include file size of malicious binaries, suspicious sections, network activities, file system activities, registry activities, etc. The intelligent information obtained from such analysis helps to get insight into the future behaviour of malware. The trends and insights ascertained from the analysis are used to identify the malware related research challenges and future research directions. The intelligent information obtained from this type of analysis can be shared with security experts, computer emergency response teams (CERTs) and other stakeholders so that they can issue early warnings and the corresponding remedial actions to deal with future threats from malware. Further, this type of analysis has the potential to facilitate researchers in selecting the parameters/features for designing faster and improved techniques for detecting unknown malware.

The article 'Trust evaluation of websites: a comprehensive study' by Himani Bansal and Shruti Kohli discusses the importance of checking the credibility of online information before using it, especially for sensitive purposes like health. They have collected a vast amount of data to testify the model conceived by them for quantising trust in the informational websites. The beauty of the model lies in the fact that by using human behaviour (non-quantifiable construct), they have quantised trust (again, a non-quantifiable construct) for informational websites. The model is implemented by them and has given good results as compared to existing trust calculating tools.

Rudra Pratap Ojha, Kavita Sharma, Pramod Kumar Srivastava and Goutam Sanyal proposed model is susceptible-exposed infectious quarantined recovered with vaccination (SEIQRV) in the article 'An epidemic model for security and performance of wireless sensor networks'. The effect of various states has been discussed. The exposed state is used to detect the presence of a worm in the network at an early stage and remove it from WSNs. Exposed nodes take some time to become infectious node during that time worm can be removed. Quarantined is used to isolate the highly infectious nodes from the network and stop the malicious signals transmission in the WSNs. The worm can be easily removed from the remote sensor nodes without any overhead. The vaccinated state prevents the early attacks on sensor nodes.

The article 'Secure handoff technique with reduced authentication delay in wireless mesh network' by Geetanjali Rathee and Hemraj Saini proposed a secure handoff mechanism where a trusted third party, i.e., an authentication server is responsible for verifying the roaming mesh clients in WMN. The authentication server authenticates the mesh clients by generating and updating the tickets by looking over the entire network after a specific interval of time. The paper's potential contribution is to describe the following aspects:

1 ticket generation phase that is needed to create the tickets and keys between the nodes

2 handoff authentication phase that explains the handoff verification of mobile clients.

The authentication process delay of the proposed mechanism is analysed under different probabilistic scenarios using the NS2 simulator. Further, an empirical study is done against certain security attacks to prove the legitimacy of the mechanism. The proposed mechanism significantly resolved the issue of storage overhead and security threats such as black hole and wormhole attacks during the clients roaming. Moreover, the proposed mechanism illustrates better results against measuring parameters of maximum and average authentication delay.

K. Srinivasa Reddy and S. Ramachandram presented a novel order-preserving encryption scheme called SCOPE through the article 'A secure, fast insert and efficient search order preserving encryption scheme for outsourced databases'. It is considerably more secure and efficient than existing OPE schemes. New definition for order-preserving security called IND-OCRPDA and probably shown that SCOPE is secure under that definition. Intuitively, SCOPE leaks nothing beyond the order of values. This is a breakthrough given that existing OPE schemes leak additional information. Query rewrite method (QRM) is introduced using QRM; SCOPE can effectively process many classes of queries including queries with range predicates, joins, and group aggregation. SCOPE supports SUM/AVG aggregate functions, which other OPE schemes would not. This experiments that SCOPE is hugely faster than mOPE and has a reasonable overhead which is 3.5 when compared with plain data and is acceptable. The proposed model shows a single user setting where the client has complete access to the query result.

The article 'Security model against worms attack in wireless sensor network' by Rudra Pratap Ojha, Pramod Kumar Srivastava and Goutam Sanyal consider the case when two types of worms present in the network simultaneously. The model is formulated using the concept of an ordinary differential equation (ODE) and studied the behaviour of WSN. The one infected node is enough in WSN to destroy the network because worm spread through neighbouring nodes. The proposed model has the six states susceptible-exposed class with short latent period-exposed class with a long latent period infectious recovered vaccination. The latent period is a time in which exposed nodes converted into infectious state. The short latent period types of nodes become infectious quickly in comparison to a long latent period. The proposed model helps in the study of the dynamic behaviour of worm propagation in WSN. The primary reproduction number of the proposed model has been obtained. This is borrowed from biomathematics. The primary reproduction number determines that the network must be stable in the worm-free state when its value is less than equal to one or when its value is higher after than the network must be stable in the endemic state. The effect of the different exposed class has been studied. The effects of recovery and vaccination have been analysed. This is found that when the rate of vaccination is a high minimum number of nodes get infected. The proposed model is verified by simulation results using MATLAB.

The article 'Untraceable privacy-preserving authentication protocol for RFID tag using salted hash algorithm' by Pinaki Ghosh and T.R. Mahesh proposed a new approach for RFID security which includes tag untraceability and a privacy-preserving authentication. The proposed protocol is a mutual authentication protocol, which authenticates the tag as well as the reader. The author uses a salted hash algorithm to implement this protocol. Nowadays, RFID communication is becoming an essential technique for short-range communication like user verification, inventory, passports, etc. Because of the openness in nature, these systems suffer from various attacks like privacy,

forgery and traceability. The author solves the privacy issues and traceability through this paper. Apart from the privacy-preservation and untraceability this protocol also solves attacks like location tracking, replay and man-in-the-middle. The author also compared this method with some of the existing methods and proved it best among them.

Seema Verma and Manoj Kumar explored the article 'Comparison of different RSA variants'. As RSA is the first and well known public key cryptosystem, it always remains the centre of attraction for the research. The simplicity of the algorithm mainly forms the base for its cryptanalysis. In this article, RSA cryptosystem is studied in detail with its complexity analysis. Various variants of RSA are studied and analysed regarding performance and security.

In the article 'GASER: genetic algorithm-based secure and energy aware routing protocol for sparse mobile ad hoc networks' by Deepika Kukreja, Deepak Kumar Sharma, S.K. Dhurandher and B.V.R. Reddy explored a novel routing protocol for sparse mobile ad hoc networks is proposed that is based on nature-inspired genetic algorithm technique. Sparse mobile ad hoc networks are a type of delay tolerant networks (DTN) that are characterised by sparse nodes' deployment and longer network partitions. Nodes in sparse ad hoc environment have limited battery power; they keep on moving in the network, sometimes they do not come in contact with the other network nodes for a longer period. Further, there are few nodes in the network which behave maliciously to save their energy and they do not relay packets to their neighbouring nodes. This type of behaviour exhibited by nodes makes the network operations especially routing more complex. The existing protocols in this area often cause the faster depletion of nodes' battery power for determining the route between the source and the destination. In the proposed work, an energy aware routing protocol is implemented for these types of environments. GASER determines a secure route for data transmission which is free from the nodes that drop data packets, the determined route is shortest and the nodes' power consumption is minimal.

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 *IJAIP* 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.

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.

Hazır, C.S., LeSage, J., and Autant-Bernard, C. (2018) 'The role of R&D collaboration networks on regional knowledge creation: evidence from information and communication technologies', *Papers in Regional Science*, Vol. 97, No. 3, pp.549–567.

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 [online] https://doi.org/10.1007/s10479-017-2658-1.