Editorial

Brij Booshan Gupta*

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

Shingo Yamaguchi

Graduate School of Science and Engineering,
Yamaguchi University,
Yamaguchi 753-8511, Japan
Email: shingo@yamaguchi-u.ac.jp

Biographical notes: Brij Booshan 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 140 research papers in international journals and conferences of high repute. His biography was selected and published in the 30th edition of *Marquis Who's Who in the World*, 2012. He is a senior member of IEEE, and a member of ACM, SIGCOMM, etc. His research interest includes information security, cyber security, mobile/smartphone, cloud computing, web security, intrusion detection, computer networks and phishing.

Shingo Yamaguchi is a Professor in the Graduate School of Science and Engineering, Yamaguchi University, Japan. He received his BE, ME and DE degrees from the Yamaguchi University, Japan, in 1992, 1994 and 2002, respectively. He has published almost 100 transactions, proceedings, and survey papers of IEEE, IEICE, etc. He was a Conference Chair of IEEE International Conferences, such as GCCE 2014 and GCCE 2015. He is currently the Chapter Chair of IEEE Consumer Electronics Society, West Japan Joint Chapter. He is an area editor of IEICE *Transactions on Fundamentals of Electronics, Communications and Computer Sciences*. He is a senior member of IEEE and IEICE.

Today, we are more and more dependent on information technology and services as they pervade every aspect of our lives. However, cyber security, analytics and human factors in information technology play an important role in the development of superlative organisations where new technologies and applications are put into the practice to strengthen everyday business processes (Stergiou et al., 2018; Gupta et al., 2016; Alomari et al., 2016). A reliable information technology system requires a solid security framework that ensures confidentiality, integrity, availability, and authenticity of the organisation's critical assets (Tewari and Gupta, 2017a, 2017b; Gupta and Akhtar, 2017; Zhang and Gupta, 2016). In this special issue on advances in cyber security, analytics and human factors in IT, we have accepted seven papers that address such issues (Alomari et al., 2012; Elmisery et al., 2017; Adat et al., 2017).

The first article, entitled 'An intelligent paradigm for denoising motion artefacts in ECG preprocessing: smart filters' co-authored by M. Arumugam and A.K. Sangaiah, presents a novel smart filter for filtering the main noise signals that distort the original ECG signal. The main noise signals are identified as power line interference, baseline wander and electromyography. Moreover, the proposed filter design is compared in terms of signal to noise ratio and power spectral density. Further, as indicated by the authors, the comparison result indicates that the proposed filter design has a good response characteristic for noise filtration. The eradication of these noise signals helps to achieve correct identification of heart disease and makes the life of physicians easier.

The second paper, entitled 'An efficient ternary tree-based TGDH protocol for dynamic secure group data sharing in cloud computing' authored by V.R. Thakare and K.J. Singh, presents a TGDH ternary tree-based secure group-sharing framework. TGDH with a ternary tree-based approach is more efficient than the binary tree approach in terms of strength of members in a subgroup, and the height of the binary tree increases when the number of members in a group increases, where the height of the tree is the number of iterations required to compute the group shared key. Similarly, computation and communication cost also increases when the number of members of a group increases proportionally. Furthermore, as mentioned by the authors, to show the strength of the proposed framework, the statistical comparison with existing TGDH protocol is shown. Finally, the extensive simulation results with CloudSim tool are shown to demonstrate the resource use by each member,

VM allocation, cloudlets allocation and execution time of proposed construction.

The third paper, entitled 'Privacy preserving secret key extraction protocol for multi-authority attribute-based encryption techniques in cloud computing' authored by P.G. Shynu and K.J. Singh, presents a privacy preserving secret key extraction protocol, which stores user attributes in a fuzzy attribute set format over the hash index. The hash index acts as a unique identity that enables easier extraction of the secret key from outsourced user attributes and it eliminates the need for the involvement of a central authority for user attribute management processes. The authors indicate that this work is implemented using charm crypto, an extensible framework for rapid prototyping system. The experimental results show that the proposed scheme provides higher levels of user access provision with improved security and privacy properties in comparison with existing MA-ABE techniques.

The fourth paper, entitled 'Automated identification of callbacks in Android framework using machine learning techniques', is authored by X. Chen et al. In this paper, authors present a machine learning approach to identifying callbacks automatically in the Android framework. As long as there is a training set of hand-annotated callbacks, the proposed approach can detect all of them in the entire framework. The authors mention that a series of experiments are conducted to identify 20,391 callbacks on Android 4.2. This proposed approach, verified by a ten-fold cross validation, is effective and efficient in terms of precision and recall, with an average of more than 91%. The evaluation results show that many of newly discovered callbacks are indeed used, which furthermore confirms that the approach is suitable for all Android framework versions.

The fifth paper, entitled 'Recovering multiple versions of YAFFS2 files based on Hash and timestamps' authored by Y. Li et al., present a new method based on the notions of hash and timestamp to recover multiple versions of YAFFS2 files during which the relationship between timestamps and file operations are analysed. To verify the effectiveness of the proposed method, the authors simulated a NAND chip under Linux and performed some experiments to show that the proposed method is both effective and efficient in the recovery of multiple versions of different types of YAFFS2 file as well as Android images.

The sixth paper, entitled 'A framework and a process for digital forensic analysis on smart phones with multiple data logs' authored by E. Benkhelifa et al., present a framework solution, which could contribute to the development of a novel and potentially market-leading mobile forensic tool. The authors claim that the proposed framework maps data from different sources including calls, geographical location, multimedia, and web logs.

The seventh paper, entitled 'Token security for internet of things' authored by S. Narendrakumar et al., presents a two-factor verification and authentication method involving hashing to secure the tokens issued for the connection. The security is provided at the identity provider layer that works on the TCP/IP layer. First, the authentication and authorisation are confirmed through two-way authentication, and the token is generated by the relying party. Since the generated token has a threat of guessing or cryptanalysis attack, the authors worked on making it more secure by using the cryptanalytics process. The cryptanalytics process is accomplished through the addition of logical operation of the token with OTP and hashing before sending the token to the user and service provider.

This special issue is due to the encouragement of Prof. Kuan-Ching Li, who was 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 schedules to review the articles submitted. This special issue presents some selected papers in touching important aspects, state-of-the-art research paradigms and on recent advances in cyber security, analytics and human factors in IT and also emphasises many open questions. The various security issues, analytics and human factors in IT are encouraging researchers to look at various open questions and a lot more work needs to be done to ensure security against cyber threats to the user community.

References

Adat, V. et al. (2017) 'Security in internet of things: issues, challenges, taxonomy, and architecture', *Telecommunication Systems*, Vol. 67, No. 3, pp.423–441, Springer.

Alomari, E. et al. (2012) *Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art*, arXiv preprint arXiv:1208.0403.

Alomari, E., Manickam, S. et al. (2016) 'A survey of botnet-based DDoS flooding attacks of application layer detection and mitigation approaches', *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*, IGI-Global's Advances in Information Security, Privacy, and Ethics (AISPE) series, USA.

Elmisery, A.M., Sertovic, M. and Gupta, B.B. (2017) 'Cognitive privacy middleware for deep learning mashup in environmental IoT', *IEEE Access*, Vol. 6, No. 1, pp.8029–8041, DOI: 10.1109/ACCESS.2017.2787422

Gupta, B.B. and Akhtar, T. (2017) 'Survey on smart power grid frameworks, tools, security issues and solutions', *Annals of Telecommunication*, Vol. 72, Nos. 9–10, pp.517–549, Springer.

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.

Stergiou, C. et al. (2018) 'Secure integration of IoT and cloud computing', *Future Generation Computer Systems*, Vol. 78, No. 3, pp.964-975.

Tewari, A. and Gupta, B.B. (2017a) 'A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices', *International Journal of Advanced Intelligence Paradigms*, Vol. 9, Nos. 2–3, pp.111–121.

Tewari, A. and Gupta, B.B. (2017b) 'Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags', *Journal of Supercomputing*, Vol. 73, No. 3, pp.1085–1102, Springer.

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