Editorial

Mu-Yen Chen*

Department of Engineering Science,
National Cheng Kung University,
No. 1, University Road, Tainan City 701, Taiwan
Email: mychen119@gs.ncku.edu.tw
*Corresponding author

L. Mary Gladence

Sathyabama Institute of Science and Technology,
Jeppiaar Nagar, SH 49A, Chennai, Tamil Nadu 600119, India
Email: marygladence.it@sathyabama.ac.in

Hsin-Te Wu

Department of Computer Science and Information Engineering,
National Taitung University,
369, Sec. 2, University Rd., Taitung 950309, Taiwan
Email: wuhsinte@nttu.edu.tw

Biographical notes: Mu-Yen Chen is working as a Professor at the National Cheng Kung University, Taiwan. He is the 2% top highly cited researcher by Stanford University (in artificial intelligence field). His current research interests include artificial intelligence, machine learning, deep learning, soft computing, with more than 200 publications in prestigious venues such as *IEEE Transactions on Fuzzy Systems*, *IEEE IoT*, *IEEE TII*, *IEEE Sensors*, *IEEE Access*, *ACM Transactions on Internet Technology*, *Applied Soft Computing*, *Soft Computing*, *Neurocomputing*, *Computer Networks*, and *FGCS*. He has served as the Editor-in-Chief on *International Journal of Big Data and Analytics in Healthcare*, and several SCI journals.

L. Mary Gladence is a Professor in the School of Computing, Sathyabama Institute of Science and Technology, Chennai, India. Her research interests include deep learning, artificial intelligence, data mining, sequential pattern Mining, pattern recognition, machine learning, bio computing, data analytics, with more than 60 publications in these areas. She has served as a co-convener in the International Conference on Artificial Intelligence and Machine Learning and has been a guest editor and reviewer in refereed international journals like *Cloud Computing*, *IEEE Access*, *Library Hi-Tech*, *Cluster Computing*, *Super Computing*, *Journal of Medical and Biological Engineering*, *Computer Communications*, etc.

Hsin-Te Wu received his PhD in Department of Computer Science and Engineering from the National Sun Yat-Sen University, Taiwan, in 2013. He is an Associate Professor of Department of Computer Science and Information Engineering from the National Taitung University, Taiwan. He has served as an associate editor for *International Journal of Big Data and Analytics in Healthcare*. He has served as a special issue guest editor of *Journal of*

Supercomputing and *IET Networks*. His research interests include computer networks, wireless network, speech compression, network security, blockchain and internet of things.

1 Introduction

Emerging technology facilitates life convenience and economic development; however, the data collected by the technology sometimes conceal severe information security vulnerability. To the implementation of the internet of things (IoT), it will distribute tremendous sensors to collect data through peer-to-peer communication; without adequate protection, the data will be missing effortlessly. Additionally, IoT devices do not possess the capacity to conduct security update automatically, which means hackers will sneak into the system if the system has any vulnerability. In recent years, many enterprises use IoT devices to do personal identification or data access. Without the technique of cryptography, it becomes straightforward for hackers to break in when accessing personal data. The technology of blockchain can improve the non-repudiation and integrity issues for IoT when collecting data. Moreover, using the distributed ledger technology of blockchain can avoid centralised databases suffering from denial-of-service attack; uses can verify the data in the blockchain.

Currently, the data in smart health systems are considered vital personal data; therefore, to verify or access data should process through identification for legal users to utilise the data. Today, the global trend is to promote fifth generation network (5G) and intelligent green communication networks proactively; through the high transmit speed and low latency Internet to transfer data and use intelligent sleep mode to decrease energy consumption. On the other hand, green communication networks are capable of maintaining a balance between Internet performance and energy consumption by using small cells to deliver data. Nonetheless, we should not neglect the protection of cybersecurity as it remains an issue, such as the situations of stealing data and denial-of-service attacks. Hence, it requires relevant research and discussions regarding the security of 5G networks and intelligent green communication networks. In advance of emerging technology, although the combination of different technologies can boost user convenience and economic opportunities, the issues of data protection, identification, and privacy are critical questions. Consequently, the security solutions from the MAC layers to application layers can reduce the risks of data stealing and cyberattack.

The special issue has attracted many experts and researchers in the fields of communications networks and information technology to present more solutions with better effectiveness for the security and privacy of emerging technology.

2 Papers in the issue

Narengbam and Dey (2024) integrated the Harris Hawks optimisation (HHO) with a sigmoid neuron network (SN) to improve the anomaly-based intrusion detection systems (ADS) performance. This research underscores the potential synergy of meta-heuristic optimisation and artificial neural networks (ANNs), providing a bright strategy to reinforce the IDS performance and reliability.

Deng (2024) adopted the multi-agent approach to develop the secure payment model of e-commerce under the blockchain mechanism. The experimental results proven the proposed model can both enhance the information security and own the advantages of the blockchain capabilities.

Liu and Ma (2024) integrated the IoT, blockchain, ant colony optimisation (ACO), and ANN to build an enterprise IoT-based security management system (SMS). The experimental results showed the proposed SMS can improve the speed and security of data transactions and network security in the enterprise operation.

Li et al. (2024) developed the ciphertext-policy attribute-based encryption (CP-ABE) model of the information centre to enhance the data encryption of IoT-based enterprises. Finally, the proposed model can enhance the core competitiveness of supply chain transformation in the IoT-based enterprises and deal with the rapid development of information security environment.

Zhang et al. (2024) designed and implemented an enterprise intelligent financial sharing mechanism under the IoT environment to address the security issue. By reviewing the sharing mechanism, critical issues such as security, privacy protection, and data governance can be investigated, and then providing theoretical guidance for constructing the trustworthy and reliable sharing mechanisms.

Jiang and Wu (2024) developed a distributed training scheme under fog computing of the competitive differences in bilateral platforms based on AI and network data security. This scheme can be a reference for data collection, storage, and processing while merging the stringent measures for data encryption, identity authentication, and access control.

Rimani et al. (2024) proposed a novel cryptosystem by block depended on the secret key and subkeys to deal with the modern cryptography for encrypting images. The experimental results showed the high security of the proposed cryptosystem with random, nonlinear, dynamic and secret scrambled (RNDSS) technique and guaranteed the security against brute force attacks.

Xiong and Wang (2024) designed a library data protection mechanism and developed a threat detection system by using encryption algorithms. The experimental results demonstrated that the average response time of unknown threats was from 0.4 s to 0.8 s in the proposed system based on network security protection. This research can improve the users' trust and users' usage experience, further promote the development of the library applications and the improvement of service quality.

3 Conclusions

We would like to thank all the contributors of this special issue for their remarkable participation and efforts. Last but not least, we deeply appreciate the Editor-in-Chief, Professor Biju Issac, with his kind encouragement for this special issue. We believe that readers of IJICS and scholars researching in the security and privacy for emerging technology will find this special issue of novel academic contributions and industry practices.

References

Deng, L. (2024) 'Multi-agent secure payment model of e-commerce based on blockchain perspective', *Int. J. Information and Computer Security*, Vol. 24, Nos. 1/2, pp.28–43.

Jiang, J. and Wu, Y. (2024) 'Analysis of competitive differences in the bilateral platforms of the digital economy using artificial intelligence and network data security', *Int. J. Information and Computer Security*, Vol. 24, Nos. 1/2, pp.98–116.

Li, Z., Kong, X. and Jiang, X. (2024) 'The relationship between digital information security of the supply chain and enterprise development', *Int. J. Information and Computer Security*, Vol. 24, Nos. 1/2, pp.60–79.

Liu, J. and Ma, H. (2024) 'The optimisation of enterprise internet of things security management system under digital economy', *Int. J. Information and Computer Security*, Vol. 24, Nos. 1/2, pp.44–59.

Narengbam, L. and Dey, S. (2024) 'Anomaly-based intrusion detection system using Harris Hawks optimisation with a sigmoid neuron network', *Int. J. Information and Computer Security*, Vol. 24, Nos. 1/2, pp.5–27.

Rimani, R., Ali-Pacha, A. and Hadj Said, N. (2024) 'Encryption by block based on rekeying and inter-intra pixel permutation', *Int. J. Information and Computer Security*, Vol. 24, Nos. 1/2, pp.117–136.

Xiong, J. and Wang, X. (2024) 'Library data protection and threat detection system based on network security', *Int. J. Information and Computer Security*, Vol. 24, Nos. 1/2, pp.137–153.

Zhang, Y., Zhang, X. and Song, J. (2024) 'Enterprise intelligent financial sharing mechanism in the security environment of the internet of things', *Int. J. Information and Computer Security*, Vol. 24, Nos. 1/2, pp.80–97.