Ann. Telecommun. (2017) 72:513–515
DOI 10.1007/s12243-017-0607-2

EDITORIAL

Editorial security, privacy, and forensics in the critical infrastructure: advances and future directions

B. B. Gupta[1] · Dharma P. Agrawal[2] · Shingo Yamaguchi[3] · Nalin A. G. Arachchilage[4] · Suresh Veluru[5]

Cyber security and privacy are essential for modern society where information technology and services pervade every aspect of our lives. Especially security, privacy, and forensics of critical infrastructure (i.e., a nation's strategic national assets; i.e., banking and finance, communications, emergency services, energy, food chain, health, water, mass gatherings, and transport) which is an essential part of our daily lives to access different systems, services, and applications are a serious issue today. However, it is challenging to achieve, as technology is changing at a rapid speed and our systems turning into ever more complex. Security and privacy of critical infrastructure networks will not only allow the achievement of a properly functioning economy market but will also enhance the security of energy supply, enable market integration, and allow consumers to benefit from new technologies. The success in protecting any country's critical infrastructure requires the involvement of every element of the infrastructure in the definition and implementation of a risk management program, incorporating analysis of the vulnerabilities, risk assessment, and implementation of hazard mitigation procedures. Furthermore, Diane Van de Hei, executive director of the Association of Metropolitan Water Agencies and contact person for the water utility Information Sharing and Analysis Center (ISAC), was quoted as saying, "If we had so many dollars to spend on a water system, most of it would go to physical security" [1–4].

These considerations have led to this special issue as a venue for critical infrastructure security researchers around the world to share their state-of-the art research and development that could be beneficial to protect the critical infrastructure of a nation. Specifically, this special issue addresses various security, privacy, and forensics issues in critical infrastructure, particularly on advances of computing technologies and related areas [5–9]. This has helped us to collect high-quality articles that reported recent research advances regarding security, privacy, and forensics issues in the critical infrastructure, covering various topics of interest.

This special issue contains nine papers dealing with different aspects of security, privacy, and forensics issues in critical infrastructure and other related areas [10–12]. The first article entitled, "A survey on smart power grid: frameworks, tools, security issues and solutions" authored by B. B. Gupta et al. presents a comprehensive survey on understanding the smart power grid, its important components, different cyber security, and other kinds of issues, existing methodologies, and approaches for communication protocols, and the architecture of smart power grids. The authors conclude this paper by discussing various research challenges that still exist in the literature, which provides a better understanding of the problem, the current solution space, and future research directions to defend smart power against different cyber-attacks.

The second paper entitled "Towards a set aggregation-based data integrity scheme for smart grids," authored by Mouzna Tahir et al. presents a novel method based on hash-chaining to verify the integrity of a set of aggregated data. This scheme divides the user's data into two diverse groups. It also enables the control center to collect more fine-grained data aggregation results at a reduced cost. In addition, the proposed scheme ensures data integrity by maintaining a hash chain and

✉ B. B. Gupta
bbgupta@nitkkr.ac.in

[1] National Institute of Technology Kurukshetra, Kurukshetra, India

[2] University of Cincinnati, Cincinnati, OH, USA

[3] Yamaguchi University, Yamaguchi, Japan

[4] University of New South Wales, Sydney, Australia

[5] United Technologies Research Centre, Ireland, UK

assigning new values in the hash chain by XORing previous hash values with the current hash value. The proposed scheme is evaluated in terms of computational cost and communication overhead. A comparative analysis of this proposed methodology with existing aggregation schemes regarding computational cost and communication overhead illustrates the optimality of this proposed scheme.

The third paper entitled "Cryptanalysis and improvement of certificateless proxy signcryption scheme for e-prescription system in mobile cloud computing", authored by T. Bhatia et al., presents a novel pairing-free certificateless proxy signcryption scheme using elliptic curve cryptography (ECC) for e-prescription system in mobile cloud computing. The authors claim that the proposed scheme is proven to be secure against indistinguishability under adaptive chosen ciphertext attack and existential forgery under adaptive chosen message attack in the random oracle model against type 1 and type 2 adversaries through formal analysis. The proposed scheme outperforms the existing schemes in terms of computational efficiency making it suitable for futuristic mobile cloud computing applications.

The fourth paper entitled "Preserving patients' privacy in health scenarios through a multicontext-aware system" is authored by Alberto Huertas Celdrán et al. In this paper, the authors present an approach for the preservation of patients' privacy in a health scenario through a multicontext-aware system called h-MAS (health-related Multicontext-Aware System). h-MAS is a privacy-preserving and context-aware solution for health scenarios with the aim of managing the privacy of the users' information in both intra- and inter-context scenarios. In a health scenario, h-MAS suggests a pool of privacy policies to users, who are aware of the health context in which they are located. Users can update the policies according to their interests. These policies protect the privacy of the users' health records, locations, as well as context-aware information being accessed by third parties without their consent. The information on patients and the health context is managed through semantic web techniques, which provide a common infrastructure that makes it possible to represent, process, and share information between independent systems more easily.

The fifth paper entitled "Universal half-blind quantum computation," authored by Xiaoqing Tan et. al., devises a simple protocol. A client delegates his or her quantum computation to a remote server in accordance with the inputs and instructions. Alice, the client, has a classical computer or limited quantum technologies, and these are not sufficient for the universal quantum computation at her disposal. Bob, the server, owns a fully-fledged quantum computer and promises to execute the computation honestly. The protocol itself is half-blind, that is, Bob may learn which quantum gate he implements but nothing about Alice's inputs and outputs. Furthermore, Alice is only required to send qubits and perform Pauli gates. Finally, the authors analyze the security, universality, half-blindness, and correctness, and briefly discuss its defects, extension, and verification.

The sixth paper entitled "Horizon: A QoS management framework for SDN-based data center networks", authored by Junjie Pang et al., presents the problem of data center operations and management as a new type of QoS that is the foundation of user-centric QoS implementation. The authors also define the quality of network service in a Software-Defined Networking (SDN)-based DCN and develop a framework called Horizon as the architecture of their QoS solution. This framework comprises a Markov-process-based method to predict link popularity, and authors use SDN technology to monitor network status. The authors have implemented the proposed method, and the experimental results indicate that Horizon can relieve congestion in DCNs to meet QoS requirements. The experimental results show that the proposed approach has a similar performance to the optimal solution. When compared with the ECMP approach, the proposed approach has a much lower latency. The results also show that the proposed approach is effective in terms of network congestion control.

The seventh paper entitled "An android malware dynamic detection method based on service call co-occurrence matrices," authored by Chundong Wang et al., proposes a new Android malware identification method. This method extracts the feature of Android system service call sequences using a co-occurrence matrix and uses machine-learning algorithm to classify the feature sequence and to verify whether this feature sequence can expose Android malware behaviors or not. By using 750 malware samples and 1000 benign samples, this paper has designed an experiment to evaluate this method. The results show that this method has a high detection precision rate (97.1%) in the best case and a low false-positive rate (2.1%) in the worst case based on the system service call co-occurrence matrix.

The eighth paper entitled "Multi-user searchable encryption with a designated server," authored by Zhen Li et al., presents a secure channel-free and TTP-free MSE scheme. It is secure against keyword guessing attack by introducing a designated server. Moreover, it achieves fine-grained access control to grant and revoke the privileges of users without TTP. More specifically, each document is encrypted with a unique and independent key, where the key distribution is integrated with user authorization and search procedures. The authors claim that they provide a concrete construction of the scheme and give formal proofs of its security in the random oracle model.

The ninth paper entitled "An improved tracking algorithm of floc based on compressed sensing and particle filter", authored by Xin Xie et al., proposes an improved algorithm combining particle filter (PF) with compressed sensing (CS). The feature of flocs image is extracted via CS theory, which is used to detect the single-frame image and get the detection value. Simultaneously, the optimal estimation of particle in the space model of non-linear and non-Gaussian state is obtained by PF. Then, the authors correlate the optimal estimate with the detected value to determine the trajectory of each particle and to achieve flock tracking. Experimental results demonstrate that this improved algorithm realizes the real-time tracking of flocs and calculation of sedimentation velocity. In addition, it eliminates the shortcomings of heavy computation and low efficiency in the process of extracting image features, and thus guarantees the accuracy and efficiency of tracking flocs.

We would like to express our special thanks to Prof. Guy Pujolle, the Editor-in-Chief of Annals of Telecommunications, for his great support and efforts throughout the whole publication process of this special issue. Moreover, this special issue is due to encouragement of Dr. Nicolas Puech, the Vice Editor-in-Chief, and Ms. Alexia Kappelmann, the managing editor, who are instrumental in the organization process, and to the Springer Journal Editorial Office for their continuous support to publish 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. This special issue presents some selected papers in touching important aspects of security, privacy, and forensics issues in critical infrastructure and other related areas and also emphasizes many open questions. The wide spread use and importance of critical infrastructure is encouraging researchers to look at various open questions and a lot more work needs to be done before it becomes a reality and widely accepted by the user community.

References

1. Yusta JM, Correa GJ, Lacal-Arántegui R (2011) Methodologies and applications for critical infrastructure protection: state-of-the-art. Energy Pol 39(10):6100–6119
2. B. B. Gupta, D. P. Agrawal, Shingo Yamaguchi, Handbook of research on modern cryptographic solutions for computer and cyber security, IGI Global Publisher, USA, 2016
3. Lee K, Choi HO, Min SD, Lee J, Gupta BB, Nam Y (2017) A Comparative Evaluation of Atrial Fibrillation Detection Methods in Koreans Based on Optical Recordings Using a Smartphone, in IEEE Access, vol. 5. pp 11437–11443. doi:10.1109/ACCESS.2017.2700488
4. Lee, Keonsoo, et al (2017) A comparative evaluation of atrial fibrillation detection methods in koreans based on optical recordings using a smartphone. IEEE Access
5. Yan Y, Qian Y, Sharif H, Tipper D (2013) A survey on smart grid communication infrastructures: motivations, requirements and challenges. IEEE Commun Surv Tutorials 15(1):5–20
6. Tewari A, Gupta BB (2017) Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. J Supercomput 73(3):1085–1102
7. Gupta S et al (2017) Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: present and future challenges. Int J Cloud Appl Comp (IJCAC) 7(3):1–43
8. Stergiou C, Psannis KE, Kim B-G, Gupta B (2016) Secure integration of IoT and cloud computing. Future Generation Computer Systems. doi:10.1016/j.future.2016.11.031
9. Zhang Z, Brij BG (2016) Social media security and trustworthiness: overview and new direction. Future Generation Computer Systems. Elsevier. doi:10.1016/j.future.2016.10.007
10. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(1):1–11
11. Miller B, Rowe D (2012) A survey SCADA of and critical infrastructure incidents. Proceedings of the 1st Annual conference on Research in information technology, Calgary, Alberta, Canada pp 51–56
12. Ten C-W, Manimaran G, Liu C-C (2010) Cybersecurity for critical infrastructures: attack and defense modeling. IEEE Trans Syst Man Cybernet Part A: Syst Hum 40(4):853–865