Hindawi
Security and Communication Networks
Volume 2021, Article ID 9830547, 2 pages
https://doi.org/10.1155/2021/9830547

Editorial

Security and Privacy in Smart Cities

Chalee Vorakulpipat[1] **Ryan K. L. Ko**[2] **Qi Li**[3] **and Ahmed Meddahi**[4]

[1] *Information Security Research Team, National Electronics and Computer Technology Center, Pathumthani 12120, Thailand*
[2] *School of Information Technology and Electrical Engineering, University of Queensland, St Lucia, Queensland 4072, Australia*
[3] *Institute for Network Sciences and Cyberspace, Beijing National Research Center for Information Science and Technology (BNRist), Tsinghua University, Beijing 100084, China*
[4] *IMT Lille Douai, Institut Mines-Télécom, Lille 59500, France*

Correspondence should be addressed to Chalee Vorakulpipat; chalee.vorakulpipat@nectec.or.th

Received 28 July 2021; Accepted 28 July 2021; Published 15 August 2021

Smart cities have a unique characteristic: integration of deployment of information and communication technology (ICT) services and innovations to handle complex data in storage devices and during citywide transmission. Technologies adopted in smart cities mostly are state of the art and may not be found outside smart cities. Moreover, smart cities today have been used as testbeds or showcases for new technologies for which security and privacy are still uncertain. Consequently, valuable data supported by those technologies can be at risk from various attacks. Security with privacy is an essential key to driving a smart city. Security and privacy issues affect not only a smart city as a whole but also its smart elements including buildings, factories, health, education, and transportation.

Particularly in the smart industry, Internet of Things (IoT), industrial IoT (IIoT), and cyber-physical systems currently lack adequate access control and antimalware and operate 24/7. They are vulnerable to attacks such as DDoS. Regarding personal data protection in a smart context, data confidentiality is vital for privacy law compliance, such as General Data Protection Regulation (GDPR) in the EU and personal data protection acts in many other countries. Cryptography, access control models, and new security architectures for specific contexts can support privacy and law compliance. Consequently, security with privacy is an essential topic for ICT audiences with an emphasis on smart cities.

This special issue aimed to collate original research and review articles emphasizing security and privacy in smart cities. After peer review, we selected seven papers, including six research articles and one review article, which all highlight current issues and trends in the related topics.

As mentioned above, IoT plays a critical role in smart cities; thus, new requirements and risks in IoT security are never ending and can always be discovered. D. Yamakawa et al. investigated the risk associated with using a public certificate authority (CA) in long-lifespan IoT devices. The study addresses the possibility that IoT devices can be disconnected from the network for a very long time, leading to the problem of certificate expiration. The paper proposes a mechanism using certificates issued and signed by a private CA in conjunction with an embedded key used for verifying firmware updates.

There is still room for improvement in terms of access control models in IoT. R. Zhang et al. enhanced the privacy of IoT devices (referred to as subjects) requesting access to other entities (referred to as objects) in the context of smart cities by proposing, implementing, and evaluating a new ABAC-based access control solution called the AB_SAC framework. The AB_SAC framework inherits the features of ABAC such as fine-grained access control, hides the identity of a subject from an entity (referred to as an authorization authority) authorizing access requests, and provides accountability in terms of tracing back the subject identity.

Natural language processing (NLP) can link to an implementation of data privacy policy and IoT. L. Yang et al. presented an information extraction system for purpose-aware rules of privacy policies in IoT to facilitate data privacy compliance and reduce privacy risks due to unfriendly policies. The purpose-aware rules written in natural language are analyzed using semantic role labeling (SRL), whereby meaningful arguments of the main verb are extracted with sequence tagging. In this paper, the actors, actions, manipulated data, and purpose are extracted from these rules. The authors also propose a method to improve the accuracy of SRL by domain adaptation on a supplementary dataset. The results show that their approach improves the accuracy of extracting the purpose-aware rules.

Privacy preservation for smart grid systems is one of the concerns in smart cities. F. L. Lako et al. addressed the differential privacy (DP) problem in smart grid-based energy delivery networks for publishing aggregate data (e.g., energy consumption of users) while guaranteeing individual privacy. The paper proposes a mechanism called clamping fourier perturbation algorithm (CFPA) that extends or "revisits" the existing FPA mechanism for better privacy protection, improving data aggregation (utility and sensitivity) without disclosing individual data.

Regarding a security intelligence mechanism combatting cyberattacks, B. A. Khalaf et al. propose an adaptive agent-based model called Adaptive Protection of Flooding Attacks (APFA) for protection against Distributed Denial of Service (DDoS) attacks and Flash Crowd (FC) flooding traffics targeting a Network Application Layer (NAL). This model aims to protect the NAL against DDoS and FC flooding by differentiating between DDoS and FC abnormal traffic and then separating DDoS botnets into Demons and Zombies to apply a suitable attack-handling methodology.

The cryptography paper by H. El Gafif and A. Toumanari presents an interesting technique for applying Ciphertext-Policy Attribute-Based Encryption (CP-ABE) as a service. Similar to many CP-ABE-based approaches, the proposed method relies on a Trusted Authority (TA) to issue keys to users. However, in the proposed scheme, the generated keys are separated and kept between a user and the ABE service provider, which allows the user to encrypt the data partially and let the ABE service provider perform the rest. This results in improvements in terms of both computational and communication costs at the user side.

Zero trust architecture (ZTA) has been increasingly mentioned these days, while very few research studies have been done. The last paper, a review article by S. Teerakanok et al., presents challenges and concerns in migrating from perimeter-based security to ZTA. Unlike the legacy network, in which everything inside the internal network is considered trustable, ZTA raises the security level of the entire system by assuming that breaches have been happening everywhere, including inside the corporate network. Based on NIST SP800-207, the authors discuss new threats and challenges in ZTA, including new attack surfaces and vendor lock-in problems. Furthermore, steps and other aspects to consider during the migration process from a legacy network to ZTA are discussed.

Conflicts of Interest

The Guest Editors declare that they have no conflicts of interest regarding the publication of this special issue.

Acknowledgments

We would like to express our appreciation and gratitude to all authors who submitted their works to our special issue. We also cordially thank all reviewers who dedicated their valuable time to consider the papers and provide constructive comments. Additionally, we would like to thank the Editorial Board of this journal for giving us this excellent opportunity, resulting in success in the publication of this special issue.

Chalee Vorakulpipat
Ryan K. L. Ko
Qi Li
Ahmed Meddahi