Project-9: Design of Security Protocols in Cloud-Based Cyber-Physical Systems (CPSs)

Cyber-Physical System (CPS), also known as smart system, is a network engineered for interaction between physical and computational components. CPSs provide abstractions, and design and analysis techniques to the whole system by integrating networking and software with the dynamics of physical processes. Similar to the Internet of Things (IoT), the coordination and combination between the computational and physical elements is higher in CPS. Applications of CPS typically involve sensor-based autonomous systems. With advancements in engineering and science, the application dimensions of CPS are increasing due to their improving efficiency, safety, reliability, usability and autonomy. These dimensions include precision (in surgery and manufacturing), coordination (in air traffic control), efficiency (in optimizing energy usage), augmenting human capabilities, etc. Some technologies re-lated to CPS are the Industrial Internet, Smart Cities and Smart Grid.

With advancements in engineering and science, various application dimensions of Cyber-Physical System (CPS) are now opening due to their improving efficiency, safety, reliability, usability and autonomy. For providing on-demand access to shared processing resources, cloud computing is necessary in order to reduce infrastructure costs. However, the communication between entities in cloud-assisted CPS is vulnerable to various attacks, such as relay, man-in-the-middle, impersonation, physical smart meters capture and privileged-insider attacks. Hence, to ensure quality of service and information, privacy and security is an important requirement in cloud-assisted CPS environment. Also, most of the existing schemes proposed in the cloud environment are either suspectable to several known attacks or they are expensive in communication and computation overheads. To address these issues, we need to propose new authenticated key agreement schemes in the cloud-assisted CPS environment.

References

[1] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang. A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid. IEEE Transactions on Cloud Computing, 3(2):233-244, 2015.

[2] F. Hu, Y. Lu, A. V. Vasilakos, Q. Hao, R. Ma, Y. Patil, T. Zhang, J. Lu, X. Li, and N. N. Xiong. Robust Cyber–Physical Systems: Concept, models, and implementation. Future Generation Computer Systems, 56:449-475, 2016.

[3] S. Rho, A. V. Vasilakos, and W. Chen. Cyberphysical systems technologies and application–Part II. Future Generation Computer Systems, 61:83-84, 2016.

[4] A. Socievole, A. Ziviani, F. De Rango, A. V. Vasilakos, and E. Yoneki. Cyber-physical systems for Mobile Opportunistic Networking in Prox-imity (MNP). Computer Networks, 111:1-5, 2016.

[5] S. Mehar, S. Zeadally, G. Remy, and S. M. Senouci. Sustainable Transportation Management System for a Fleet of Electric Vehicles. IEEE Transactions on Intelligent Transportation Systems, 16(3):1401-1414, 2015.

[6] S. Misra, S. Bera, and T. Ojha. D2P: Distributed Dynamic Pricing Policy in Smart Grid for PHEVs Management. IEEE Transactions on Parallel and Distributed Systems, 26(3):702-712, 2015.

[7] X. Fang, S. Misra, G. Xue, and D. Yang. Managing smart grid information in the cloud: opportunities, model, and applications. IEEE Network, 26(4):32-38, 2012.

[8] N. Kumar, S. Zeadally, and S. C. Misra. Mobile cloud networking for efficient energy management in smart grid cyber-physical systems. IEEE Wireless Communications, 23(5):100-108, 2016.

[9] H. Sun, Q. Wen, H. Zhang, and Z. Jin. A novel remote user authentication and key agreement scheme for mobile client-server environment. Applied Mathematics and Information Sciences, 7(4):1365-1374, 2013.

[10] H. Li, F. Li, C. Song, and Y. Yan. Towards Smart Card Based Mutual Authentication Schemes in Cloud Computing. KSII Transactions on Internet and Information Systems, 9(7):2719-2735, 2015.