Progressive and Fast Authentication Large-Scale Internet of Things

Tabinda Shehzadi[1] and Tabinda Shehrazi[1]

[1]Affiliation not available

August 23, 2022

Progressive and Fast Authentication Large-Scale Internet of Things

Tabinda Shehrazi

Abstract

Security provisioning has become the most important design consideration for large-scale Internet of Things (IoT) systems due to their critical roles to support diverse vertical applications by connecting heterogeneous devices, machines and industry processes. Conventional authentication and authorization schemes are insufficient in dealing the emerging IoT security challenges due to their reliance on both static digital mechanisms and computational complexity for improving security level. Furthermore, the isolated security designs for different layers and link segments while ignoring the overall protection lead to cascaded security risks as well as growing communication latency and overhead. Potential security risks and attacks could lead to catastrophic consequences and cause avalanche-like damages in large-scale IoT networks. This is mainly due to the critical roles of IoT to support a wide variety of vertical applications by connecting tremendous heterogeneous devices, machines and industry processes, as well as cascaded reaction from the enormous parallel interconnection contained in IoT. Moreover, the widely used resource-constrained devices, e.g. sensors, can be compromised easily, thus resulting in widely distributed threats to the IoT network through data injection, spoofing, eavesdropping, and so on.

Challenges for Conventional Authentication and Authorization in Large-Scale IoT:

The conventional authentication and authorization methods, including key-based cryptography techniques and physical layer key generation techniques, may suffer from their high complexity and long latency, and may be ineffective to adapt to the complex dynamic environment, especially in large-scale IoT networks[1, 2].

Long security induced latency in large-scale IoT. The conventional cryptography techniques require increased overhead and lengthy process for increased level of security, thus leading to high communication and computation overhead, more importantly, long communication latency[3]. These are intolerable for the large-scale IoT network having significantly increasing number of intelligent machines and resource-constrained devices with concurrent communications[4].

Ineffective adaptation to complex dynamic IoT environment. Conventional security solutions may also suffer from cascading risks in complex dynamic IoT scenarios due to their reliance on static binary authentication/authorization mechanisms[5, 6].

Potential key leakage in the security management procedures. Conventional cryptographic techniques also require appropriate key management procedures to generate, distribute, refresh and revoke digital security keys, leading to the potential key leakage[7].

Artificial Intelligence for Security Enhancement in Large-Scale IoT

Security management may be accelerated by AI based on multi-domain information in large-scale IoT[8, 9]. In a large-scale IoT system, the gateways and routers may undertake the AI management, such as data collection, training and testing, thus the communication and computation overhead could be reduced at low-power devices.[10-12]

AI provides real-time learning under limited statistical properties and unpredictable dynamics.[13]

Privacy protection in the security management may be achieved with the help of AI techniques. To achieve security enhancement, the authentication and authorization mechanisms should be protected from the privacy leakage[14, 15].

References:

[1] M. Heydari, Z. Xiaohu, L. K. Keung, and Y. Shang, "Entrepreneurial Intentions and Behaviour as the Creation of Business: Based on the Theory of Planned Behaviour Extension Evidence from Polish Universities and Entrepreneurs," *Propósitos y representaciones,* vol. 8, no. 2, p. 46, 2020.

[2] R. Oak, M. Du, D. Yan, H. Takawale, and I. Amit, "Malware detection on highly imbalanced data through sequence modeling," in *Proceedings of the 12th ACM Workshop on artificial intelligence and security*, 2019, pp. 37-48.

[3] Z. Xiaohu, M. Heydari, K. K. Lai, and Z. Yuxi, "Analysis and modeling of corruption among entrepreneurs," *REICE: Revista Electrónica de Investigación en Ciencias Económicas,* vol. 8, no. 16, pp. 262-311, 2020.

[4] R. Oak, "Poster: Adversarial Examples for Hate Speech Classifiers," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 2621-2623.

[5] M. Heydari, K. K. Lai, and Z. Xiaohu, *Corruption, Infrastructure Management and Public–Private Partnership: Optimizing through Mathematical Models*. Routledge, 2021.

[6] R. Oak, "A study of digital image segmentation techniques," *Int. J. Eng. Comput. Sci,* vol. 5, no. 12, pp. 19779-19783, 2016.

[7] M. Heydari *et al.*, "Emergency and Disaster Logistics Processes for Managing ORs Capacity in Hospitals: Evidence from United States," *International Journal of Business and Management (IJBM),* vol. 1, no. 1, pp. 63-85, 2022.

[8] S. A. Shah and N. Mazher, "A review on security on internet of things," in *November 2018 Conference: 1st International Multi-Disciplinary Research Conference (IMDRC 2017)*.

[9] R. Oak, "Extractive techniques for automatic document summarization: a survey," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 4, no. 3, pp. 4158-4164, 2016.

[10] M. Heydari, Z. Xiaohu, M. Saeidi, K. K. Lai, Y. Shang, and Z. Yuxi, "Analysis of the role of social support-cognitive psychology and emotional process approach," *European Journal of Translational Myology,* vol. 30, no. 3, 2020.

[11] N. Mazher and I. Ashraf, "A Survey on data security models in cloud computing," *International Journal of Engineering Research and Applications (IJERA),* vol. 3, no. 6, pp. 413-417, 2013.

[12] N. Mazher, M. Alhadaad, and O. Shagdar, "A Brief Summary of Cybersecurity attacks in V2X Communication," 2022.

[13] R. Oak, M. Khare, A. Gogate, and G. Vipra, "Dynamic Forms UI: Flexible and Portable Tool for easy UI Design," in *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 2018: IEEE, pp. 1926-1931.

[14] I. Ashraf and N. Mazher, "An Approach to Implement Matchmaking in Condor-G."

[15] N. Mazher, A. Brighteni, and F. Haider, "Vehicular Platooning to be Secure against Cybersecurity Attacks," 2022.