electronics

MDPI

Editorial

Emerging Trends and Challenges in IoT Networks

Hosung Park [1] and Soochang Park [2,*]

[1] Department of Cyber Security and Police, Busan University of Foreign Studies, Busan 46234, Republic of Korea; hspark0865@bufs.ac.kr
[2] Department of Computer Engineering, Chungbuk National University, Cheongju 28644, Republic of Korea
* Correspondence: cewinter@chungbuk.ac.kr

The nature of novel ICT technologies such as digital twins, various blockchain technologies, AI, technologies beyond 5G and 6G, etc., in terms of Internet of Things (IoT) networks plays a major role in seamless data acquisition and provision. Such a key role can be achieved via intensive integration and reliable connectivity among heterogeneous devices and communication technologies. As they are used in various applications related to our daily and near-future needs, IoT networks are facing diverse challenges related to quality of experience (QoE), cyber–physical security, privacy, trustworthiness, reliability, and self-sustainability, including social issues, which are being addressed via the establishment of technologies such as green technology. New applications also make up one of these challenges, from smart homes with small-scale coverage to smart cities that connect the devices of industries and consumers. Promising approaches such as edge AI, blockchain, and cloud/fog/edge-based data intelligence may help to solve these emerging challenges.

In this Special Issue, we present groundbreaking research and case studies that have developed a wide variety of novel IoT technologies related to cybersecurity, AI-aided smart services, and future-driven network and hardware technologies.

Jinhyeok Jang et al. introduced network-based intrusion detection systems (NIDSs) and their main target problems related to creating feasible backdoor attacks on NIDS data. The backdoor attacks on the data, mainly tabular data, remain a research challenge due to various constraints and practical concerns, such as the difficulties faced in defining and manipulating a model to specific columns or values and inserting a small number of effective backdoor triggers [1,2]. Hence, Contribution 1 proposes a backdoor attack scenario and method for tabular data; the authors executed the attack based on feature importance and the decision conditions of a decision tree. Through the demonstrated efficacy of the attack, vulnerabilities in NIDSs facing backdoor attacks were revealed. Two manual detection methods for anomaly detection, namely, the statistical methodology KL divergence and the machine learning approach OneClassSVM, were adopted. This study led to the discovery that a tradeoff between the success rate of backdoor attacks and outliers needs to be carefully considered

Imanol Martín Toral et al. proposed a multi-layer architecture based on the OpenFog architecture that focuses on corporative buildings and includes complex algorithms based on AI techniques. The proposed architecture implements edge, fog, and cloud computing layers [3] through various types of devices. In particular, the fog layer is responsible for collecting data from the edge node and executing control algorithms to ensure adequate indoor environment conditions. Fuzzy logic is an intuitive technique used for monitoring IAQ systems, and it is also used in the proposed architecture. The architecture also allows one to integrate advanced services offered in the form of cloud services. The proposed architecture was tested experimentally using a prototype.

Patryk Pyt et al. (Contribution 3) developed BLE Beacon-Based IoT Localization to improve accessibility. The mechanism for determining the RSSI (Received Signal Strength Indicator) coefficient for IoT positioning is commonly used in radiocommunication devices. RSSI measurement techniques are often supplemented by RF patterns, known as

check for updates

Citation: Park, H.; Park, S. Emerging Trends and Challenges in IoT Networks. *Electronics* **2024**, *13*, 513. https://doi.org/10.3390/electronics13030513

Received: 19 January 2024
Accepted: 24 January 2024
Published: 26 January 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

fingerprints [4,5]. The core concept behind the fingerprint method is to use intelligent algorithms that allow for estimations of RSSI coefficients to be verified. This means that unique RF signature databases should be prepared; that is, advanced software algorithms must be used in fingerprinting methods, which are associated with an enormous amount of additional work and costs. Therefore, in this contribution, a novel selection method was used to select an appropriate beacon for the designed application, with the selected beacon's performance being based on the energy demand characteristics at the assumed power settings and time intervals of the emitted signal. Also, this contribution focuses on various concepts related to transmitter deployment inside campus buildings in order to demonstrate possible configurations in which the IoT localization will work correctly.

Ibrahim S. Alsukayti proposed an innovative approach for dynamic RPL (Routing Protocol for Low-Power and Lossy Networks) topology management, named Dynamic-RPL, for energy-efficient wireless Low-Power and Lossy Networks (LLNs). This approach allows for more topology flexibility and dynamicity in varying-scale networks deployed for any IoT application. It introduces simple in-protocol modifications to the standard RPL [6] to extend its functionality and make it more effective. Dynamic-RPL incorporates modified RPL topology establishment, customized RPL objective function and parent selection, a new dynamic topology management algorithm, and additional inter-routing support.

Minh Dang et al. focused on the various aspects of digital face manipulation creation and detection methods that can efficiently and effectively identify manipulated multi-media data signals to address the threat of facial manipulation images, which are progressively advancing in terms of achieving greater levels of realism. The authors of this study came up with a survey to address this issue by providing a comprehensive analysis of the methods used to produce a given manipulative face image, focusing on the discovery of deep fake technology and emerging techniques that are being used to detect fake images [7,8]. The main focus of the survey was facial manipulation, especially deep false technology. Regarding the authors' methodology, firstly, they classified facial manipulation into four main categories: facial replacement, facial reconstitution, facial attribute manipulation, and facial synthesis. Subsequently, they explained the benchmark datasets and standard generation and detection methods for each category of manipulation. Additionally, this contribution also discusses the challenges and trends pertaining to each category.

Daniel Poul Mtowe et al. present an innovative strategy to enhance low-latency control performance in Wireless Networked Control Systems (WNCSs) by integrating edge computing. Conventional WNCSs face challenges with periodic data transmission from remote sensors, negatively impacting performance via delays and packet dropouts [9]. The proposed approach utilizes edge computing to preprocess raw data before extracting the essential features from the data and transmitting them, reducing raw data transmission to only 3.42%. An adaptive scheme further reduced data traffic by adjusting periodic transmission based on necessity, achieving a 20% frequency reduction without compromising control performance. A comparative analysis with Web Real-Time Communication technology [10] demonstrated a 58.16% latency reduction in a 5G environment. This study highlights the importance of concurrently considering communication and computation aspects to ensure optimal WNCS performance. The main contributions of this study include the fact that it introduces an adaptive scheme to reduce data traffic, as well as an algorithm for threshold computation, and includes experimental validation results showcasing reduced communication cycles alongside well-maintained system performance. The paper concludes by emphasizing the potential applicability of the proposed strategy to various WNCSs and suggests future research directions, including using the in proposed strategy to analyze energy consumption in the context of low-delay communication.

Panagiotis Sotiropoulos et al. summarize security-related issues in the context of IoT software and existing solutions and, based on this, introduce a software vulnerability management framework for an IoT platform software. The framework addresses challenges related to software vulnerabilities in IoT systems, offering solutions for configuration, security testing, vulnerability impact estimation, and the prioritization of fixes. It emphasizes

minimizing the attack surface by configuring software to include only necessary features and provides a statistical method for estimating the impact of detected vulnerabilities. The framework employs an integer programming-based algorithm to prioritize security fixes, considering the associated technical debt and available security budget. The proposed method is positioned as a valuable tool for software architects, developers, and security experts involved in IoT platform implementation. The paper contributes to the field by providing a comprehensive framework that considers multiple aspects in the security analysis of platform software.

Breno Sousa et al. explore the application of 5G technology in vehicles, addressing the security challenges in Internet of Vehicles (IoV) technologies. Focusing on flooding attacks, the authors propose an intrusion detection system (IDS) that utilizes machine learning algorithms. Simulations are conducted using Network Simulator 3 (NS-3), generating four labeled datasets based on different vehicular scenarios with Urban Mobility (SUMO) patterns. The results demonstrate the IDS's effectiveness in detecting flooding attacks, as it achieved F1 scores of 1.00 and 0.98 with decision trees and random forests, respectively. A comparison with similar studies [11,12] highlighted the proposed system's superior performance, emphasizing the importance of data diversity in training sets. The study concludes that simplicity, as seen in decision trees and random forests, can be as effective as complex learning methods in vehicular scenarios.

For the first time in the literature, Dunge Liu et al. theoretically analyzed the impact of the application of Intelligent Reconfigurable Surface (IRS) phase modulation technology on localization accuracy in Passive Wireless Sensor Networks (PWSNs). In their study, two algorithms, an approximation algorithm (AP) and a genetic algorithm (GA), were proposed to achieve optimal phase modulation in order to enhance localization accuracy. A PWSN refers to a wireless network composed of sensor nodes that harvest energy from the surrounding environment without batteries, and an IRS is a next-generation ultra-small antenna technology that can correct the transmission and reflection directions of radio waves by controlling material properties. The simulation results reported in this study show that, with the proposed algorithms, localization accuracy can be significantly improved in both line-of-sight (LoS) and non-line-of-sight (NLoS) environments. The accuracy improved the most when the GA algorithm was applied in NLoS environments. This study provides valuable insights into enhancing PWSN localization through IRS-based techniques, laying the foundation for future practical implementations.

Fahad Qaswar et al., based on 115 selected articles, reviewed and analyzed ontology (i.e., the explicit specification of a concept) in IoT scenarios. In this in-depth review, the authors provide useful information by categorizing and analyzing existing studies on various topics, such as the types of ontologies, the requirements for ontologies in the IoT domain, ontology languages, the limitations of existing ontologies, and ontology reuse. They also provide valuable insights through discussing future trends.

We hope that the research findings presented in the referenced studies contribute to advancing the IoT domain and scientific knowledge. We would also like to express our sincere gratitude to all of the authors, reviewers, and other valued contributors who made this Special Issue possible.

Author Contributions: Conceptualization, H.P. and S.P.; writing—original draft preparation, H.P. and S.P.; writing—review and editing, H.P. and S.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

List of Contributions

1. Jang, J.; An, Y.; Kim, D.; Choi, D. Feature Importance-Based Backdoor Attack in NSL-KDD. *Electronics* **2023**, *12*, 4953.

2. Martín Toral, I.; Calvo, I.; Xenakis, J.; Artetxe, E.; Barambones, O. Architecture for Smart Buildings Based on Fuzzy Logic and the OpenFog Standard. *Electronics* **2023**, *12*, 4889.
3. Pyt, P.; Skrobacz, K.; Jankowski-Mihułowicz, P.; Węglarski, M.; Kamuda, K. Empowering Accessibility: BLE Beacon-Based IoT Localization. *Electronics* **2023**, *12*, 4012.
4. Alsukayti, I.S. Dynamic-RPL: Enhancing RPL-Based IoT Networks with Effective Support of Dynamic Topology Management. *Electronics* **2023**, *12*, 3834.
5. Dang, M.; Nguyen, T.N. Digital Face Manipulation Creation and Detection: A Systematic Review. *Electronics* **2023**, *12*, 3407.
6. Mtowe, D.P.; Kim, D.M. Edge-Computing-Enabled Low-Latency Communication for a Wireless Networked Control System. *Electronics* **2023**, *12*, 3181.
7. Sotiropoulos, P.; Mathas, C.M.; Vassilakis, C.; Kolokotronis, N. A Software Vulnerability Management Framework for the Minimization of System Attack Surface and Risk. *Electronics* **2023**, *12*, 2278.
8. Sousa, B.; Magaia, N.; Silva, S. An Intelligent Intrusion Detection System for 5G-Enabled Internet of Vehicles. *Electronics* **2023**, *12*, 1757.
9. Liu, D.; Chen, S.; Lu, Z.; Jin, S.; Zhao, Y. CRLB Analysis for Passive Sensor Network Localization Using Intelligent Reconfigurable Surface and Phase Modulation. *Electronics* **2022**, *12*, 202.
10. Qaswar, F.; Rahmah, M.; Raza, M.A.; Noraziah, A.; Alkazemi, B.; Fauziah, Z.; Hassan, M.K.A.; Sharaf, A. Applications of Ontology in the Internet of Things: A Systematic Analysis. *Electronics* **2022**, *12*, 111.

References

1. Byunggill, J.; Yonghyeon, P.; Jihun, H.; Shin, I.; Jiyeon, L. Exploiting Missing Value Patterns for a Backdoor Attack on Machine Learning Models of Electronic Health Records: Development and Validation Study. *JMIR* **2022**, *10*, 8.
2. Joe, B.; Mehra, A.; Shin, I.; Hamm, J. Machine Learning with Electronic Health Records is vulnerable to Backdoor Trigger Attacks. In Proceedings of the AAAI Workshop on Trustworthy AI for Healthcare, Online Workshop, 28 February 2021.
3. Linthicum, D. Responsive Data Architecture for the Internet of Things. *Computer* **2016**, *49*, 72–75. [CrossRef]
4. Ruan, L.; Zhang, L.; Zhou, T.; Long, Y. An Improved Bluetooth Indoor Positioning Method Using Dynamic Fingerprint Window. *Sensors* **2020**, *20*, 7269. [CrossRef] [PubMed]
5. Khan, I.M.; Thompson, A.; Al-Hourani, A.; Sithamparanathan, K.; Rowe, W.S.T. RSSI and Device Pose Fusion for Fingerprinting-Based Indoor Smartphone Localization Systems. *Future Internet* **2023**, *15*, 220. [CrossRef]
6. Winter, T.; Thubert, P.; Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.; Alexander, R. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. In *IETF RFC 6550*; IETF: Fremont, CA, USA, 2012.
7. Tolosana, R.; Vera-Rodriguez, R.; Fierrez, J.; Morales, A.; Ortega-Garcia, J. Deepfakes and beyond: A survey of face manipulation and fake detection. *Inf. Fusion* **2020**, *64*, 131–148. [CrossRef]
8. Kietzmann, J.; Lee, L.W.; McCarthy, I.P.; Kietzmann, T.C. Deepfakes: Trick or treat? *Bus. Horizons* **2020**, *63*, 135–146. [CrossRef]
9. Khanh, Q.V.; Hoai, N.V.; Manh, L.D.; Le, A.N.; Jeon, G. Wireless communication technologies for IoT in 5G: Vision, applications, and challenges. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 3229294.
10. Tiberkak, A.; Hentout, A.; Belkhir, A. WebRTC-based MOSR remote control of mobile manipulators. *Int. J. Intell. Robot. Appl.* **2023**, *7*, 304–320. [CrossRef] [PubMed]
11. Polat, H.; Turkoglu, M.; Polat, O. Deep network approach with stacked sparse autoencoders in detection of DDoS attacks on SDN-based VANET. *IET Commun.* **2020**, *14*, 4089–4100. [CrossRef]
12. Otoum, Y.; Wan, Y.; Nayak, A. Transfer Learning-Driven Intrusion Detection for Internet of Vehicles (IoV). In Proceedings of the 2022 International Wireless Communications and Mobile Computing (IWCMC), Dubrovnik, Croatia, 30 May–3 June 2022; pp. 342–347.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.