electronics

Editorial

Recent Advances in Internet of Things and Emerging Social Internet of Things: Vision, Challenges and Trends

Farhan Amin [1,*], Ikram Asghar [2], Aftab Ali [3] and Seong-Oun Hwang [4]

1 Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Korea
2 Faculty of Computing, Engineering and Science, University of South Wales, Pontypridd CF37 1LP, UK; ikram.asghar@southwales.ac.uk
3 School of Computing, Ulster University, Shore Rd, Newtownabbey BT37 0QB, UK; a.ali@ulster.ac.uk
4 Department of Computer Engineering, Gachon University, Seongnam 13120, Korea; sohwang@gachon.ac.kr
* Correspondence: farhanamin10@hotmail.com

Citation: Amin, F.; Asghar, I.; Ali, A.; Hwang, S.-O. Recent Advances in Internet of Things and Emerging Social Internet of Things: Vision, Challenges and Trends. *Electronics* **2022**, *11*, 2033. https://doi.org/10.3390/electronics11132033

Received: 25 June 2022
Accepted: 26 June 2022
Published: 29 June 2022

1. Introduction

In recent years, the Internet of Things (IoT), together with its related emerging technologies, has been driving a revolution in the way people perceive and interact with the surrounding environment. Smart homes and smart offices are effective examples that are enriched with sensing, actuating, communication, and computing capabilities. The IoT provides an umbrella under which many heterogeneous technologies and objects are interacting and co-operating. The need to enhance its performance with characteristics from other more mature technologies is rising. The full potential of the emerging IoT paradigm requires a large amount of industrial and academic research efforts directed to the design, development, and assessment of novel architectures, methodologies, and technologies. The Social Internet of Things (SIoT) refers to the convergence of the IoT and social networking paradigms for the creation of social networks in which things are nodes that establish social links as humans do. In recent years, this concept has become a hot topic in academic research. The benefits derived from the potential of social networks within the IoT domain, such as simplification in the navigability of a dynamic network of billions of objects, robustness in the trustworthiness of objects and efficiency in the dynamic discovery of services and information.

For this purpose, this Special Issue aims to involve both academic and industrial communities that operate in the fields of computer science, electronics, and telecommunications control systems and to highlight the latest research concerning emerging technologies. Participants were invited to write about one of the subjects listed below, but they were not limited to these.

- Internet of Things;
- Cyber-physical systems;
- Smart environments;
- Standards and protocols for the Internet of Things;
- IoT toward COVID-19;
- Trusted IoT ecosystem;
- Smart home;
- Big Data for IoT;
- Machine learning and artificial intelligence for the Internet of Things;
- Social Internet of Things;
- SIoT application in health care and hospital information system;
- Data mining and analytics in SIoT;
- SIoT and smart cities;
- Cybersecurity in SIoT;
- SIoT and autonomous driving systems;

- ○ SIoT application in the smart home system;
- ○ SIoT experimental platforms;
- ○ Machine learning techniques in SIoT.

2. Review Papers

Kilani et al. [1], as part of ongoing research, developed a model for studying the opportunistic interactions between the industrial Internet of Things (IoT). In the proposed model, the SIoT concept is integrated into the industrial IoT. The integration of SIoT into the industry is known as the Social Internet of Industrial Things. This model relies on six principles of the interaction and is based on the transposition of human social interaction mechanisms and the principles toward the industrial communication objects that we encounter in manufacturing and logistics facilities. The implementation is performed using Netlogo. The efficiency and the practicability of the proposed model were examined by elaborating the socialized interactions and calculating all messages generated by the objects. The attained results confirmed that messaging traffic between socialized industrial communicating objects is deterministic and can be estimated a priori with a simple equation.

Rahim et al. [2] proposed a deep learning-based model for the monitoring of COVID social distance violations. Currently, the standard operating procedure (SoP) for social distance is one of the good methods to mimic the coronavirus (COVID-19). This model is specially designed for underdeveloped countries where the common problem is poor ventilation and also congested homes. These problems cause people to gather in open spaces such as parks, streets, and markets. To address the violation in social distancing. The authors suggested an efficient social distance monitoring scheme named DepTSol. This approach uses a low-cost and easy-to-maintain motionless monocular time-of-flight (ToF) camera and a deep learning object detection algorithm for real-time social distance monitoring. The proposed approach first identifies various people standing in low-light environments. Then, it calculates the distance in terms of pixels and predicts the pixel distance into real-world units. Finally, it highlights those people who were violating the social distancing. The results indicate that the proposed model proves good accuracy with 51.2% and 99% mean average precision (mAP) scores. It is also helpful for researchers who had the intention to learn the timely and responsive real-world applications.

Tahirkheli et al. [3] surveyed the security aspect of the could computing (CC). The CC and IoT are the most prevalent emerging technologies in the future. Cloud computing is a leading and trending technology in recent years. It is used for online storage because it is highly acceptable and highly scalable. In addition, it is also very useful in reducing the workfare and the capital cost. These key aspects attract the organizations that are conducting their business and also providing financial activities over the cloud. In this survey article, the authors surveyed various articles and discussed the advantages and disadvantages of cloud computing. They also provide a comprehensive security analysis of CC-enabled IoT and present state-of-the-art in the research area. They summarized different CC mechanisms for trust, privacy, and security.

Banerjee et al. [4] proposed a lightweight model using fog computing for the IoT. The IoT-based fog systems are very helpful to minimize the latency in IoT applications. In this study, the authors proposed a new lightweight security mechanism to improve the initial authentication to overcome the fog nodes' failover. The robustness of the proposed model has been confirmed by using a detailed security analysis along with the formal security analysis under the ROR random oracle model. The informal security analysis and also formal security verification has been performed using AVISPA. A comparative analysis has been performed among the proposed scheme and state-of-the-art recent schemes. Finally, the effectiveness of the proposed model is measured in terms of communication and computational overheads.

Shaheen et al. [5] presented an analytical survey of wireless sensors network (WSN) using fog computing and the cloud. The WSN are networks comprised of a large number of nodes. These nodes communicate with other neighbors and provide various interesting applications, such as: temperature, humidity, pressure, etc. The applications of WSN are monitoring and runtime decision-making. The limitations of WSN are battery life, computing power and limited storage resources. These limitations make the network restricted for data transmission. The integration of cloud and WSN offers an adaptable, open, and more reconfigurable stage for security checks. In brief, this survey presented an integration of WSN and cloud computing (CC). The authors have performed a comparative analysis and discussed various open issues. The combined benefits of WSN-CC are low energy consumption, latency, real-time data streaming, and data processing. According to the authors, the FC is not useful for distributed computing. So far, it is utilized to improve the productivity of the sensors.

Acknowledgments: We would like to take this opportunity to appreciate and thank all authors for their outstanding contributions and the reviewers for their fruitful comments and feedback. Special appreciation should also be paid to the Editorial Board of MDPI's *Electronics* journal for the opportunity to guest edit this Special Issue and to the *Electronics* Editorial Office staff for their hard and precise work in maintaining a rigorous peer-review schedule and timely publication.

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

References

1. Kilani, R.; Zouinkhi, A.; Bajic, E.; Abdelkrim, M.N. A Socio-Inspired Methodology and Model for Advanced and Opportunistic Interactions between Industrial IoT Objects. *Electronics* **2022**, *11*, 1281. [CrossRef]
2. Rahim, A.; Maqbool, A.; Mirza, A.; Afzal, F.; Asghar, I. DepTSol: An Improved Deep-Learning- and Time-of-Flight-Based Real-Time Social Distance Monitoring Approach under Various Low-Light Conditions. *Electronics* **2022**, *11*, 458. [CrossRef]
3. Tahirkheli, A.I.; Shiraz, M.; Hayat, B.; Idrees, M.; Sajid, A.; Ullah, R.; Ayub, N.; Kim, K.I. A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. *Electronics* **2021**, *10*, 1811. [CrossRef]
4. Banerjee, S.; Das, A.K.; Chattopadhyay, S.; Jamal, S.S.; Rodrigues, J.J.; Park, Y. Lightweight Failover Authentication Mechanism for IoT-Based Fog Computing Environment. *Electronics* **2021**, *10*, 1417. [CrossRef]
5. Shaheen, Q.; Shiraz, M.; Aziz Butt, S.; Gani, A.; Khan, M.A. An Analytical Survey of WSNs Integration with Cloud and Fog Computing. *Electronics* **2021**, *10*, 2625. [CrossRef]