applied sciences

MDPI

Editorial

Cognitive Computing with a Big Data System in a Secure Internet of Things

Xiaochun Cheng [1,*], Ding-Zhu Du [2], Arun Kumar Sangaiah [3] and Rongxing Lu [4]

[1] Department of Computer Science, Swansea University, Swansea SA2 8PP, UK
[2] Department of Computer Science, University of Texas at Dallas, Richardson, TX 75080, USA
[3] International Graduate Institute of AI, National Yunlin University of Science and Technology, Douliu 64002, Taiwan
[4] Faculty of Computer Science, University of New Brunswick, Fredericton, NB E3B 5A3, Canada
* Correspondence: xiaochun.cheng@swansea.ac.uk

This editorial aims to summarize the contents of the ten papers included in the Special Issue entitled "Cognitive Computing with a Big Data System in a Secure Internet of Things".

Cognitive computing is transdisciplinary, involving principles, methods, and technologies from several domains. IoT applications enable information exchange and interactions of physical and digital objects. IoT systems are expected to be smart and secure, and to be designed with reliability, resilience against attacks, operational efficiency, energy efficiency, and resource utilization efficiency. Cognitive computing embedded data technologies are used to process and analyze large amounts of data collected through secure IoT systems to help human experts perform decision-making. This Special Issue collected innovative solutions in this research area.

Two of the key topics of recent advances in cyber security research are data hiding and digital watermarking. New technologies with strategies to use them have emerged. Article [1] focuses on homomorphic public key encryption in a reversible data hiding scheme. The cover image is segmented, and the reference pixel and target pixels are self-embedded into other parts of the image. The data hider embeds the encrypted additional data into the target pixels by means of homomorphic addition in ciphertexts, while the reference pixel remains unchanged.

Internet of Things and big data applications have increased in recent years, and security monitoring is one of the most difficult challenges in this field. FFTD in article [2] is a Fast Face Tracking-by-Detection algorithm that uses the Kernelized Correlation Filter as the basic tracker, multitask CNNs to detect the face, and a new tracking update strategy to update the filter mode.

Cyberattacks use domain names to maintain a connection with clients and generate new domain names to avoid the blacklist mechanism. To address this, article [3] proposes a DGA domain name classification method based on LSTM with an attention mechanism.

A knowledge graph conflict resolution method incorporating deep learning is proposed in article [4] that resolves fact conflicts with high precision by combining time attributes, semantic embedding representations, and graph structure features.

ECG signals are necessary for the analysis and diagnosis of heart diseases. The application value of ECG signals is, however, susceptible to contamination by a variety of disturbances. In order to reduce noise in ECG signals, paper [5] suggests a denoising technique that combines wavelet energy with a sub-band smoothing filter.

Concurrent access in IoT software development is a challenging task. Paper [6] proposes a refactoring framework for fine-grained read–write locking and an automatic refactoring tool to help developers convert built-in monitors into fine-grained Re-entrant Read Write Locks, tested by 1072 built-in monitors.

Article [7] presents a new face recognition approach for security applications based on Goldstein branching and face radial curve elastic matching to address the problem of

Citation: Cheng, X.; Du, D.-Z.; Sangaiah, A.K.; Lu, R. Cognitive Computing with a Big Data System in a Secure Internet of Things. *Appl. Sci.* **2023**, *13*, 7037. https://doi.org/10.3390/app13127037

Received: 7 June 2023
Accepted: 8 June 2023
Published: 12 June 2023

the long recognition time and high equipment cost of intelligent security robots. It has a greater rate of facial identification and is resistant to lighting changes and noises.

Paper [8] focused on learning representations of abstract concepts. The proposed method, Regulated Activation Network (RAN), has an evolving topology and learns representations of abstract concepts by exploiting the geometrical view of concepts, without supervision. It was evaluated with eight UCI benchmarks and five Machine Learning models to establish its credibility.

Short text is widely seen in applications including Internet of Things. The Entity-based Concept Knowledge-Aware (ECKA) method is a multi-level short text semantic representation model that extracts semantic features from words, entities, and concepts with different knowledge levels, as explained in article [9].

An efficient BGV-type homomorphic encryption scheme is proposed in article [10] for secure computing in IoT systems. It reduces storage space and ciphertext evaluation time by allowing constant switch keys and repeated multiplication operations between two sublayers.

In summary, these ten contributions published in this Special Issue indicate the research trends of cognitive computing with big data communicated through a secure Internet of Things.

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

References

1. Zhou, N.; Zhang, M.; Wang, H.; Liu, M.; Ke, Y.; Wang, X. Reversible Data Hiding Scheme in Homomorphic Encrypted Image Based on EC-EG. *Appl. Sci.* **2019**, *9*, 2910. [CrossRef]
2. Su, J.; Gao, L.; Li, W.; Xia, Y.; Cao, N.; Wang, R. Fast Face Tracking-by-Detection Algorithm for Secure Monitoring. *Appl. Sci.* **2019**, *9*, 3774. [CrossRef]
3. Qiao, Y.; Zhang, B.; Zhang, W.; Sangaiah, A.; Wu, H. DGA Domain Name Classification Method Based on Long Short-Term Memory with Attention Mechanism. *Appl. Sci.* **2019**, *9*, 4205. [CrossRef]
4. Wang, Y.; Qiao, Y.; Ma, J.; Hu, G.; Zhang, C.; Sangaiah, A.; Zhang, H.; Ren, K. A Novel Time Constraint-Based Approach for Knowledge Graph Conflict Resolution. *Appl. Sci.* **2019**, *9*, 4399. [CrossRef]
5. Zhang, D.; Wang, S.; Li, F.; Wang, J.; Sangaiah, A.; Sheng, V.; Ding, X. An ECG Signal De-Noising Approach Based on Wavelet Energy and Sub-Band Smoothing Filter. *Appl. Sci.* **2019**, *9*, 4968. [CrossRef]
6. Zhang, Y.; Shao, S.; Ji, M.; Qiu, J.; Tian, Z.; Du, X.; Guizani, M. An Automated Refactoring Approach to Improve IoT Software Quality. *Appl. Sci.* **2020**, *10*, 413. [CrossRef]
7. Wang, Z.; Zhang, X.; Yu, P.; Duan, W.; Zhu, D.; Cao, N. A New Face Recognition Method for Intelligent Security. *Appl. Sci.* **2020**, *10*, 852. [CrossRef]
8. Sharma, R.; Ribeiro, B.; Miguel Pinto, A.; Cardoso, F. Exploring Geometric Feature Hyper-Space in Data to Learn Representations of Abstract Concepts. *Appl. Sci.* **2020**, *10*, 1994. [CrossRef]
9. Hou, W.; Liu, Q.; Cao, L. Cognitive Aspects-Based Short Text Representation with Named Entity, Concept and Knowledge. *Appl. Sci.* **2020**, *10*, 4893. [CrossRef]
10. Yuan, W.; Gao, H. An Efficient BGV-type Encryption Scheme for IoT Systems. *Appl. Sci.* **2020**, *10*, 5732. [CrossRef]