Mathematical Biosciences and Engineering

MBE, 21 (8): 7012–7015.
DOI: 10.3934/mbe.2024307
Received: 21 June 2024
Revised: 21 June 2024
Accepted: 26 August 2024
Published: 29 August 2024

https://www.aimspress.com/journal/MBE

Editorial

Editorial: Artificial Intelligence-based Security Applications and Services for Smart Cities

Jong Hyuk Park*

Department of Computer Science and Engineering, Seoul National University of Science and Technology, 232 Gongneung-ro, Nowon-gu, Seoul, 01811, Korea.

***Correspondence:** Email: jamespark.seoul@gmail.com; jhpark1@seoultech.ac.kr.

The rapid advancement of Smart Cities is crucial for the economic growth and sustainable development of urban areas. These cities rely on a vast network of sensors that collect enormous amounts of data, posing significant challenges in secure data collection, management, and storage. Artificial Intelligence (AI) has emerged as a powerful computational model, demonstrating notable success in processing large datasets, particularly in unsupervised settings. Deep Learning models provide efficient learning representations, enabling systems to learn features from data automatically.

However, the rise in cyberattacks presents ongoing threats to data privacy and integrity in Smart Cities. Unauthorized access and data breaches are growing concerns, exacerbated by various network vulnerabilities and risks. This highlights the necessity for further research to address security issues, ensuring that Smart City operations remain secure, resilient, and dependable.

The main aim of this Special Issue is to gather high-quality research papers and reviews focusing on AI-based solutions, incorporating other enabling technologies such as Blockchain and Edge Intelligence. These technologies address the challenges of data security, privacy, and network authentication in IoT-based Smart Cities. After a rigorous review process, 14 papers were accepted. These papers cover a broad scope of topics and offer valuable contributions to the field of AI-based security applications in Smart Cities. They provide innovative solutions for secure data management, advanced algorithms for threat detection and prevention, and techniques for ensuring data privacy and integrity.

All accepted papers are categorized into six different dimensions: 1) Prediction and forecasting models, 2) Security and encryption techniques, 3) Edge computing and IoT, 4) Automotive and

transportation systems, 5) Artificial intelligence and machine learning applications, and 6) 3D printing and object identification. The brief contributions of these papers are discussed as follows:

In the prediction and forecasting models dimension, Tang et al. [1] proposed a ride-hailing demand prediction model named the spatiotemporal information-enhanced graph convolution network. This model addresses issues of inaccurate predictions and difficulty in capturing external spatiotemporal factors. By utilizing gated recurrent units and graph convolutional networks, the model enhances its perceptiveness to external factors. Experimental results on a dataset from Chengdu City show that the model performs better than baseline models and demonstrates robustness in different environments. Similarly, Chen et al. [2] constructed a novel BILSTM-SimAM network model for short-term power load forecasting. The model uses Variational Mode Decomposition (VMD) to preprocess raw data and reduce noise. It combines Bidirectional Long Short-Term Memory (BILSTM) with a simple attention mechanism (SimAM) to enhance feature extraction from load data. The results indicate an R^2 of 97.8%, surpassing mainstream models like Transformer, MLP, and Prophet, confirming the method's validity and feasibility

In the security and encryption techniques dimension, Bao et al. [3] developed a Fibonacci-Diffie-Hellman (FIB-DH) encryption scheme for network printer data transmissions. This scheme uses third-order Fibonacci matrices combined with the Diffie-Hellman key exchange to secure data. Experiments demonstrate the scheme's effectiveness in improving transmission security against common attacks, reducing vulnerabilities to data leakage and tampering. Cai et al. [4] introduced a robust and reversible database watermarking technique to protect shared relational databases. The method uses hash functions for grouping, firefly and simulated annealing algorithms for efficient watermark location, and differential expansion for embedding the watermark. Experimental results show that this method maintains data quality while providing robustness against malicious attacks. Yu et al. [11] investigated Transport Layer Security (TLS) fingerprinting techniques for analyzing and classifying encrypted traffic without decryption. The study discusses various fingerprint collection and AI-based techniques, highlighting their pros and cons. The need for step-by-step analysis and control of cryptographic traffic is emphasized to use each technique effectively. Salim et al. [14] proposed a lightweight authentication scheme for securing IoT devices from rogue base stations during handover processes. The scheme uses SHA256 and modulo operations to enable quick authentication, significantly reducing communication overhead and enhancing security compared to existing methods.

In the edge computing and IoT dimension, Yu et al. [5] proposed an edge computing-based intelligent monitoring system for manhole covers (EC-MCIMS). The system uses sensors, LoRa communication, and a lightweight machine learning model to detect and alert about unusual states of manhole covers, ensuring safety and timely maintenance. Tests demonstrate higher responsiveness and lower power consumption compared to cloud computing models. Zhu et al. [7] introduced an online poisoning attack framework for edge AI in IoT-enabled smart cities. The framework includes a rehearsal-based buffer mechanism and a maximum-gradient-based sample selection strategy to manipulate model training by incrementally polluting data streams. The proposed method outperforms existing baseline methods in both attack effectiveness and storage management. Firdaus et al. [10] discussed personalized federated learning (PFL) with a blockchain-enabled distributed edge cluster (BPFL). Combining blockchain and edge computing technologies enhances client privacy, security,

and real-time services. The study addresses the issue of non-independent and identically distributed data and statistical heterogeneity, aiming to achieve personalized models with rapid convergence.

In the automotive and transportation systems dimension, Douss et al. [6] presented a survey on security threats and protection mechanisms for Automotive Ethernet (AE). The paper introduces and compares different in-vehicle network protocols, analyzes potential threats targeting AE, and discusses current security solutions. Recommendations are proposed to enhance AE protocol security. Yang et al. [13] proposed a lightweight fuzzy decision blockchain scheme for vehicle intelligent transportation systems. The scheme uses MQTT for communication, DH and Fibonacci transformation for security, and the F-PBFT consensus algorithm to improve fault tolerance, security, and system reliability. Experimental results show significant improvements in fault tolerance and system sustainability.

In the artificial intelligence and machine learning applications dimension, Pan et al. [8] focused on aerial image target detection using a cross-scale multi-feature fusion method (CMF-YOLOv5s). The method enhances detection accuracy and real-time performance for small targets in complex backgrounds by using a bidirectional cross-scale feature fusion sub-network and optimized anchor boxes. Wang et al. [9] reviewed various AI techniques for ground fault line selection in modern power systems. The review discusses artificial neural networks, support vector machines, decision trees, fuzzy logic, genetic algorithms, and other emerging methods. It highlights future trends like deep learning, big data analytics, and edge computing to improve fault line selection efficiency and reliability.

In the 3D printing and object identification dimension, Shin et al. [12] presented an all-in-one encoder/decoder approach for the non-destructive identification of 3D-printed objects using terahertz (THz) waves. The method involves 3D code insertion into the object's STL file, THz-based detection, and code extraction. Experimental results indicate that this approach enhances the identification efficiency and practicality of 3D-printed objects.

In conclusion, 14 excellent full-length research articles have been provided in this special issue on "Artificial Intelligence-based Security Applications and Services for Smart Cities." These papers offer valuable contributions to secure data management, threat detection, and data privacy in IoT-based Smart Cities. We would like to thank all the researchers for their contributions, the MBE editorial assistance, and all the referees for their support in making this issue possible.

References

1. Z. Tang, C. Chen, Spatio-temporal information enhance graph convolutional networks: A deep learning framework for ride-hailing demand prediction, *Math. Biosci. Eng*., **21** (2024), 2542–2567. https://doi.org/10.3934/mbe.2024112
2. M. Chen, F. Qiu, X. Xiong, Z. Chang, Y. Wei, J. Wu, BILSTM-SimAM: An improved algorithm for short-term electric load forecasting based on multi-feature, *Math. Biosci. Eng*., **21** (2024), 2323–2343. https://doi.org/ 10.3934/mbe.2024102
3. Y. Bao, Q. Zhao, J. Sun, W. Xu, H. Lu, An edge cloud and Fibonacci-Diffie-Hellman encryption scheme for secure printer data transmission, *Math. Biosci. Eng*., **21** (2024), 96–115. https://doi.org/ 10.3934/mbe.2024005

4. C. Cai, C. Peng, J. Niu, W. Tan, H. Tang, Low distortion reversible database watermarking based on hybrid intelligent algorithm, *Math. Biosci. Eng*., **20** (2023), 21315–21336. https://doi.org/10.3934/mbe.2023943
5. L. Yu, Z. Zhang, Y. Lai, Y. Zhao, F. Mo, Edge computing-based intelligent monitoring system for manhole cover, *Math. Biosci. Eng*., **20** (2023), 18792–18819. https://doi.org/10.3934/mbe.2023833
6. B. C. Douss, R. Abassi, D. Sauveron, State-of-the-art survey of in-vehicle protocols and automotive Ethernet security and vulnerabilities, *Math. Biosci. Eng*., **20** (2023), 17057–17095. https://doi.org/10.3934/mbe.2023761
7. Y. Zhu, H. Wen, J. Wu, R. Zhao, Online data poisoning attack against edge AI paradigm for IoT-enabled smart city, *Math. Biosci. Eng*., **20** (2023), 17726–17746. https://doi.org/10.3934/mbe.2023788
8. Y. Pan, J. Yang, L. Zhu, L. Yao, B. Zhang, Aerial images object detection method based on cross-scale multi-feature fusion, *Math. Biosci. Eng.*, **20** (2023), 16148–16168. https://doi.org/10.3934/mbe.2023721
9. F. Wang, Z. Zhang, K. Wu, D. Jian, Q. Chen, C. Zhang, L. Dong, Artificial intelligence techniques for ground fault line selection in power systems: State-of-the-art and research challenges, *Math. Biosci. Eng*., **20** (2023), 14518–14549. https://doi.org/ 10.3934/mbe.2023650
10. M. Firdaus, S. Noh, Z. Qian, H. T. Larasati, K. H. Rhee, Personalized federated learning for heterogeneous data: A distributed edge clustering approach, *Math. Biosci. Eng*., **20** (2023), 10725–10740. https://doi.org/10.3934/mbe.2023475
11. S. Yu, Y. Won, A survey of methods for encrypted network traffic fingerprinting, *Math. Biosci. Eng*., **20** (2023), 2183–2202. https://doi.org/ 10.3934/mbe.2023101
12. C. Shin, S. H. Hong, H. Jeong, H. Yoon, B. Koh, All-in-one encoder/decoder approach for non-destructive identification of 3D-printed objects, *Math. Biosci. Eng*., **19** (2022), 14102–14115. https://doi.org/10.3934/mbe.2022657
13. Z. Yang, Y. Bao, Y. Liu, Q. Zhao, H. Zheng, W. Xu, Lightweight blockchain fuzzy decision scheme through MQTT and Fibonacci for sustainable transport, *Math. Biosci. Eng*., **19** (2022), 11935–11956. https://doi.org/10.3934/mbe.2022556
14. M. M. Salim, J. Kang, Y. Pan, J. H. Park, A lightweight authentication scheme for IoT against rogue base station attacks, *Math. Biosci. Eng*., **19** (2022), 11735–11755. https://doi.org/10.3934/mbe.2022546

AIMS Press