sustainability

MDPI

Editorial

Secure, Sustainable Smart Cities and the Internet of Things: Perspectives, Challenges, and Future Directions

Iqram Hussain

Department of Anesthesiology, Weill Cornell Medicine, New York, NY 10065, USA; iqh4001@med.cornell.edu

1. Perspectives

A secure smart city integrates advanced technologies to enhance efficiency, sustainability, and safety while safeguarding citizens' privacy and data. Through interconnected Internet of Things (IoT) devices, real-time monitoring, and data analytics, a city can optimize transportation, healthcare, energy usage, waste management, and public services. Robust encryption protocols and cybersecurity measures are implemented to protect against cyber threats and unauthorized access to sensitive information [1].

In a secure smart healthcare system, cutting-edge technologies converge to optimize patient care while safeguarding sensitive data. Advanced encryption protocols ensure the confidentiality of patient information, while robust authentication mechanisms guarantee secure access to medical records. Interconnected IoT devices monitor patients remotely, enabling real-time health data collection and analysis [2]. Artificial intelligence algorithms process these data to predict health trends and provide personalized treatment recommendations [3,4]. Additionally, blockchain technology maintains immutable records of medical transactions, enhancing transparency and accountability across the healthcare ecosystem.

Secure smart transportation systems form the backbone of efficient urban mobility in a smart city. Integrated with advanced technologies such as IoT sensors, AI-driven traffic management systems, and encrypted communication networks, these transportation networks ensure seamless and safe journeys for citizens [5,6]. Robust authentication protocols and encryption mechanisms safeguard user data and transactions, mitigating cybersecurity threats.

Secure smart energy systems integrate advanced technologies to ensure the reliable, efficient, and resilient delivery of energy while addressing cybersecurity challenges. These systems leverage interconnected devices, data analytics, and automation to optimize energy generation, distribution, and consumption. Advanced authentication mechanisms, such as biometrics and multifactor authentication, mitigate unauthorized access, while continuous monitoring and response strategies enable real-time threat detection and mitigation.

In the context of illuminating recent advancements, technologies, and case studies related to sustainability, smart cities, smart health, data-driven technology, and the IoT, this Special Issue entitled "Secure, Sustainable Smart Cities, and the IoT" (available at https://www.mdpi.com/journal/sustainability/special_issues/7SKG529PVX, accessed on 3 February 2024) comprehensively explores a multitude of research endeavors in this domain. We express our gratitude to all of the authors who contributed to the success of this Special Issue. In this Editorial, perspectives, challenges, and future directions for secure, sustainable smart cities and the IoT are explored.

2. Summary of This Special Issue

The articles within the present Special Issue encompass the most promising approaches and ideas across various domains, including sustainable transportation, smart grid technologies, smart healthcare, security and privacy measures, and other pertinent areas.

check for updates

Citation: Hussain, I. Secure, Sustainable Smart Cities and the Internet of Things: Perspectives, Challenges, and Future Directions. *Sustainability* **2024**, *16*, 1390. https://doi.org/10.3390/su16041390

Received: 4 February 2024
Accepted: 5 February 2024
Published: 6 February 2024

Akhilesh et al. (Contribution 1) introduced the dynamic aware transmission range parallel Euclidean distance (DA-TRPED) technique to enhance intelligent vehicular clustering routing protocols. They incorporated heuristic-based solutions within an enhanced ant colony optimizer (ACO) framework to evaluate vehicular nodes based on parallel Euclidean distance (PED), simplifying the search process. This enhancement was reflected in performance metrics such as data packet delivery, data packet drop, lifetime analysis, and other parameters of vehicular ad hoc network (VANET) clustered nodes.

Shokry et al. (Contribution 2) assessed information security risk assessment (ISRA) for advanced metering infrastructure (AMI) by harmonizing evaluation criteria for energy metering systems with ISRA methodologies in smart grid applications. Their study offers an extensive comparison of cutting-edge ISRA techniques, considering various input specifications, tool characteristics, and risk assessment methodologies. Furthermore, the research explored crucial prerequisites for AMI system risk evaluations and matched AMI risk assessment requirements with multiple ISRA approaches to determine the most appropriate method in smart grid contexts.

Sunil et al. (Contribution 3) focused on developing an authentication protocol ensuring data privacy and security in smart city applications while maintaining a minimalist model. The proposed framework enabled secure access to smart city applications via the IoT environment, ensuring mutual authentication between users and gateways. Security analysis confirmed the framework's effectiveness in minimizing energy consumption and computational overhead. Performance evaluation using BAN logic and AVISPA security verification tools demonstrated its reliability and superior performance compared to existing methods.

Ali et al. (Contribution 4) introduced a novel hybrid trust management approach for enhancing the security and privacy of IoT-based smart parking systems. Integrating machine learning approaches, they focused on trustworthiness, accessibility, and confidence as key parameters. Employing ensemble machine learning techniques, they ensured efficient system performance and reliability, achieving impressive results in identifying and neutralizing malicious or compromised nodes.

Egala et al. (Contribution 5) presented Coviblock as a blockchain-based decentralized distributed assistance system, aimed at protecting the privacy and security of electronic health records (EHRs) during the pandemic. The researchers suggested a decentralized distributed storage system (DDSS) and a distributed, decentralized resource access control (DDRAC) approach to uphold data privacy. Using an Ethereum test network exhibited Coviblock's real-time functionality and markedly enhanced performance compared to prevailing cloud-based healthcare cyber–physical systems (CPSs) utilizing blockchain methodology.

3. Challenges and Future Directions

The advancement of research in secure, sustainable smart cities and the IoT entails addressing multifaceted challenges while exploring promising avenues for future investigation. A primary hurdle involves fortifying cybersecurity measures to counter potential cyber threats and breaches within smart city infrastructures and IoT networks. Interoperability issues among diverse IoT devices and systems also present a significant challenge, necessitating standardization efforts and innovative solutions for seamless integration. Moreover, privacy concerns surrounding data collection, storage, and utilization in smart city environments underscore the need for developing privacy-preserving technologies and regulatory frameworks. Energy efficiency and sustainability emerge as critical imperatives, prompting the optimization of energy consumption and the integration of renewable energy sources within smart city architectures. Future research endeavors may delve into novel methodologies to enhance the resilience, scalability, and adaptability of smart city systems, leveraging emerging technologies such as edge computing, blockchain, and artificial intelligence. Interdisciplinary collaboration and stakeholder engagement will play pivotal roles in addressing these challenges and unlocking the full potential of secure, sustainable smart cities and the IoT.

Conflicts of Interest: The author declares no conflicts of interest.

List of Contributions:

1. Bijalwan, A.; Hussain, I.; Purohit, K.C.; Kumar, M.A. Enhanced Ant Colony Optimization for Vehicular Ad Hoc Networks Using Fittest Node Clustering. *Sustainability* **2023**, *15*, 15903.
2. Shokry, M.; Awad, A.I.; Abd-Ellah, M.K.; Khalaf, A.A. When Security Risk Assessment Meets Advanced Metering Infrastructure: Identifying the Appropriate Method. *Sustainability* **2023**, *15*, 9812.
3. Gupta, S.; Alharbi, F.; Alshahrani, R.; Kumar Arya, P.; Vyas, S.; Elkamchouchi, D.H.; Soufiene, B.O. Secure and Lightweight Authentication Protocol for Privacy Preserving Communications in Smart City Applications. *Sustainability* **2023**, *15*, 5346.
4. Ali, J.; Khan, M.F. A Trust-Based Secure Parking Allocation for Iot-Enabled Sustainable Smart Cities. *Sustainability* **2023**, *15*, 6916.
5. Egala, B.S.; Pradhan, A.K.; Gupta, S.; Sahoo, K.S.; Bilal, M.; Kwak, K.S. Coviblock: A Secure Blockchain-Based Smart Healthcare Assisting System. *Sustainability* **2022**, *14*, 16844.

References

1. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of Things for Smart Cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. [CrossRef]
2. Islam, M.S.; Hussain, I.; Rahman, M.M.; Park, S.J.; Hossain, M.A. Explainable Ai Model for Stroke Prediction Using Eeg Signal. *Sensors* **2022**, *22*, 9859. [CrossRef] [PubMed]
3. Hussain, I.; Park, S.J. Healthsos: Real-Time Health Monitoring System for Stroke Prognostics. *IEEE Access* **2020**, *8*, 213574–213586. [CrossRef]
4. Hussain, I.; Park, S.J. Big-Ecg: Cardiographic Predictive Cyber-Physical System for Stroke Management. *IEEE Access* **2021**, *9*, 123146–123164. [CrossRef]
5. Park, S.J.; Hong, S.; Kim, D.; Hussain, I.; Seo, Y. Intelligent in-Car Health Monitoring System for Elderly Drivers in Connected Car. In Proceedings of the 20th Congress of the International Ergonomics Association (IEA 2018), Florence, Italy, 26–30 August 2018.
6. Hussain, I.; Young, S.; Park, S.J. Driving-Induced Neurological Biomarkers in an Advanced Driver-Assistance System. *Sensors* **2021**, *21*, 6985. [CrossRef] [PubMed]