IoT and Sustainable Smart Cities

Subjects: Computer Science, Artificial Intelligence

Contributor: Khalid Haseeb

The Internet of Things (IoT) is an emerging technology and provides connectivity with the physical world using the support of 5G communication. In recent decades, there have been a lot of applications based on IoT technology for the sustainability of smart cities, such as farming, e-healthcare, education, smart homes, weather monitoring, etc. These applications communicate in a collaborative manner between embedded IoT devices and systematize daily routine tasks. However, it is observed that transmission system in constraint oriented network is still a burning research issue in smart cities. Also, there is an existence of a lot of malicious machines that can damage sustainable services of smart cities and compromised the connected devices. Thus, proposing an efficient solution using a 5G system is a demanding task for a smart environment that efficiently utilizes the communication resources and securing the data over insecure routes.

Internet of Things 5G sustainable routing mobile networks smart cities data security

1. Introduction

IoT is a network of intelligent devices that exchange online data and support sustainable services. In all aspects of daily life, IoT plays a significant role with the integration of next-generation 5G networks [1][2][3] to facilitate many areas such as healthcare, vehicles, entertainment, industrial equipment, sport, homes, social networking, etc. IoT is one of the most advanced developments in the last century and has been used in many applications, but still, privacy and authentication are among research challenges [4][5][6] for sustainable computing. On the other hand, the number of connected devices is being increased consistently and their number has surpassed 50 billion, with the data produced by these devices also increasing exponentially. Indeed, the overall ubiquity of IoT facilitates day-to-day activities and enables people to interact with each other using 5G networks [7][8]. However, this holistic view also raises security issues such as data preserving, botnet attacks, hijacking IoT devices, etc.

The main challenges faced in IoT applications are manufacturing standards, update management, physical hardening, user knowledge, and awareness [9][10]. As a result, various IoT structures have been used to build and launch many IoT security applications. An IoT structure is a set of instructions, protocols, and specifications that simplifies the implementation of IoT. The accomplishment of these applications depends primarily on the characteristics of the IoT framework's ecosystems, with a special focus on safety mechanisms where protection and privacy problems are of vital importance [11][12][13]. Traditional IoT architecture is composed of three physical, network, and application layers. Devices are embedded in the physical layer that employ certain techniques to

sense the environment and perform wireless communication to other devices [14][15][16]. A lot of research work has reported on IoT protection and privacy issues. However, once the latest technology arrives, it will overcome the security dilemma in IoT as well.

IoT has various uses in real-time contexts and therefore has made a huge impact in almost every sector of life. It combines sensors, smart devices, and RFID technologies through the Internet to create intelligent coordination. The sensors are tiny energy-constrained devices employed to sense information and deliver it over the network for intelligent decisions. These networks in an IoT environment come in a different structure, such as distributed, ubiquitous, grid, and vehicular. However, due to rapid development, extensive use, and their ubiquitous nature, IoT networks face various protection, privacy, and vulnerability issues in their applications and infrastructure. A few works on these security issues reported in the literature mainly employed machine learning and blockchain approaches. Different researchers have worked on different security aspects of IoT networks, including privacy preservation [17][18][19], authentications [20][21][22], access control [23][24][25], scalability [26][27][28], information sharing [29][30][31], and trust management [32][33][34]. However, proposing a decentralized communication platform for facilitating connected users over the insecure Internet and mobile network is a demanding task. In addition, the gathered data should be transmitted without compromising the identification of nodes and sensitive information. **Figure 1** illustrates the components of the proposed architecture. The proposed architecture presents a sustainable development for public health applications, which is a significant factor in optimizing the system management and flow of information to assist society. It utilizes the technology of IoT, sensors, and 5G to share the resources and communication bandwidth efficiently. In addition, the cooperation of mobile sink highly distributes a load of IoT technology using the 5G network and increases mobility support and resource management.

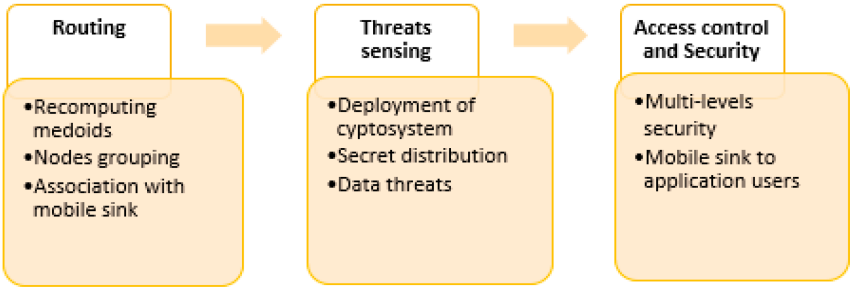

Figure 1. Main components of the proposed architecture.

2. Related work

In [35], the authors defined the required infrastructure and the protocol for the secure implementation of the IoT framework. They identified several new methods that could be used to address IoT security problems using machine learning and blockchain-based approaches. Advance 5G wireless sensor technologies [36][37] facilitate mobile communication for complex and highly dynamic environments. These technologies acquiring the information by sensing the data from a real-world environment and transmit to a sink node to fulfill the demands of the application users. To collaborate with mobile IoT networks, the solution should be robust and more reliable to support the requests of application users. In [38], the authors investigated the outage probability (OP) and predicted

wireless communication. It was based on the improved grey wolf optimization algorithm and an Elman neural network was proposed. The simulation-based results illustrate that the prediction accuracy was higher than other solutions and managed the wireless transmission system more accurately for mobile IoT networks. The authors in [39] proposed an Internet of Things-based WBAN for disaster cases. It ensures life savings and smooth communication using technologies of the wireless network. In addition, a gateway selection algorithm using fuzzy logic was developed that aims to select a suitable wireless communication technology.

The authors in [40] maximized the task throughput for the IoT-enabled 5G network in the presence of heterogeneous task demands and constraint resources. They utilized multi-graph coloring and proposed an efficient two-stage process. The computational complexity and correctness of the proposed algorithm were analyzed. The simulation-based results demonstrate its efficacy against existing work. The authors in [41] suggested a rigorous prediction model using a rule-based machine learning classification method, i.e., the decision tree, on the noise-free accuracy dataset for real-life cell phone data of individual users. The Naive Bayes classifier and Laplace estimator were used to increase the model's prediction accuracy by minimizing noisy instances in the results. In [42], for Industrial Internet of Things (IIoT) devices, a machine learning-based anomaly detection system was proposed to detect cyber threats such as backdoor, order injection, and Structured Query Language (SQL) injection attacks. A distributed ledger-based blockchain (DLBC) technology was recommended in [43] to fix IoT protection and privacy problems such as spoofing and false authentication. In [44], a distributed intelligence system was proposed to reduce unnecessary data transfer to the cloud through immediate decision-making. They also resolved several security issues in the IoT environment using blockchain technology.

In [45], classified devices with an ML approach were used to boost IoT environment security by identifying malicious data in the blockchain network. Similarly, a trust protection mechanism was introduced in [46] to provide stable and effective access control to identify and remove intrusions in a distributed IoT system. The authors in [47] presented a Safe Private Blockchain (SPB) that allows energy prosumers to negotiate energy rates and share energy with an IoT smart grid deployment. It consists of a three-layered trust management system in which trust is tracked based on the interactions between supply chain members, and trust. Finally, credibility is dynamically allocated based on these interaction scores [48]. In [49], a blockchain-based, privacy-preserving update protocol was suggested that allows users to update apps but also preserve their privacy. It increases the security level as compared to an existing solution with improved network performance. The authors in [50] proposed a clustering perturbation algorithm to preserve privacy for social networks that aim to introduce a strategy of exchanging attributes among vertices of the same degree randomly. It makes the network attackers pursue fake targets and accordingly maintains the stable structure of the observing field. In [51], the authors proposed a deep-reinforcement-learning-based quality-of-service (QoS)-aware secure routing protocol (DQSP). It ensures the QoS along with the extraction of knowledge from traffic history. In addition, it optimizes the routing policy and improves the data delivery performance against other solutions. The authors in [52] proposed a telemedicine system based on MEC and artificial intelligence for remote health monitoring and automatic disease diagnosis. The concept of mobile edge computing (MEC) among users and cloud systems reduces the problem of 5G scenarios in terms of latency and processing. Different computing technologies are also utilized in the proposed solution to significantly improve the efficacy of the patient treatment by decreasing the computing cost using an intelligent paradigm.

IoT technology has gained prominent attention for the development of sustainable smart cities with the support of a 5G network. **Table 1** describes the research findings along with limitations based on the discussed work.

Table 1. Summary of discussed work.

	Contributions and Limitations
Existing solutions	• Many solutions offer quality-aware services and lead to higher bandwidth and improved data delivery performance. • However, most of the solutions face connectivity problems when the load on IoT nodes increases especially in 5G mobile networks. • Due to frequent network disconnectivity issues, it was also observed that most of the proposed solutions have a high data latency for real-time applications. • It was also noticed that 5G communication offers attention to many real-world network technologies for the growth of promising solutions with the collaboration of cloud and mobile infrastructure. • However, most of the network technologies with the collaboration of the 5G network lack security and communication trust.
Proposed architecture	A solution was developed using a 5G network for real-time public health application that increases the sustainability of complex operations in the presence of unpredictable events. It also facilitates application users with high communication bandwidth and optimal performance.

3. Conclusions

We proposed a mobility support 5G architecture with real-time routing for sustainable smart cities. Its main factors are highlighted as follows:

i. It supports the delivery of online data with a high level of security and network continuity for mobile networks. Unlike other traditional approaches, it leads to few data delays and decreases the processing cost with the availability of higher bandwidth.
ii. It also secures the 5G ecosystem with a nominal risk rate and supports trustworthy communication. The mobile sink collaborates with both gateway nodes and medical storage centers to gather the IoT data, which explicitly increases the success rate of sensitive data with optimum delay.
iii. Moreover, instead of only securing the boundary points for data routing, the proposed architecture performs risk analysis for the IoT nodes and links. The proposed architecture was tested and evaluated against existing work in terms of various experiments and it was seen to have significantly

better performance. The multi-level security secures the routing for next-generation networks without imposing additional resource usage.

However, it was observed that the proposed architecture still lacks intelligence in distributing the IoT data on established routes and leads to communication complexity when network nodes increase. Therefore, its aim is to introduce some machine learning schemes to train the proposed architecture with nominal latency and support emergency communications.

References

1. Wang, D.; Chen, D.; Song, B.; Guizani, N.; Yu, X.; Du, X. From IoT to 5G I-IoT: The Next Generation IoT-Based Intelligent Algorithms and 5G Technologies. IEEE Commun. Mag. 2018, 56, 114–120.
2. Haseeb, K.; Islam, N.; Saba, T.; Rehman, A.; Mehmood, Z. LSDAR: A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks. Sustain. Cities Soc. 2019, 54, 101995.
3. Lloret, J.; Parra, L.; Taha, M.; Tomás, J. An architecture and protocol for smart continuous eHealth monitoring using 5G. Comput. Netw. 2017, 129, 340–351.
4. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet Things 2020, 11, 100227.
5. Singh, S.; Sharma, P.K.; Yoon, B.; Shojafar, M.; Cho, G.H.; Ra, I.-H. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. Sustain. Cities Soc. 2020, 63, 102364.
6. Saba, T.; Haseeb, K.; Ahmed, I.; Rehman, A. Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. J. Infect. Public Health 2020, 13, 1567–1575.
7. González-Landero, F.; García-Magariño, I.; Lacuesta, R.; Lloret, J. PriorityNet App: A mobile application for establishing priorities in the context of 5G ultra-dense networks. IEEE Access 2018, 6, 14141–14150.
8. Sharma, T.; Chehri, A.; Fortier, P. Review of optical and wireless backhaul networks and emerging trends of next generation 5G and 6G technologies. Trans. Emerg. Telecommun. Technol. 2020, 32, e4155.
9. Haseeb, K.; Almogren, A.; Din, I.U.; Islam, N.; Altameem, A. SASC: Secure and Authentication-Based Sensor Cloud Architecture for Intelligent Internet of Things. Sensors 2020, 20, 2468.

10. Taha, M.; Parra, L.; Garcia, L.; Lloret, J. An Intelligent handover process algorithm in 5G networks: The use case of mobile cameras for environmental surveillance. In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 21–25 May 2017.
11. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M.S. Internet of Things (IoT): A vision, architectural elements, and future directions. Futur. Gener. Comput. Syst. 2013, 29, 1645–1660.
12. Elrawy, M.F.; Awad, A.I.; Hamed, H.F. Intrusion detection systems for IoT-based smart environments: A survey. J. Cloud Comput. 2018, 7, 1–20.
13. Rehman, A.; Haseeb, K.; Saba, T.; Lloret, J.; Tariq, U. Secured Big Data Analytics for Decision-Oriented Medical System Using Internet of Things. Electronics 2021, 10, 1273.
14. Kotenko, I.; Saenko, I.; Branitskiy, A. Framework for Mobile Internet of Things Security Monitoring Based on Big Data Processing and Machine Learning. IEEE Access 2018, 6, 72714–72723.
15. Ren, J.; Guo, H.; Xu, C.; Zhang, Y. Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing. IEEE Netw. 2017, 31, 96–105.
16. Yelamarthi, K.; Aman, S.; AbdelGawad, A. An Application-Driven Modular IoT Architecture. Wirel. Commun. Mob. Comput. 2017, 2017, 1–16.
17. Sagirlar, G.; Carminati, B.; Ferrari, E. Decentralizing privacy enforcement for Internet of Things smart objects. Comput. Netw. 2018, 143, 112–125.
18. Lv, P.; Wang, L.; Zhu, H.; Deng, W.; Gu, L. An IOT-Oriented Privacy-Preserving Publish/Subscribe Model Over Blockchains. IEEE Access 2019, 7, 41309–41314.
19. Saba, T.; Haseeb, K.; Shah, A.A.; Rehman, A.; Tariq, U.; Mehmood, Z. A Machine-Learning-Based Approach for Autonomous IoT Security. IT Prof. 2021, 23, 69–75.
20. Hossain, E.; Khan, I.; Un-Noor, F.; Sikander, S.S.; Sunny, S.H. Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review. IEEE Access 2019, 7, 13960–13988.
21. Liu, Z.; Seo, H. IoT-NUMS: Evaluating NUMS Elliptic Curve Cryptography for IoT Platforms. IEEE Trans. Inf. Forensics Secur. 2018, 14, 720–729.
22. Mohanta, B.K.; Sahoo, A.; Patel, S.; Panda, S.S.; Jena, D.; Gountia, D. Decauth: Decentralized authentication scheme for iot device using ethereum blockchain. In Proceedings of the TENCON 2019-2019 IEEE Region 10 Conference (TENCON), Kochi, India, 17–20 October 2019.
23. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Commun. Surv. Tutorials 2019, 21, 2671–2701.

24. Ali, G.; Ahmad, N.; Cao, Y.; Asif, S.; Cruickshank, H.; Ali, Q.E. Blockchain based permission delegation and access control in Internet of Things (BACI). Comput. Secur. 2019, 86, 318–334.
25. Qiu, J.; Tian, Z.; Du, C.; Zuo, Q.; Su, S.; Fang, B. A Survey on Access Control in the Age of Internet of Things. IEEE Internet Things J. 2020, 7, 4682–4696.
26. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. J. Parallel Distrib. Comput. 2019, 134, 180–197.
27. Rehman, A.; Haseeb, K.; Saba, T.; Kolivand, H. M-SMDM: A model of security measures using Green Internet of Things with Cloud Integrated Data Management for Smart Cities. Environ. Technol. Innov. 2021, 24, 101802.
28. Arellanes, D.; Lau, K.-K. Evaluating IoT service composition mechanisms for the scalability of IoT systems. Futur. Gener. Comput. Syst. 2020, 108, 827–848.
29. Si, H.; Sun, C.; Li, Y.; Qiao, H.; Shi, L. IoT information sharing security mechanism based on blockchain technology. Futur. Gener. Comput. Syst. 2019, 101, 1028–1040.
30. Li, Z.; Liu, L.; Barenji, A.V.; Wang, W. Cloud-based Manufacturing Blockchain: Secure Knowledge Sharing for Injection Mould Redesign. Procedia CIRP 2018, 72, 961–966.
31. Gope, P.; Gheraibia, Y.; Kabir, S.; Sikdar, B. A secure IoT-based modern healthcare system with fault-tolerant decision making process. IEEE J. Biomed. Health Inform. 2020, 25, 862–873.
32. Danzi, P.; Kalor, A.E.; Stefanovic, C.; Popovski, P. Delay and Communication Tradeoffs for Blockchain Systems With Lightweight IoT Clients. IEEE Internet Things J. 2019, 6, 2354–2365.
33. Wang, N.; Jiang, T.; Lv, S.; Xiao, L. Physical-Layer Authentication Based on Extreme Learning Machine. IEEE Commun. Lett. 2017, 21, 1557–1560.
34. Xu, X.; Liu, X.; Xu, Z.; Dai, F.; Zhang, X.; Qi, L. Trust-Oriented IoT Service Placement for Smart Cities in Edge Computing. IEEE Internet Things J. 2019, 7, 4084–4091.
35. Dedeoglu, V.; Jurdak, R.; Dorri, A.; Lunardi, R.; Michelin, R.; Zorzo, A.; Kanhere, S. Blockchain Technologies for iot. In Advanced Applications of Blockchain Technology; Lee, S.-W., Singh, I., Mohammadian, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 55–89.
36. Sadowski, S.; Spachos, P. Wireless technologies for smart agricultural monitoring using internet of things devices with energy harvesting capabilities. Comput. Electron. Agric. 2020, 172, 105338.
37. Wang, N.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; Zeng, K. Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. IEEE Internet Things J. 2019, 6, 8169–8181.
38. Xu, L.; Yu, X.; Gulliver, T.A. Intelligent Outage Probability Prediction for Mobile IoT Networks Based on an IGWO-Elman Neural Network. IEEE Trans. Veh. Technol. 2021, 70, 1365–1375.

39. Cicioğlu, M.; Çalhan, A. IoT-based wireless body area networks for disaster cases. Int. J. Commun. Syst. 2018, 33, e3864.
40. Pratap, A.; Gupta, R.; Nadendla, V.S.S.; Das, S.K. Bandwidth-constrained task throughput maximization in IoT-enabled 5G networks. Pervasive Mob. Comput. 2020, 69, 101281.
41. Sarker, I.H. A machine learning based robust prediction model for real-life mobile phone data. Internet Things 2019, 5, 180–193.
42. Zolanvari, M.; Teixeira, M.A.; Gupta, L.; Khan, K.M.; Jain, R. Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things. IEEE Internet Things J. 2019, 6, 6822–6834.
43. Kumar, N.M.; Mallick, P.K. Blockchain technology for security issues and challenges in IoT. Procedia Comput. Sci. 2018, 132, 1815–1823.
44. Sadique, K.M.; Rahmani, R.; Johannesson, P. Towards Security on Internet of Things: Applications and Challenges in Technology. Procedia Comput. Sci. 2018, 141, 199–206.
45. Dorri, A.; Roulin, C.; Jurdak, R.; Kanhere, S.S. On the activity privacy of blockchain for IoT. In Proceedings of the 2019 IEEE 44th Conference on Local Computer Networks (LCN), Osnabrück, Germany, 14–17 October 2019.
46. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trust management in decentralized IoT access control system. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020.
47. Dorri, A.; Luo, F.; Kanhere, S.S.; Jurdak, R.; Dong, Z.Y. SPB: A secure private blockchain-based solution for distributed energy trading. IEEE Commun. Mag. 2019, 57, 120–126.
48. Malik, S.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trustchain: Trust management in blockchain and iot supported supply chains. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Seoul, Korea, 14–17 July 2019.
49. Zhao, Y.; Liu, Y.; Tian, A.; Yu, Y.; Du, X. Blockchain based privacy-preserving software updates with proof-of-delivery for Internet of Things. J. Parallel Distrib. Comput. 2019, 132, 141–149.
50. Yu, F.; Chen, M.; Yu, B.; Li, W.; Ma, L.; Gao, H. Privacy preservation based on clustering perturbation algorithm for social network. Multimedia Tools Appl. 2017, 77, 11241–11258.
51. Guo, X.; Lin, H.; Li, Z.; Peng, M. Deep-reinforcement-learning-based QoS-aware secure routing for SDN-IoT. IEEE Internet Things J. 2019, 7, 6242–6251.
52. Zhang, Y.; Chen, G.; Du, H.; Yuan, X.; Kadoch, M.; Cheriet, M. Real-time remote health monitoring system driven by 5G MEC-IoT. Electronics 2020, 9, 1753.