Use of AI-Based Drones in Smart Cities

Imdad Ali Shah (/affiliate/imdad-ali-shah/436254/), Noor Zaman Jhanjhi (/affiliate/noor-zaman-jhanjhi/436256/), Sarfraz Nawaz Brohi (/affiliate/sarfraz-nawaz-brohi/463061/)

Source Title: Cybersecurity Issues and Challenges in the Drone Industry (/gateway/book/324607)

Pages: 19
ISBN13: 9798369307748ISBN13 Softcover: 9798369345627EISBN13: 9798369307755
DOI: 10.4018/979-8-3693-0774-8.ch015

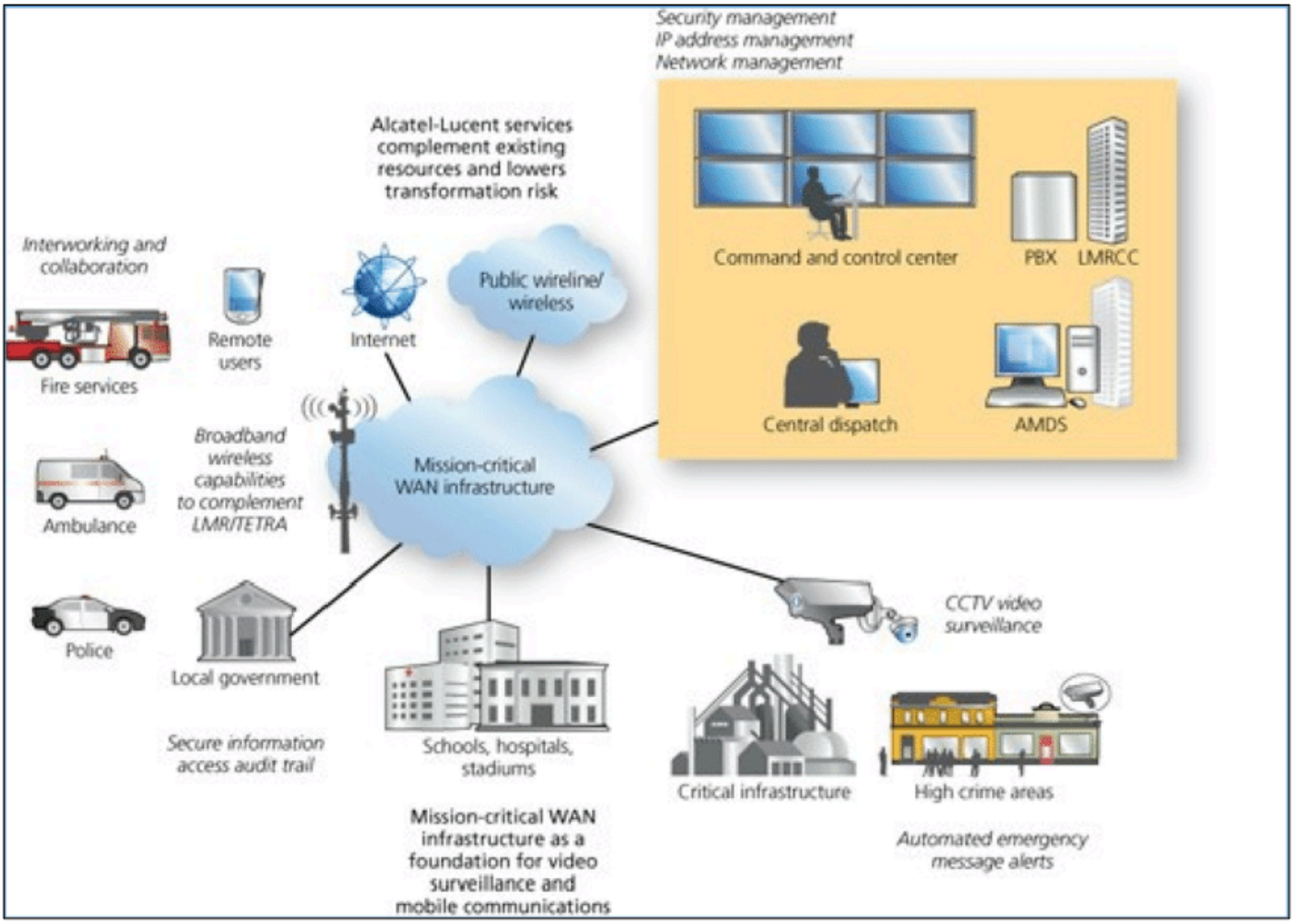
Abstract

Autonomous drones, known as AI drones, have been working without human intervention. It is doing something like navigation, avoiding obstacles, and taking picture recognition without explicit human direction, thanks to AI technology. It's an advantage of AI-based drones that they are capable of flying without human intervention. This can be used for missions such as monitoring searches and rescue operations in remote areas where human lives are at risk. Because of their sophisticated cameras and detectors, AI-based drones are able to collect and analyze large amounts of data in real-time. With this data, comprehensive maps may be made, locations of interest can be found, and the situational awareness of human operators can be improved. These days, the concept of a “smart city” intrigues everyone. Advanced technologies such as AI, blockchain, the IoT, drones, and many more are integrated.

1. Introduction

Smart city integration of AI-based drones has many advantages, including improved infrastructure monitoring, emergency response, and surveillance. However, using these drones also raises several security issues requiring careful attention. Artificial intelligence is one of the most rapidly developing and commonly used technologies in the modern era. AI uses simulations of human brain activity to address practical issues. Robots, smart cars, prediction, e-commerce, navigation, human resources, and healthcare are a few examples of applications for AI farming, video games, cars, social networking, and marketing. Security is a crucial concern (Alsamhi, S., 2018). Issues affecting individuals, groups, or societies are handled with synthetic intelligence. AI security is using artificial intelligence in tools and procedures (Alsamhi, S.; Rajput, N., 2016). They use AI to recognize and react to potential cyber threats based on similarities. AI and machine learning can assist in keeping up with cyber criminals, automating threat detection, and responding more efficiently than traditional software-driven or manual techniques in the face of cyberattacks and the exponential growth of devices today (Alsamhi, S.H., 2018; Al-Hourani, A., 2017). This is an intriguing area where AI can compete. The usage of AI extends beyond the previously mentioned application areas. One of the technologies that works best for managing smart cities is AI. Numerous publications in the same field have highlighted the importance of AI for smart cities. AI applications for smart cities include identity management, smart traffic, smart grid, precision farming, and smart healthcare. Appropriately and successfully using AI-based drones in smart cities depends on addressing these security issues (Alzenad, M., 2020). A comprehensive approach combining technology, legislation, and public awareness is required to ensure that the advantages of drone technology are achieved while reducing associated risks. An overview of the public safety network is in Figure 1.

Figure 1. Overview of Public Safety Network adopted from Tomasino 35 al. (2017)



(https://igiprodst.blob.core.windows.net:443/source-content/9798369307748_324607/979-8-3693-0774-8.ch015.f01.png?sv=2015-12-11&sr=c&sig=z0%2BGq4sMXffd26jTAzfwCAdwMwupHKmI3dVAPTj53qs%3D&se=2024-10-28T16%3A28%3A59Z&sp=r)

Wearable technology cannot transmit data long distances due to its low transmission power. However, drone technology can provide real-time services over a vast geographic area (B. Bera et al., 2020). Drone technology is the most affordable and effective means to

real-time services over a vast geographic area (D. Bera et al., 2020). Drone technology is the most affordable and effective means to track down a fleeing criminal, locate a missing person, and examine a disaster site.

The chapter will focus on the following points.

1. This chapter focused on drone technology.
2. This chapter focused on drones and smart cities.
3. This chapter focused on the Security Concerns of using drones in smart cities.
4. This chapter discusses the privacy violation of drones.
4. This chapter provides future directions.

2. Literature Review

AI-powered drones are becoming a bigger and bigger component of smart city ecosystems. They offer the capacity to gather data in real time, keep an eye on infrastructure, and respond swiftly to emergencies. Thanks to advanced AI algorithms, these drones can perform tasks independently, which makes them perfect for use by law enforcement, emergency response teams, and urban planners. Drones powered by AI and integrated into smart cities have the potential to transform many aspects of urban life, including infrastructure management and emergency response (A. Brokaw, 2016). These drones employ artificial intelligence to enhance data collection, decision-making, and surveillance procedures. The deployment of smart cities also presents a number of security challenges and difficulties that must be properly addressed in order to protect the privacy and security of their inhabitants. Here's a summary of the challenges and security risks associated with employing AI-powered drones in smart cities.

References

Al-Hourani A. Chandrasekharan S. Kandeepan S. Jamalipour A. (2017). Aerial platforms for public safety networks and performance optimization. In Wireless Public Safety Networks 3 (pp. 133–152). Elsevier. 10.1016/B978-1-78548-053-9.50007-X

Alladi. (2020). SecAuthUAV: A Novel Authentication Scheme for UAVGround Station and UAV-UAV Communication. *IEEE Trans. Vehic. Tech.*, *69*(12), 68–77.

Alsamhi, S., Ma, O., & Ansari, M. (2018). *Artificial Intelligence-Based Techniques for Emerging Robotics Communication: A Survey and Future Perspectives*. arXiv:1804.09671

Alsamhi, S., Ma, O., Ansari, M. S., & Meng, Q. (2018). *Greening Internet of Things for Smart Everywhere with a Green Environment Life: A Survey and Future Prospects*. arXiv:1805.00844

Alsamhi S. Rajput N. (2016). An Efficient Channel Reservation Technique for Improved QoS for Mobile Communication Deployment Using High Altitude Platform. Wireless Personal Communications, 91(3), 1095–1108. 10.1007/s11277-016-3514-3

Alsamhi. (2019). Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities. *IEEE Access*, *7*, 128125–52.

Alsamhi S. H. Ansari M. S. Ma O. Almalki F. Gupta S. K. (2018). Tethered Balloon Technology in Design Solutions for Rescue and Relief Team Emergency Communication Services.Disaster Medicine and Public Health Preparedness, 1–8.29789025

Alsamhi S. H. Ansari M. S. Rajput N. S. (2017). Disaster coverage prediction for the emerging tethered balloon technology: Capability for preparedness, detection, mitigation, and response.Disaster Medicine and Public Health Preparedness, 12(2), 222–231. 10.1017/dmp.2017.5428789726

Alzenad M. El-Keyi A. Yanikomeroglu H. (2018). 3D placement of an unmanned aerial vehicle base station for maximum coverage of users with different QoS requirements.IEEE Wireless Communications Letters, 7(1), 38–41. 10.1109/LWC.2017.2752161

Balakrishnan, S., Ruskhan, B., Zhen, L. W., Huang, T. S., Soong, W. T. Y., & Shah, I. A. (2023). Down2Park: Finding New Ways to Park. *Journal of Survey in Fisheries Sciences*, 322-338.

Bera B. Chattaraj D. Das A. K. (2020). Designing Secure Blockchain-Based Access Control Scheme in IoT-Enabled Internet of Drones Deployment. Computer Communications, 153, 229–249. 10.1016/j.comcom.2020.02.011

Bera B. Saha S. Das A. K. Kumar N. Lorenz P. Alazab M. (2020). Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment. IEEE Transactions on Vehicular Technology, 69(8), 9097–9111. 10.1109/TVT.2020.3000576

Bilal, M., Usmani, R. S. A., Tayyab, M., Mahmoud, A. A., Abdalla, R. M., Marjani, M., Pillai, T. R., & Targio Hashem, I. A. (2020). Smart cities data: Framework, applications, and challenges. *Handbook of smart cities*, 1-29.

Brokaw, A. (2016). Autonomous search-and-rescue drones outperform humans at navigating forest trails. *Verge*, *11*. Available online: https://www.theverge.com/2016/2/11/10965414/autonomous-drones-deep-learning-navigation-mapping (https://www.theverge.com/2016/2/11/10965414/autonomous-drones-deep-learning-navigation-mapping)

Follow Reference Chen X. Guo D. (2016). Public Safety Broadband Network with Rapid-deployment Base Stations. In Wireless Public Safety Networks 2 (pp. 173–198). Elsevier. 10.1016/B978-1-78548-052-2.50006-2

Chou, S.-F., Yu, Y.-J., Pang, A.-C., & Lin, T.-A. (2018). Energy-Aware 3D Aerial Small-Cell Deployment over Next Generation Cellular Networks. *Proceedings of the 2018 IEEE 87th Vehicular Technology Conference (VTC Spring),* 1–5.

Dauphin L. Adjih C. Petersen H. Baccelli E. (2017). Low-Cost Robots in the Internet of Things: Hardware, Software & Communication Aspects.Proceedings of the 2017 International Conference on Embedded Wireless Systems and Networks, 284–289.

Dawson, M., & Walker, D. (2022). Argument for Improved Security in Local Governments Within the Economic Community of West African States. *Cybersecurity Measures for E-Government Frameworks*, 96-106.

Follow Reference Dhillon H. S. Huang H. Viswanathan H. (2017). Wide-area wireless communication challenges for the Internet of Things.IEEE Communications Magazine, 55(2), 168–174. 10.1109/MCOM.2017.1500269CM

Follow Reference Favraud R. Apostolaras A. Nikaein N. Korakis T. (2016). Public Safety Networks: Enabling Mobility for Critical Communications. In Wireless Public Safety Networks 2 (pp. 95–126). Elsevier. 10.1016/B978-1-78548-052-2.50004-9

Follow Reference Fraga-Lamas P. Fernández-Caramés T. M. Suárez-Albela M. Castedo L. González-López M. (2016). A review on internet of things for defence and public safety.Sensors (Basel), 16(10), 1644. 10.3390/s1610164427782052

Gautam B. P. Wasaki K. Sharma N. (2016). A novel approach of fault management and restoration of network services in IoT cluster to ensure disaster readiness.Proceedings of the 2016 International Conference on Networking and Network Applications (NaNA),423–428.

Follow Reference Guillen-Perez A. Cano M.-D. (2018). Flying Ad Hoc Networks: A New Domain for Network Communications.Sensors (Basel), 18(10), 3571. 10.3390/s1810357130347892

Follow Reference Hasan H. AlHadhrami E. AlDhaheri A. Salah K. Jayaraman R. (2019). Smart Contract-Based Approach for Efficient Shipment Management. Computers & Industrial Engineering, 136, 149–159. 10.1016/j.cie.2019.07.022

Follow Reference Hassija V. Chamola V. Krishna D. N. G. Guizani M. (2020). A Distributed Framework for Energy Trading Between UAVs and Charging Stations for Critical Applications. IEEE Transactions on Vehicular Technology, 69(5), 5391–5402. 10.1109/TVT.2020.2977036

Follow Reference He X. Yu W. Xu H. Lin J. Yang X. Lu C. Fu X. (2018). Towards 3D Deployment of UAV Base Stations in Uneven Terrain.Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN),1–9. 10.1109/ICCCN.2018.8487319

Follow Reference Hossein Motlagh N. Taleb T. Arouk O. (2016). Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives. IEEE Internet of Things Journal, 3(6), 899–922. 10.1109/JIOT.2016.2612119

Follow Reference Hu B. Wang C. A. Chen S. Wang L. Yang H. (2018). Proactive Coverage Area Decisions Based on Data Field for Drone Base Station Deployment.Sensors (Basel), 18(11), 3917. 10.3390/s1811391730428635

Follow Reference Hussain M. Talpur M. S. H. Humayun M. (2022). The Consequences of Integrity Attacks on E-Governance: Privacy and Security Violation. In Cybersecurity Measures for E-Government Frameworks (pp. 141–156). IGI Global. 10.4018/978-1-7998-9624-1.ch009

Follow Reference Jhanjhi N. Z. Ahmad M. Khan M. A. Hussain M. (2022). The impact of cyber attacks on e-governance during the covid-19 pandemic. In Cybersecurity Measures for E-Government Frameworks (pp. 123–140). IGI Global. 10.4018/978-1-7998-9624-1.ch008

Follow Reference Kiran S. R. A. Rajper S. Shaikh R. A. Shah I. A. Danwar S. H. (2021). Categorization of CVE Based on Vulnerability Software By Using Machine Learning Techniques.International Journal (Toronto, Ont.), 10(3).

Follow Reference Kolios P. Pitsillides A. Mokryn O. Papdaki K. (2016). 7—Data Dissemination in Public Safety Networks. In CâmaraD.NikaeinN. (Eds.), Wireless Public Safety Networks 2 (pp. 199–225). Elsevier. 10.1016/B978-1-78548-052-2.50007-4

Follow Reference Lee E. Seo Y.-D. Oh S.-R. Kim Y.-G. (2021). A Survey on Standards for Interoperability and Security in the Internet of Things. IEEE Communications Surveys and Tutorials, 23(2), 1020–1047. 10.1109/COMST.2021.3067354

Long, T., Ozger, M., Cetinkaya, O., & Akan, O. B. Energy neutral internet of drones. *IEEE Commun. Mag.*, *56*, 22–28.

Follow Reference Mehmood Y. Ahmad F. Yaqoob I. Adnane A. Imran M. Guizani S. (2017). Internet-of-things-based smart cities: Recent advances and challenges.IEEE Communications Magazine, 55(9), 16–24. 10.1109/MCOM.2017.1600514

Follow Reference Mohamed N. Al-Jaroodi J. Jawhar I. Idries A. Mohammed F. (2018). (in press). Unmanned aerial vehicles applications in future smart cities.Technological Forecasting and Social Change.

Mozaffari, M., Kasgari, A. T. Z., Saad, W., Bennis, M., & Debbah, M. (2018). *Beyond 5G with UAVs: Foundations of a 3D Wireless Cellular Network*. arXiv:1805.06532

Follow Reference Mozaffari M. Saad W. Bennis M. Debbah M. (2016). Unmanned aerial vehicle with underlaid device-to-device communications: Performance and tradeoffs.IEEE Transactions on Wireless Communications, 15(6), 3949–3963. 10.1109/TWC.2016.2531652

Mozaffari, M., Saad, W., Bennis, M., Nam, Y.-H., & Debbah, M. (2018). *A tutorial on UAVs for wireless networks: Applications, challenges, and open problems.* arXiv:1803.00680

Follow Reference Msadaa I. C. Dhraief A. (2016). Internet of Things in Support of Public Safety Networks: Opportunities and Challenges. In Wireless Public Safety Networks 2 (pp. 1–23). Elsevier. 10.1016/B978-1-78548-052-2.50001-3

Follow Reference Muzafar S. Humayun M. Hussain S. J. (2022). Emerging Cybersecurity Threats in the Eye of E-Governance in the Current Era. In Cybersecurity Measures for E-Government Frameworks (pp. 43–60). IGI Global. 10.4018/978-1-7998-9624-1.ch003

Follow Reference Naqvi S. A. R. Hassan S. A. Pervaiz H. Ni Q. (2018). Drone-aided communication as a key enable. 5G and resilient public safety networks.IEEE Communications Magazine, 56(1), 36–42. 10.1109/MCOM.2017.1700451

Follow Reference Pahl C. El Ioini N. Helmer S. Lee B. (2018). An architecture pattern for trusted orchestration in IoT edge clouds.Proceedings of the 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC),63–70. 10.1109/FMEC.2018.8364046

Follow Reference Ray P. P. Mukherjee M. Shu L. (2017). Internet of things for disaster management: State-of-the-art and prospects.IEEE Access : Practical Innovations, Open Solutions, 5, 18818–18835. 10.1109/ACCESS.2017.2752174

Follow Reference Reina D. Camp T. Munjal A. Toral S. Tawfik H. (2018). Evolutionary Deployment and Hill Climbing-Based Movements of Multi-UAV Networks in Disaster Scenarios. In Applications of Big Data Analytics (pp. 63–95). Springer. 10.1007/978-3-319-76472-6_4

Follow Reference Reina D. G. Camp T. Munjal A. Toral S. L. (2018). Evolutionary deployment and local search-based movements of 0th responders in disaster scenarios.Future Generation Computer Systems, 88, 61–78. 10.1016/j.future.2018.05.024

Roy Chowdhury, A. (2017). IoT and Robotics: A synergy. *PeerJ Prepr.*, *5*, e2760v1.

Follow Reference Sánchez-García J. García-Campos J. Arzamendia M. Reina D. Toral S. Gregor D. (2018). A survey on unmanned aerial and aquatic vehicle multi-hop networks: Wireless communications, evaluation tools and applications.Computer Communications, 119, 43–65. 10.1016/j.comcom.2018.02.002

Follow Reference Shah I. A. Jhanjhi N. Z. Amsaad F. Razaque A. (2022). The Role of Cutting-Edge Technologies in Industry 4.0. In Cyber Security Applications for Industry 4.0 (pp. 97–109). Chapman and Hall/CRC. 10.1201/9781003203087-4

Follow Reference Shah I. A. Jhanjhi N. Z. Laraib A. (2023). Cybersecurity and Blockchain Usage in Contemporary Business. In Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications (pp. 49–64). IGI Global.

Shah, I. A., Sial, Q., Jhanjhi, N. Z., & Gaur, L. (2023). Use Cases for Digital Twin. In *Digital Twins and Healthcare: Trends, Techniques, and Challenges* (pp. 102-118). IGI Global.

Shah, I. A., Sial, Q., Jhanjhi, N. Z., & Gaur, L. (2023). The Role of the IoT and Digital Twin in the Healthcare Digitalization Process: IoT and Digital Twin in the Healthcare Digitalization Process. In *Digital Twins and Healthcare: Trends, Techniques, and Challenges* (pp. 20-34). IGI Global.

Shah, I. A., Wassan, S., & Usmani, M. H. (2022). E-Government Security and Privacy Issues: Challenges and Preventive Approaches. In *Cybersecurity Measures for E-Government Frameworks* (pp. 61-76). IGI Global.

Follow Reference Sharma V. (2018). An Energy-Efficient Transaction Model for the Blockchain-enabled Internet of Vehicles (IoV).IEEE Communications Letters.

Follow Reference Sharma V. Kumar R. (2017). Cooperative frameworks and network models for flying ad hoc networks: A survey.Concurrency and Computation, 29(4), e3931. 10.1002/cpe.3931

Follow Reference Shi W. Li J. Xu W. Zhou H. Zhang N. Zhang S. Shen X. (2018). Multiple Drone-Cell Deployment Analyses and Optimization in Drone Assisted Radio Access Networks.IEEE Access : Practical Innovations, Open Solutions, 6, 12518–12529. 10.1109/ACCESS.2018.2803788

statista.com . (n.d.). https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Follow Reference Tomasino A. P. Fedorowicz J. Williams C. B. (2017). Public Sector Shared Services Move Out of the" Back-Office" The Role of Public Policy and Mission Criticality.The Data Base for Advances in Information Systems, 48(3), 83–109. 10.1145/3130515.3130521

Follow Reference Ujjan R. M. A. Hussain K. Brohi S. N. (2022). The impact of Blockchain technology on advanced security measures for E-Government. In Cybersecurity Measures for E-Government Frameworks (pp. 157–174). IGI Global. 10.4018/978-1-7998-9624-1.ch010

Follow Reference Ujjan R. M. A. Khan N. A. Gaur L. (2022). E-Government Privacy and Security Challenges in the Context of Internet of Things. In Cybersecurity Measures for E-Government Frameworks (pp. 22–42). IGI Global. 10.4018/978-1-7998-9624-1.ch002

Follow Reference Ujjan, R. M. A., Pervez, Z., & Dahal, K. (2018, June). Suspicious traffic detection in SDN with collaborative techniques of snort and deep neural networks. In *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* (pp. 915-920). IEEE. 10.1109/HPCC/SmartCity/DSS.2018.00152

Follow Reference Ujjan R. M. A. Pervez Z. Dahal K. Bashir A. K. Mumtaz R. González J. (2020). Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN.Future Generation Computer Systems, 111, 763–779. 10.1016/j.future.2019.10.015

Follow Reference Ujjan R. M. A. Taj I. Brohi S. N. (2022). E-Government Cybersecurity Modeling in the Context of Software-Defined Networks. In Cybersecurity Measures for E-Government Frameworks (pp. 1–21). IGI Global. 10.4018/978-1-7998-9624-1.ch001

Follow Reference Umrani S. Rajper S. Talpur S. H. Shah I. A. Shujrah A. (2020). Games based learning: A case of learning Physics using Angry Birds.Indian Journal of Science and Technology, 13(36), 3778–3784. 10.17485/IJST/v13i36.853

Follow Reference Vattapparamban E. Güvenç İ. Yurekli A. İ. Akkaya K. Uluağaç S. (2016). Drones for smart cities: Issues in cybersecurity, privacy, and public safety.Proceedings of the 2016 International Wireless Communications and Mobile computing Conference (IWCMC),216–221. 10.1109/IWCMC.2016.7577060

Wang, Q., Lee, B., Murray, N., & Qiao, Y. (2018). MR-IoT: An information centric MapReduce framework for IoT. *Proceedings of the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC),* 1–6.

Follow Reference Wang S. (2020). Secure Crowdsensing in 5G Internet of Vehicles: When Deep Reinforcement Learning Meets Blockchain. IEEE Consumer Electronics Magazine. Advance online publication. 10.1109/MCE.2020.3048238

Follow Reference

Yanmaz E. Yahyanejad S. Rinner B. Hellwagner H. Bettstetter C. (2018). Drone networks: Communications, coordination, and sensing.Ad Hoc Networks, 68, 1–15. 10.1016/j.adhoc.2017.09.001