Securing the Internet of Things in Logistics: Challenges, Solutions, and the Role of Machine Learning in Anomaly Detection

Syed Nizam Ud Din (/affiliate/syed-nizamud-din/469884/), Syeda Mariam Muzammal, Ruqia Bibi (/affiliate/ruqia-bibi/469886/), Muhammad Tayyab, Noor Zaman Jhanjhi, Muhammad Habib (/affiliate/muhammad-habib/469888/)

Source Title: Digital Transformation for Improved Industry and Supply Chain Performance (/gateway/book/339902)
 | Pages: 33

ISBN13: 9798369353752 | ISBN13 Softcover: 9798369353769 | EISBN13: 9798369353776

DOI: 10.4018/979-8-3693-5375-2.ch007

Abstract

Internet of things (IoT), a network of interconnected devices capable of collecting, storing, analyzing, and transmitting data, has garnered significant attention. Its widespread adoption has transformed various industries, including healthcare, transportation, manufacturing, and agriculture, owing to its numerous benefits and innovative potential. However, the rapid expansion of IoT has raised concerns about its security, presenting unique challenges compared to traditional information technology (IT) platforms. Securing the IoT environment is particularly challenging due to inherent constraints in IoT devices, such as limited resources, as well as the diverse range of devices with varying capabilities and communication protocols. The decentralized nature of the IoT network adds complexity to ensuring its security. Consequently, employing conventional host-based security techniques like anti-virus and anti-malware software in IoT is deemed impractical and inefficient.

Full Text Preview

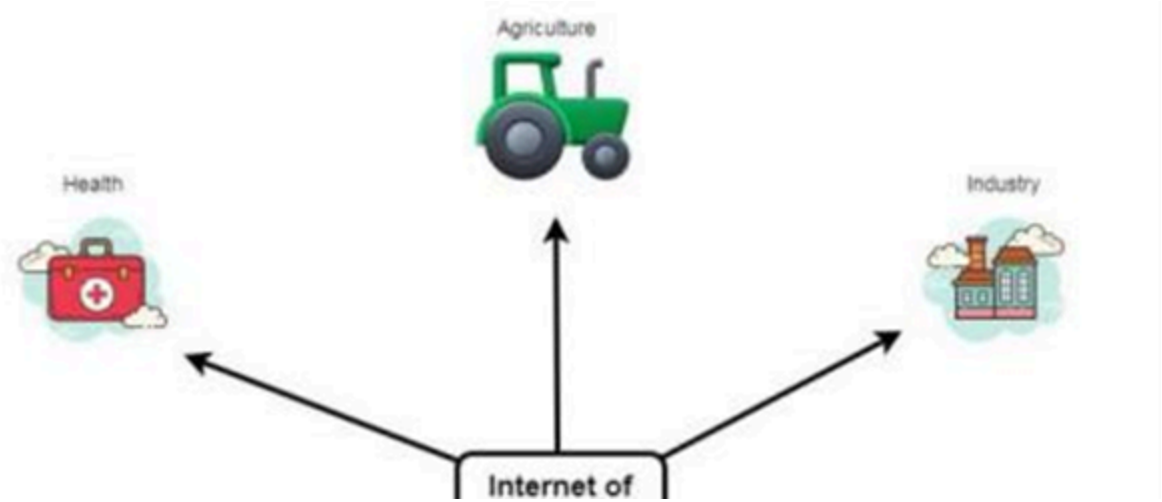
Introduction

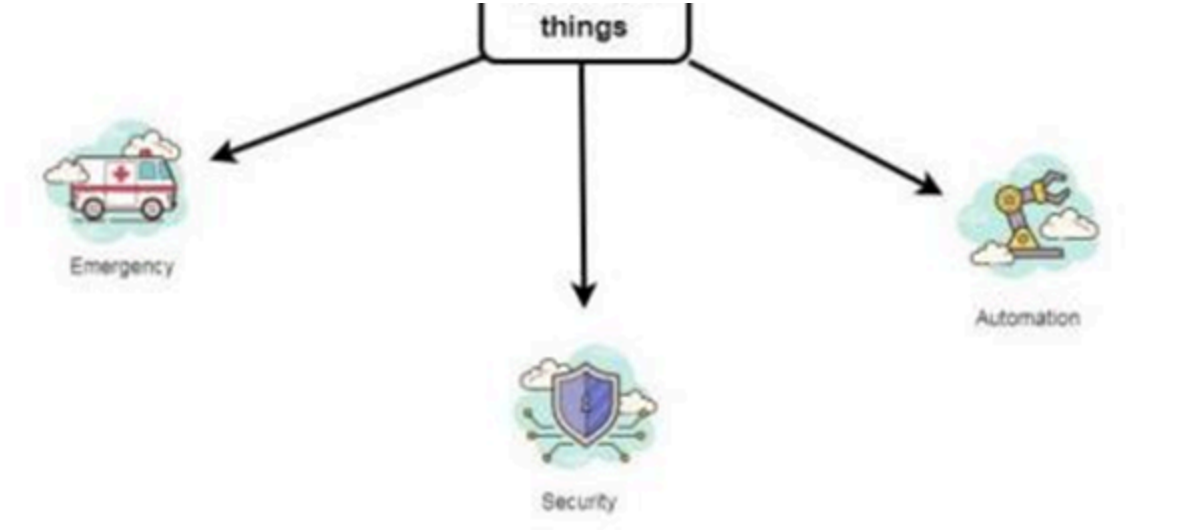
The advent of a new era marked by the rapid proliferation of Internet of Things (IoT) devices has brought about a transformative impact on infrastructure, industry, and daily life. The digital landscape is now intricately connected with diverse sensors, devices, and gadgets, offering virtually unlimited developmental opportunities (Muzammal & Ali Shah, 2016). However, the formidable challenge accompanying this unprecedented connectivity lies in securing the extensive and varied IoT landscape (Diro et al., 2021). Securing IoT networks from emerging threats has become imperious, with anomaly detection and machine learning techniques emerging as crucial strategies to address this pressing issue (Mahadevappa et al., 2021; Muzammal et al., 2022). Particularly, attacks such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) emphasize the need for reliable methods to identify anomalous behavior, even when devices appear to be functioning normally (Abdullahi et al., 2022).

The Rise of Internet of Things

IoT has witnessed a significant boost, connecting a diverse range of smart devices with capabilities for data collection, processing, and transmission. This transformative technology has brought about fundamental improvements and facilities in healthcare, transportation, and agriculture. Furthermore, it opens up unique prospects for enhancing creativity and improving efficiency (Ryalat et al., 2023). Organizations can now leverage substantial information and make data-driven decisions due to the exponential growth in the volume of data generated by the increasing number of IoT devices. The potential advantages are enormous, given that IoT devices are omnipresent in various aspects of our lives – from smart homes and wearable technology to industrial sensors and autonomous vehicles (Mansour et al., 2023). These devices have the capability to enhance productivity, optimize resource utilization, facilitate the development of new services and business models, and improve decision-making. The transformative impact of IoT extends across multiple industries, contributing to an enhanced quality of life and fostering economic growth. Figure 1 depicts some of the potential areas for IoT applications.

Figure 1. Some potential IoT application areas





(https://igiprodst.blob.core.windows.net:443/source-content/9798369353752_339902/979-8-3693-5375-2.ch007.f01.png?sv=2015-12-11&sr=c&sig=byC6%2FpQyEcCKwV8yEpjDe6O0Gn0FdrvrmWLVnFXHTto%3D&se=2024-05-13T11%3A43%3A17Z&sp=r)

Challenges in Securing IoT

Despite its advantages, the increasing adoption of IoT has raised concerns regarding its security. The interconnectivity of IoT networks exposes vulnerabilities that attackers may exploit, potentially leading to data breaches, privacy violations, and disruptions of critical services. Securing data and systems to maintain the cybersecurity standards of confidentiality, integrity, and availability (CIA triad) becomes challenging due to the vast number and diverse range of linked devices (Corno & Mannella, 2023). Furthermore, because IoT prioritizes functionality over security, vulnerabilities are often left unaddressed, providing opportunities for attackers. The security vulnerabilities in IoT can have significant consequences.

Compromised IoT devices can be utilized to execute large-scale distributed denial-of-service (DDoS) attacks or serve as access points for attacks on other systems. Unauthorized access or the disclosure of personal information can result in privacy violations (Abdullahi et al., 2022). Additionally, compromised IoT devices pose a risk of manipulating essential systems. Given these security concerns, which have raised alarms among users, organizations, and policymakers, the IoT ecosystem now requires robust security measures. Figure 2 illustrates some of the security challenges in IoT landscape. Moreover, the dynamic and evolving nature of IoT networks poses challenges for threat identification and mitigation. The substantial amount of data generated by IoT devices makes it difficult to detect anomalies or malicious activity in real-time. Detecting coordinated attacks or deviations from normal behavior becomes exceptionally challenging due to the wide range of IoT devices and communication protocols.

Continue Reading (/gateway/chapter/full-text-html/346170)

References

Abbas, A. W., Marwat, S. N. K., Ahmed, S., Hafeez, A., Ullah, K., & Khan, I. U. (2020). Proposing model for security of IoT devices in smart logistics: A review. *2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, (pp. 1–4). IEEE. https://ieeexplore.ieee.org/abstract/document/9073916/ (https://ieeexplore.ieee.org/abstract/document/9073916/)

Follow Reference — Abdullahi M. Baashar Y. Alhussian H. Alwadain A. Aziz N. Capretz L. F. Abdulkadir S. J. (2022). Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review.Electronics (Basel), 11(2), 2. 10.3390/electronics11020198

Follow Reference — Ahmad Antouz Y. Akour I. A. Turki Alshurideh M. Alzoubi H. M. Alquqa E. K. (2023). The impact of Internet of Things (IoT) and Logistics Activities on Digital Operations.2023 International Conference on Business Analytics for Technology and Security (ICBATS), (pp. 1–5). IEEE. 10.1109/ICBATS57792.2023.10111287

Follow Reference — Al-amri R. Murugesan R. K. Man M. Abdulateef A. F. Al-Sharafi M. A. Alkahtani A. A. (2021). A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data.Applied Sciences (Basel, Switzerland), 11(12), 12. 10.3390/app11125320

Follow Reference — Alanazi R. Aljuhani A. (2022). Anomaly Detection for Industrial Internet of Things Cyberattacks.Computer Systems Science and Engineering, 44(3), 2361–2378. 10.32604/csse.2023.026712

Follow Reference — Alex S. A. Ponkamali S. Andrew T. R. Jhanjhi N. Z. Tayyab M. (2022). Machine Learning-Based Wearable Devices for Smart Healthcare Application With Risk Factor Monitoring. In Empowering Sustainable Industrial 4.0 Systems With Machine Intelligence (pp. 174–185). IGI Global. https://www.igi-global.com/chapter/machine-learning-based-wearable-devices-for-smart-healthcare-application-with-risk-factor-monitoring/301509 (https://www.igi-global.com/chapter/machine-learning-based-wearable-devices-for-smart-healthcare-application-with-risk-factor-monitoring/301509)10.4018/978-1-7998-9201-4.ch009

Follow Reference — Alsudani M. Q. Jaber M. M. Ali M. H. Abd S. K. Alkhayyat A. Kareem Z. H. Mohhan A. R. (2023). RETRACTED ARTICLE: Smart logistics with IoT-based enterprise management system using global manufacturing.Journal of Combinatorial Optimization, 45(2), 57. 10.1007/s10878-022-00977-5

Follow Reference Arts J. Basten R. Van Houtum G.-J. (2019). Maintenance Service Logistics. In ZijmH.KlumppM.RegattieriA.HeraguS. (Eds.), Operations, Logistics and Supply Chain Management (pp. 493–517). Springer International Publishing. 10.1007/978-3-319-92447-2_22

Follow Reference Astillo P. V. Duguma D. G. Park H. Kim J. Kim B. You I. (2022). Federated intelligence of anomaly detection agent in IoTMD-enabled Diabetes Management Control System.Future Generation Computer Systems, 128, 395–405. 10.1016/j.future.2021.10.023

Follow Reference Ayvaz S. Alpay K. (2021). Predictive maintenance system for production lines in manufacturing: A machine learning approach using IoT data in real-time.Expert Systems with Applications, 173, 114598. 10.1016/j.eswa.2021.114598

Follow Reference Azeem, M. R., Muzammal, S. M., Zaman, N., & Khan, M. A. (2022). Edge Caching for Mobile Devices. *2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, (pp. 1–6). IEEE. 10.1109/MACS56771.2022.10022729

Follow Reference Bandyopadhyay D. Sen J. (2011). Internet of Things: Applications and Challenges in Technology and Standardization.Wireless Personal Communications, 58(1), 49–69. 10.1007/s11277-011-0288-5

Follow Reference Chen J. Xu S. Liu K. Yao S. Luo X. Wu H. (2022). Intelligent Transportation Logistics Optimal Warehouse Location Method Based on Internet of Things and Blockchain Technology.Sensors (Basel), 22(4), 4. 10.3390/s2204154435214444

Follow Reference Corno F. Mannella L. (2023). Security Evaluation of Arduino Projects Developed by Hobbyist IoT Programmers.Sensors (Basel), 23(5), 5. 10.3390/s2305274036904941

Follow Reference Ding Y. Jin M. Li S. Feng D. (2021). Smart logistics based on the internet of things technology: An overview.International Journal of Logistics, 24(4), 323–345. 10.1080/13675567.2020.1757053

Follow Reference Diro A. Chilamkurti N. Nguyen V.-D. Heyne W. (2021). A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms.Sensors (Basel), 21(24), 24. 10.3390/s2124832034960414

Follow Reference Douiba M. Benkirane S. Guezzaz A. Azrour M. (2023). An improved anomaly detection model for IoT security using decision tree and gradient boosting.The Journal of Supercomputing, 79(3), 3392–3411. 10.1007/s11227-022-04783-y

Follow Reference Flores-García E. Jeong Y. Liu S. Wiktorsson M. Wang L. (2023). Enabling industrial internet of things-based digital servitization in smart production logistics.International Journal of Production Research, 61(12), 3884–3909. 10.1080/00207543.2022.2081099

Follow Reference Gadal S. Mokhtar R. Abdelhaq M. Alsaqour R. Ali E. S. Saeed R. (2022). Machine Learning-Based Anomaly Detection Using K-Mean Array and Sequential Minimal Optimization.Electronics (Basel), 11(14), 14. 10.3390/electronics11142158

Follow Reference Golpîra H. Khan S. A. R. Safaeipour S. (2021). A review of logistics Internet-of-Things: Current trends and scope for future research.Journal of Industrial Information Integration, 22, 100194. 10.1016/j.jii.2020.100194

Follow Reference Gupta K. Sharma D. K. Datta Gupta K. Kumar A. (2022a). A tree classifier based network intrusion detection model for Internet of Medical Things.Computers & Electrical Engineering, 102, 108158. 10.1016/j.compeleceng.2022.108158

Follow Reference Gupta K. Sharma D. K. Datta Gupta K. Kumar A. (2022b). A tree classifier based network intrusion detection model for Internet of Medical Things.Computers & Electrical Engineering, 102, 108158. 10.1016/j.compeleceng.2022.108158

Follow Reference Habib M. Hussain A. Rehman E. Muzammal S. M. Cheng B. Aslam M. Jilani S. F. (2023). Convolved Feature Vector Based Adaptive Fuzzy Filter for Image De-Noising.Applied Sciences (Basel, Switzerland), 13(8), 8. 10.3390/app13084861

Hameed, K., Haseeb, J., Tayyab, M., Junaid, M., Maqsood, T. B., & Naqvi, M. H. (2017). Secure provenance in wireless sensor networks-a survey of provenance schemes. *2017 International Conference on Communication, Computing and Digital Systems (C-CODE)*, (pp. 11–16). IEEE. https://ieeexplore.ieee.org/abstract/document/7918893/ (https://ieeexplore.ieee.org/abstract/document/7918893/)

Follow Reference Hameed M. Yang F. Ghafoor M. I. Jaskani F. H. Islam U. Fayaz M. Mehmood G. (2022). IOTA-Based Mobile Crowd Sensing: Detection of Fake Sensing Using Logit-Boosted Machine Learning Algorithms.Wireless Communications and Mobile Computing, 2022, e6274114. 10.1155/2022/6274114

Follow Reference Hussain F. Hassan S. A. Hussain R. Hossain E. (2020). Machine Learning for Resource Management in Cellular and IoT Networks: Potentials, Current Solutions, and Open Challenges.IEEE Communications Surveys and Tutorials, 22(2), 1251–1275. 10.1109/COMST.2020.2964534

Follow Reference Imtiaz S. I. Khan L. A. Almadhor A. S. Abbas S. Alsubai S. Gregus M. Jalil Z. Lakshmanna K. (2022). Efficient Approach for Anomaly Detection in Internet of Things Traffic Using Deep Learning.Wireless Communications and Mobile Computing, 2022, 1–15. 10.1155/2022/8266347

Follow Reference Khan A. R. Kashif M. Jhaveri R. H. Raut R. Saba T. Bahaj S. A. (2022). Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions.Security and Communication Networks, 2022, e4016073. 10.1155/2022/4016073

Follow Reference Khilar R. Mariyappan K. Christo M. S. Amutharaj J. Anitha T. Rajendran T. Batu A. (2022). Artificial Intelligence-Based Security Protocols to Resist Attacks in Internet of Things.Wireless Communications and Mobile Computing, 2022, e1440538. 10.1155/2022/1440538

Follow Reference Kumar D. Kr Singh R. Mishra R. Fosso Wamba S. (2022). Applications of the internet of things for optimizing warehousing and logistics operations: A systematic literature review and future research directions.Computers & Industrial Engineering, 171, 108455. 10.1016/j.cie.2022.108455

Follow Reference Lagorio A. Cimini C. Pinto R. Cavalieri S. (2023). 5G in Logistics 4.0: Potential applications and challenges.Procedia Computer Science, 217, 650–659. 10.1016/j.procs.2022.12.261

Follow Reference Latif S. Huma Z. Jamal S. S. Ahmed F. Ahmad J. Zahid A. Dashtipour K. Aftab M. U. Ahmad M. Abbasi Q. H. (2022). Intrusion Detection Framework for the Internet of Things Using a Dense Random Neural Network.IEEE Transactions on Industrial Informatics, 18(9), 6435–6444. 10.1109/TII.2021.3130248

Follow Reference Lei N. (2022). Intelligent logistics scheduling model and algorithm based on Internet of Things technology.Alexandria Engineering Journal, 61(1), 893–903. 10.1016/j.aej.2021.04.075

Follow Reference Liu C. Ma T. (2022). Green logistics management and supply chain system construction based on internet of things technology.Sustainable Computing : Informatics and Systems, 35, 100773. 10.1016/j.suscom.2022.100773

Follow Reference Mahadevappa, P., Muzammal, S. M., & Murugesan, R. K. (2021). *A Comparative Analysis of Machine Learning Algorithms for Intrusion Detection in Edge-Enabled IoT Networks* (arXiv:2111.01383). arXiv. https://doi.org//arXiv.2111.0138310.48550

Follow Reference Mahmud B. (2017). Internet of things (IoT) for manufacturing logistics on SAP ERP applications. [JTEC]. Journal of Telecommunication, Electronic and Computer Engineering, 9(2–6), 43–47.

Follow Reference Mansour M. Gamal A. Ahmed A. I. Said L. A. Elbaz A. Herencsar N. Soltan A. (2023). Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions.Energies, 16(8), 8. 10.3390/en16083465

Follow Reference Marchi B. Zanoni S. (2023). Technical note on “Inventory management in supply chains with consideration of Logistics, green investment and different carbon emissions policies.”. Computers & Industrial Engineering, 175, 108870. 10.1016/j.cie.2022.108870

Follow Reference Mashayekhy Y. Babaei A. Yuan X.-M. Xue A. (2022). Impact of Internet of Things (IoT) on Inventory Management: A Literature Survey.Logistics, 6(2), 2. 10.3390/logistics6020033

Follow Reference Mukherjee I. Sahu N. K. Sahana S. K. (2023). Simulation and Modeling for Anomaly Detection in IoT Network Using Machine Learning.International Journal of Wireless Information Networks, 30(2), 173–189. 10.1007/s10776-021-00542-7

Follow Reference Muzammal, S. M., & Ali Shah, M. (2016). ScreenStealer: Addressing Screenshot attacks on Android devices. *2016 22nd International Conference on Automation and Computing (ICAC)*, (pp. 336–341). IEEE. 10.1109/IConAC.2016.7604942

Follow Reference Muzammal S. M. Murugesan R. K. (2020). A Study on Secured Authentication and Authorization in Internet of Things: Potential of Blockchain Technology. In AnbarM.AbdullahN.ManickamS. (Eds.), Advances in Cyber Security (pp. 18–32). Springer. 10.1007/978-981-15-2693-0_2

Follow Reference Muzammal S. M. Murugesan R. K. (2021). Enhanced authentication and access control in Internet of Things: A potential blockchain-based method.International Journal of Grid and Utility Computing, 12(5–6), 469–485. 10.1504/IJGUC.2021.120090

Follow Reference Muzammal S. M. Murugesan R. K. Jhanjhi N. (2021). Introducing Mobility Metrics in Trust-based Security of Routing Protocol for Internet of Things.2021 National Computing Colleges Conference (NCCC), (pp. 1–5). IEEE. 10.1109/NCCC49330.2021.9428799

Follow Reference Muzammal S. M. Murugesan R. K. Jhanjhi N. Z. Humayun M. Ibrahim A. O. Abdelmaboud A. (2022). A Trust-Based Model for Secure Routing against RPL Attacks in Internet of Things.Sensors (Basel), 22(18), 18. 10.3390/s2218705236146400

Follow Reference Muzammal, S. M., Shah, M. A., Zhang, S., & Yang, H. (2016). *Conceivable security risks and authentication techniques for smart devices*. 10.1007/s11633-016-1011-5

Follow Reference Raza Z. Woxenius J. Vural C. A. Lind M. (2023). Digital transformation of maritime logistics: Exploring trends in the liner shipping segment.Computers in Industry, 145, 103811. 10.1016/j.compind.2022.103811

Follow Reference Rock L. Y. Tajudeen F. P. Chung Y. W. (2022). Usage and impact of the internet-of-things-based smart home technology: A quality-of-life perspective.Universal Access in the Information Society. Advance online publication. 10.1007/s10209-022-00937-036407566

Rosero-Montalvo, P. D., István, Z., Tözün, P., & Hernandez, W. (2023). Hybrid anomaly detection model on trusted iot devices. *IEEE Internet of Things Journal*. IEEE. https://ieeexplore.ieee.org/abstract/document/10039052/

Follow Reference Ryalat M. ElMoaqet H. AlFaouri M. (2023). Design of a Smart Factory Based on Cyber-Physical Systems and Internet of Things towards Industry 4.0.Applied Sciences (Basel, Switzerland), 13(4), 4. 10.3390/app13042156

Follow Reference Saba T. Rehman A. Sadad T. Kolivand H. Bahaj S. A. (2022). Anomaly-based intrusion detection system for IoT networks through deep learning model.Computers & Electrical Engineering, 99, 107810. 10.1016/j.compeleceng.2022.107810

Follow Reference Sarwar A. Alnajim A. M. Marwat S. N. K. Ahmed S. Alyahya S. Khan W. U. (2022). Enhanced Anomaly Detection System for IoT Based on Improved Dynamic SBPSO.Sensors (Basel), 22(13), 13. 10.3390/s2213492635808425

Follow Reference Solomon F. A. M. Sathianesan G. W. Ramesh R. (2023). Logistic Regression Trust-A Trust Model for Internet-of-Things Using Regression Analysis.Computer Systems Science and Engineering, 44(2). https://cdn.techscience.cn/ueditor/files/csse/TSP_CSSE-44-2/TSP_CSSE_24292/TSP_CSSE_24292.pdf (https://cdn.techscience.cn/ueditor/files/csse/TSP_CSSE-44-2/TSP_CSSE_24292/TSP_CSSE_24292.pdf)

Follow Reference Song Y. Yu F. R. Zhou L. Yang X. He Z. (2021). Applications of the Internet of Things (IoT) in Smart Logistics: A Comprehensive Survey.IEEE Internet of Things Journal, 8(6), 4250–4274. 10.1109/JIOT.2020.3034385

Follow Reference Tang X. (2020). Research on Smart Logistics Model Based on Internet of Things Technology.IEEE Access : Practical Innovations, Open Solutions, 8, 151150–151159. 10.1109/ACCESS.2020.3016330

Follow Reference Tayyab M. Marjani M. Jhanjhi N. Hashim I. A. T. Almazroi A. A. Almazroi A. A. (2021). Cryptographic based secure model on dataset for deep learning algorithms.CMC Comput. Mater. Contin, 69, 1183–1200. 10.32604/cmc.2021.017199

Tayyab, M., Marjani, M., Jhanjhi, N. Z., & Hashem, I. A. T. (2021). A Light-weight Watermarking-Based Framework on Dataset Using Deep Learning Algorithms. *2021 National Computing Colleges Conference (NCCC)*, (pp. 1–6). IEEE. https://ieeexplore.ieee.org/abstract/document/9428845/ (https://ieeexplore.ieee.org/abstract/document/9428845/)

Follow Reference Tran-Dang H. Krommenacker N. Charpentier P. Kim D.-S. (2022). The Internet of Things for Logistics: Perspectives, Application Review, and Challenges.IETE Technical Review, 39(1), 93–121. 10.1080/02564602.2020.1827308

Follow Reference Tyagi A. K. Dananjayan S. Agarwal D. Thariq Ahmed H. F. (2023). Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0.Sensors (Basel), 23(2), 2. 10.3390/s2302094736679743

Follow Reference Vitorino J. Andrade R. Praça I. Sousa O. Maia E. (2022). A Comparative Analysis of Machine Learning Techniques for IoT Intrusion Detection. In AïmeurE.LaurentM.YaichR.DupontB.Garcia-AlfaroJ. (Eds.), Foundations and Practice of Security (pp. 191–207). Springer International Publishing. 10.1007/978-3-031-08147-7_13

Follow Reference Vivaldini M. Pires S. R. de Souza F. B. (2012). Improving logistics services through the technology used in fleet management.Journal of Information Systems and Technology Management, 9(3), 541–562. 10.4301/S1807-17752012000300006

Follow Reference Wang S. Jia H. Lu J. Yang D. (2023). Crude oil transportation route choices: A connectivity reliability-based approach.Reliability Engineering & System Safety, 235, 109254. 10.1016/j.ress.2023.109254

Follow Reference Yazdinejad A. Kazemi M. Parizi R. M. Dehghantanha A. Karimipour H. (2023). An ensemble deep learning model for cyber threat hunting in industrial internet of things.Digital Communications and Networks, 9(1), 101–110. 10.1016/j.dcan.2022.09.008