Internet of Things in the Industry Revolution 4.0

Subjects: Computer Science, Information Systems

Contributor: Abdul Javed

Researchers offers a wide range of information on Industry 4.0, finds research gaps and recommends future directions. Seven research questions are addressed: (i) What are the contributions of WSN in IR 4.0? (ii) What are the contributions of IoT in IR 4.0? (iii) What are the types of WSN coverage areas for IR 4.0? (iv) What are the major types of network intruders in WSN and IoT systems? (v) What are the prominent network security attacks in WSN and IoT? (vi) What are the significant issues in IoT and WSN frameworks? and (vii) What are the limitations and research gaps in the existing work? Researchers mainly focuses on the solutions and new techniques to automate Industry 4.0 and analyzed over 130 articles from 2014 until 2021. The entry covers several aspects of Industry 4.0, from the designing phase to security needs, from the deployment stage to the classification of the network, the difficulties, challenges, and future directions.

Internet of Things (IoT)   industrial revolution 4.0 (IR 4.0)

1. Introduction

In physical production systems, grid and energy-saving applications minimize the energy resources and noise pollution. In the last few decades, transportation has improved a lot with the usage of smart IoT devices, such as signals and high-resolution cameras on roads, which has led to an increase in traffic flow. RFID readers are deployed at toll booths that automatically deduct toll amounts after reading RFID tags on vehicles. In the transportation sector, smart vehicles reduce the travelling time and also fuel consumption with low cost of mobility and reduced human efforts [1], atmospheric monitoring reduces pollution, and surveillance applications reduce crime. Nowadays, WSN also plays a role in precision agriculture. On the other hand, WSN applications facilitate our day to day lives, making them more comfortable, such as healthcare applications that improve our health and longevity.

Besides WSN, IoT has also played an important role in human life. IoT and the digital age play essential roles in overcoming social and physical barriers and providing ease and mobility to people, resulting in improved and equal opportunities, and access to information [2][3]. IoT also has many application areas such as agribusiness, climate, clinical care, education, transportation, and finance.

In regard to information and communication technology, researchers are attracted to IoT [4]. By adopting this essential technology, companies have become smarter, more competitive, automated, and sustainable in the global supply chain. In today’s competitive marketplace, supply chains are struggling as they compete with each other. Therefore, IoT devices are an effective way to authenticate, monitor, and track products using GPS and many technologies [5][6]. Industry 4.0 stands for the fourth industrial revolution in the digital age, it is associated with virtualizing real-world scenarios of production and processing without human intervention. This virtual world is linked to IoT devices, allowing the creation of cyber–physical systems to communicate and cooperate [7][8]. This fully connected manufacturing system—operating without human intervention by generating, transferring, receiving, and processing necessary data to conduct all required tasks for producing all kinds of goods—is one of Industry 4.0’s key “constructs”. The concept of Industry 4.0 is based on the combination of three main elements: people, things, and business [9]. A complete cyber–physical production system created by the integration of IoT devices, things and objects (IoT), sensor nodes (WSN), and people, is shown in **Figure 1**. CPS is a typical example of Industry 4.0. IoT is the connection of smart devices, objects, or machines to the internet and with each other. In WSN systems, there is no direct connection of these devices to the Internet. These systems can send their data to the Internet by connecting several sensor nodes to a central routing node. While CPS systems involve the integration of IoT devices, computation, networking, and physical process, IoT is an essential component of CPS. CPS systems are key elements in the implementation of IR 4.0 [10]. Industry 4.0 is the network-enabled entity that automates the whole process of manufacturing, connecting business and processes. Market demands and the advancements in new technologies are transforming manufacturing firms’ business operations into smart factories and warehouses. Due to this automation, IoT devices are producing a massive amount of data daily, known as big data [11][12]. Statistics show that, at the end of 2021, there were more than 10 billion active IoT devices globally [13]. By 2030, the number of active IoT devices is expected to exceed 10 billion to 25.4 billion. By 2025, the data created by IoT devices will reach 73.1 ZB (zeta bytes) [14]. In 2020, the IoT industry was predicted to generate more than USD 450 billion, including hardware, software, systems integration, and data services. By the end of 2021, it reached USD 520 billion. The global amount expected to be spent on the IoT in 2022 is USD 1 trillion. The IoT industry is predicted to grow to more than USD 2 trillion by 2027 [15][16]. The increasing number of devices and the usage by humans shows the importance of IoT devices; moreover, the industry is growing and gaining revenue.

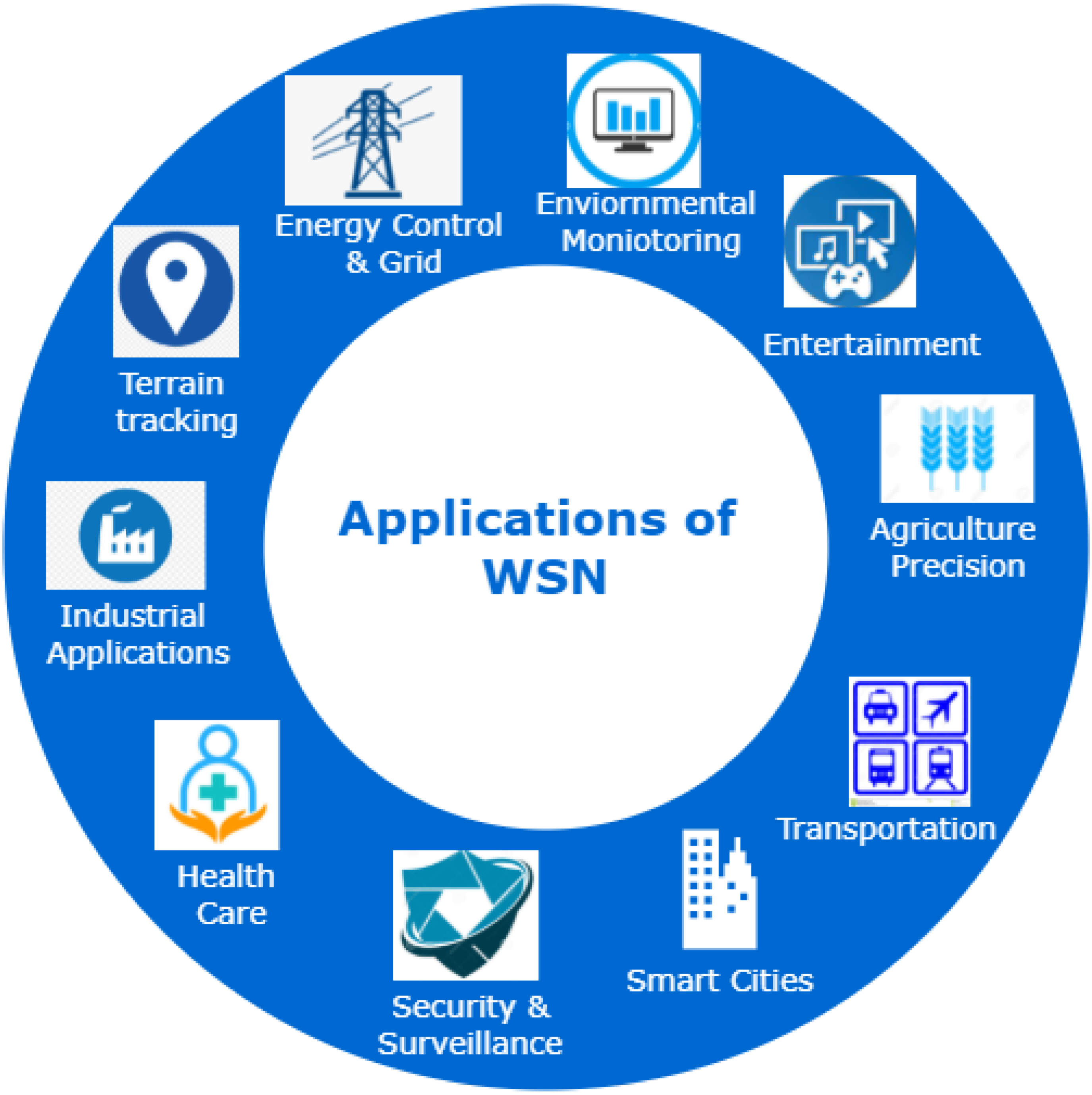

Figure 1. CPS system–integration of IoT, wireless devices, and people in Industry 4.0.

2. Contributions of IoT in IR 4.0

An integrated digital system would introduce a new intelligent and economical manufacturing process using cutting-edge technology for a variety of existing items and processes [17]. The data collected from production process warehouses and consumer information can be critically analyzed to make a decision in real time under Industry 4.0. The real-time decision-making capability of each small and medium organization enables them to efficiently accept new technologies [18][19]. Industrial IoT delivers solutions and services that provide insights into an organization's ability to monitor and control its operations and assets. IIoT software and tools provide important solutions for better process, layout scheduling, organization, and administration.

In addition, IIoT enables real-time and decision-making features among numerous networked devices that can communicate and interact with each other [20]. Because of the rapid communication and data transfer, attackers can attack data and cause harm to an organization, resulting in cyber attacks. Cyber attacks have become a major challenge for the industrial Internet of Things (IIoT). Therefore, integrating IoT with Industry 4.0 plays a critical role in securing IoT devices from attacks. Unique security objectives and challenges of IIoT have been introduced to overcome industrial-level issues. IIoT challenges and objectives relate to IoT being used by consumers and its capabilities leading to longer life of IoT devices and sensor nodes. In [21], the authors analyzed security challenges and attacks at three levels of the network (perception, network, and application). They considered cryptographic challenges, authentication, network monitoring, and access control mechanisms. The IIoT also addresses local network connectivity and protection from attackers inside. Cyber attacks have become a serious challenge for the IIoT. Hackers attack infrastructure/devices through intrusion and hiding, resulting in poor performance. A bidirectional long and short term memory network with a multi-feature layer has been developed to avoid temporal attacks. Machine learning-based networks that learn temporal attacks from historical data and make associations with test data can effectively identify and detect different attacks within different intervals [22].

DL-IIoT has enormous potential to improve data processing and contribute to IR 4.0. Similarly, machine learning algorithms, such as logistic regression, are widely used for malware detection and security threat protection [23]. Deep learning algorithms are also used for intelligent analysis and processing. Deep learning [24] algorithms such as CNN, auto-encoders, and recurrent neural networks have applications such as intelligent assembly and manufacturing, network monitoring, and accident prevention. The application of deep learning algorithms in IIoT has also enabled various smart applications such as manufacturing, active attack detection and prevention systems, smart meters, and smart agriculture [25]. DL-IIoT relies heavily on data collection, which affects the privacy of the organization's data. Therefore, differentiated privacy is used to protect user privacy, reduce privacy risk, and achieve high performance in IIoT.

On the other hand, IoT and IIoT must provide "differentiated privacy" for individuals and industrial data [26][27][28]. The contribution of IoT in Industry 4.0 has improved the average availability and sustainability of the enterprise by knowing market trends and decreasing unanticipated downturns [29]. The taxonomy of existing studies and the contribution of IoT in IR 4.0 is shown in **Figure 2**.

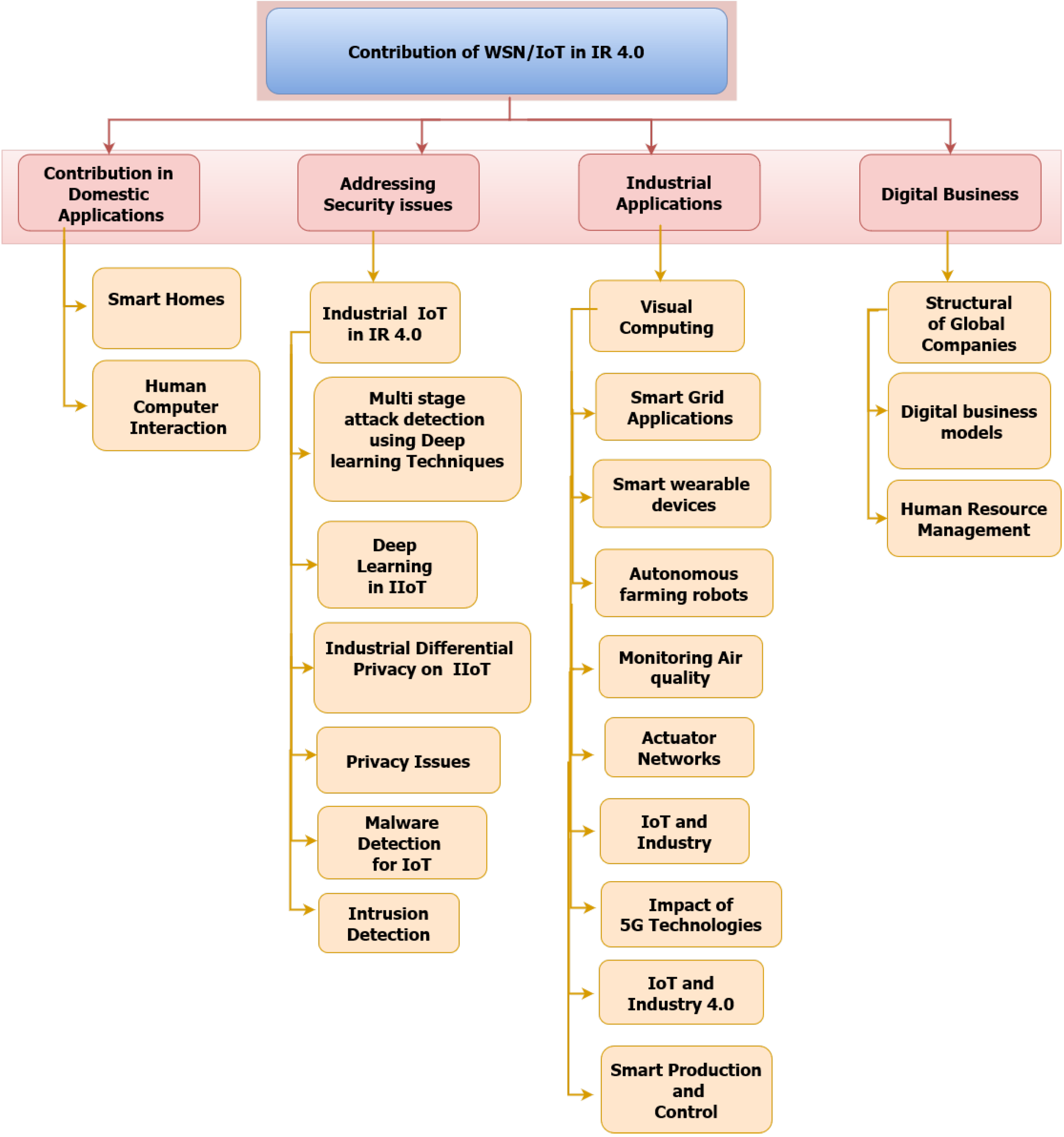
Contribution of WSN/IoT in IR 4.0
Contribution in Domestic Applications
Addressing Security issues
Industrial Applications
Digital Business
Smart Homes
Human Computer Interaction
Industrial IoT in IR 4.0
Multi stage attack detection using Deep learning Techniques
Deep Learning in IIoT
Industrial Differential Privacy on IIoT
Privacy Issues
Malware Detection for IoT
Intrusion Detection
Visual Computing
Smart Grid Applications
Smart wearable devices
Autonomous farming robots
Monitoring Air quality
Actuator Networks
IoT and Industry
Impact of 5G Technologies
IoT and Industry 4.0
Smart Production and Control
Structural of Global Companies
Digital business models
Human Resource Management

Figure 2. Taxonomy of existing studies.

References

1. Ravi, C.; Tigga, A.; Reddy, G.T.; Hakak, S.; Alazab, M. Driver Identification Using Optimized Deep Learning Model in Smart Transportation. ACM Trans. Internet Technol. 2020.

2. Tandale, U.; Momin, B.; Seetharam, D.P. An empirical study of application layer protocols for IoT. In Proceedings of the International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, 1–2 August 2017; pp. 2447–2451.
3. Kumar, R.; Kumar, P.; Srivastava, G.; Gupta, G.P.; Tripathi, R.; Gadekallu, T.R.; Xiong, N.N. PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. IEEE Trans. Netw. Sci. Eng. 2021, 8, 2326–2341.
4. Farsi, M.; Daneshkhah, A.; Hosseinian-Far, A.; Jahankhani, H. (Eds.) Digital Twin Technologies and Smart Cities; Springer: Berlin/Heidelberg, Germany, 2020.
5. Majeed, M.A.A.; Rupasinghe, T.D. Internet of things (IoT) embedded future supply chains for Industry 4.0: An assessment from an ERP-based fashion apparel and footwear industry. Int. J. Supply Chain. Manag. 2017, 6, 25–40.
6. Oliff, H.; Liu, Y. Towards Industry 4.0 Utilizing Data-Mining Techniques: A Case Study on Quality Improvement. Procedia CIRP 2017, 63, 167–172.
7. Ovsthus, A.A.K.S.K.; Kristensen, L.M. An Industrial Perspective on Wireless Sensor Networks—A Survey of Requirements, Protocols, and Challenges. IEEE Commun. Surv. Tutor. 2014, 16, 1391–1412.
8. Muneeba, N.; Javed, A.R.; Tariq, M.A.; Asim, M.; Baker, T. Feature engineering and deep learning-based intrusion detection framework for securing edge IoT. J. Super Comput. 2022, 1–15.
9. Osterrieder, P.; Budde, L.; Friedli, T. The smart factory as a key construct of Industry 4.0: A systematic literature review. Int. J. Prod. Econ. 2020, 221, 107476.
10. Devesh, M.; Kant, A.K.; Suchit, Y.R.; Tanuja, P.; Kumar, S.N. Fruition of CPS and IoT in Context of Industry 4.0. In Intelligent Communication, Control and Devices; Springer: Singapore, 2020; pp. 367–375.
11. Saniuk, S.; Grabowska, S.; Gajdzik, B. Social expectations and market changes in the context of developing the Industry 4.0 concept. J. Sustain. 2020, 12, 1362.
12. Deepa, N.; Pham, Q.V.; Nguyen, D.C.; Bhattacharya, S.; Prabadevi, B.; Gadekallu, T.R.; Pathirana, P.N. A survey on blockchain for big data: Approaches, opportunities, and future directions. Future Gener. Comput. Syst. 2022, 131, 209–226.
13. Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2030. 2021. Available online: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (accessed on 21 January 2022).
14. Jovanović, B. Key IoT Statistics. 2021. Available online: Https://dataprot.net/statistics/iot-statistics/ (accessed on 20 December 2021).

15. AI Multiple. 30 Internet of Things—IoT Stats from Reputable Sources in 2021. Available online: https://research.aimultiple.com/iot-stats/ (accessed on 21 February 2022).
16. O'Dea, S. Wide-Area and Short-Range IoT Devices Installed Base Worldwide 2014–2026. 2021. Available online: Https://www.statista.com/statistics/1016276/wide-area-and-short-range-iot-device-installed-base-worldwide/ (accessed on 14 December 2021).
17. Lange, S. Digitalization, and energy consumption. Does ICT reduce energy demand? J. Ecol. Econ. 2020, 176, 106760.
18. Müller, J.M. Fortune favors the prepared: How SMEs approach business model innovations in Industry 4.0. Technol. Forecast. Soc. Change 2018, 132, 2–17.
19. Masood, T.; Sonntag, P. Industry 4.0: Adoption challenges and benefits for SMEs. J. Comput. Ind. 2020, 121, 103261.
20. Zhu, J. Measurement and analysis of corporate operating vitality in the age of digital business models. Appl. Econ. Lett. 2020, 27, 511–517.
21. Serror, M.; Hack, S.; Henze, M.; Schuba, M.; Wehrle, K. Challenges and Opportunities in Securing the Industrial Internet of Things. IEEE Trans. Ind. Inform. 2021, 17, 2985–2996.
22. Li, X.; Xu, M.; Vijayakumar, P.; Kumar, N.; Liu, X. Detection of low-frequency and multi-stage attacks in industrial internet of things. IEEE Trans. Veh. Technol. 2020, 69, 8820–8831.
23. Akram, Z.; Majid, M.; Habib, S. A Systematic Literature Review: Usage of Logistic Regression for Malware Detection. In Proceedings of the International Conference on Innovative Computing (ICIC), Seoul, Korea, 9–10 November 2021; pp. 1–8.
24. Azmoodeh, A.; Dehghantanha; Choo, K.K.R. Robust malware detection for Internet of (battlefield) Things devices using deep eigenspace learning. IEEE Trans. Sustain. Comput. 2019, 4, 88–95.
25. Khalil, R.A.; Saeed, N.; Masood, M.; Fard, Y.M.; Alouini, M.-S.; Al-Naffouri, T.Y. Deep learning in the industrial internet of things: Potentials, challenges, and emerging applications. IEEE Internet Things J. 2021, 8, 11016–11040.
26. Jiang, B.; Li, J.; Yue, G.; Song, H. Differential privacy for Industrial Internet of Things: Opportunities, applications and challenges. IEEE Internet Things J. 2021, 8, 10430–10451.
27. Ahmed, A.; Javed, A.R.; Jalil, Z.; Srivastava, G.; Gadekallu, T.R. Privacy of Web Browsers: A Challenge in Digital Forensics. In Proceedings of the International Conference on Genetic and Evolutionary Computing, Jilin, China, 21–21 October 2021; Springer: Singapore, 2021; pp. 493–504.
28. Vangala, A.; Das, A.K.; Kumar, N.; Alazab, M. Smart secure sensing for IoT-based agriculture: Blockchain perspective. IEEE Sensors J. 2021, 21, 17591–17607.

29. Maddikunta, P.K.R.; Pham, Q.V.; Prabadevi, B.; Deepa, N.; Dev, K.; Gadekallu, T.R.; Liyanage, M. Industry 5.0: A survey on enabling technologies and potential applications. J. Ind. Inf. Integr. 2021, 100257.

Retrieved from https://encyclopedia.pub/entry/history/show/49478