Mesopotamian journal of Big Data
Vol. **(2023)**, 2023, **pp**. 63–69
DOI: https://doi.org/10.58496/MJBD/2023/009 ISSN: 2958-6453
https://mesopotamian.press/journals/index.php/BigData

Review Article

Analysing the Connection Between AI and Industry 4.0 from a Cybersecurity Perspective: Defending the Smart Revolution

Indu Bala[1], Maad M. Mijwil[2, *], Guma Ali[3], Emre Sadıkoğlu[4]

[1] *School of Electrical and Electronics Engineering, Lovely Professional University, Punjab, India*

[2] *Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq*

[3] *Department of Computer Science and Electrical Engineering, Muni University, Arua, Uganda*

[4] *Department of Computer Engineering, Yalova University, Yalova, Turkey*

ARTICLE INFO

Article History
Received 12 Mar 2023
Accepted 05 May 2023

Keywords
Industry 4.0
Internet of Things
Cybersecurity
Artificial Intelligence
Machine Learning

ABSTRACT

In recent years, the significance and efficiency of business performance have become dependent heavily on digitization, as jobs in companies are seeking to be transformed into digital jobs based on smart systems and applications of the fourth industrial revolution. Cybersecurity systems must interact and continuously cooperate with authorized users through the Internet of Things and benefit from corporate services that allow users to interact in a secure environment free from electronic attacks. Artificial intelligence methods contribute to the design of the Fourth Industrial Revolution principles, including interoperability, information transparency, technical assistance, and decentralized decisions. Through this design, security gaps may be generated that attackers can exploit in order to be able to enter systems, control them, or manipulate them. In this paper, the role of automated systems for digital operations in the fourth industrial revolution era will be examined from the perspective of artificial intelligence and cybersecurity, as well as the most significant practices of artificial intelligence methods. This paper concluded that artificial intelligence methods play a significant role in defending and protecting cybersecurity and the Internet of Things, preventing electronic attacks, and protecting users' privacy.

1. Introduction

Developments in artificial intelligence methods, especially machine learning algorithms that are used to predict and analyse data behaviours, have brought about rapid developments in the information revolution [1-4]. These methods create the process of data analysis and automated intelligent operations vital in digital processes [5][6]. With the increase of data analysis solutions and predictive computational models, the digital world has witnessed the emergence of many and many applications and electronic devices that contribute to the growth of the environment for companies and individuals [7-9]. Moreover, these methods present significant economic and structural challenges to industries. Machine learning algorithms contribute to prediction and significantly improve the accuracy of procedures [10-13]. Through these algorithms, correct decisions can be made based on data whose behaviour has been studied and analysed to improve industrial processes, reduce time and effort, and improve productivity. At the same time, the emergence of automated intelligent processes has simplified various industrial jobs, automating repetitive and labour-intensive processes, thus growing efficiency and saving costs. Artificial intelligence methods seek to analyse big data and develop new possibilities for various industrial applications [14][15]. These methods enable harnessing vast amounts of data and extracting beneficial insights. Through sophisticated analytics, companies can identify patterns, trends, and abnormalities that were previously inaccessible. By leveraging these insights and plans, companies can improve their operations, enhance the quality of products, and enhance resource allocation. Predictive algorithms can be utilized to predict specific equipment failures or identify business needs and address potential problems. Also, companies can reduce downtime, improve the use of applications and devices, and reduce maintenance costs. These strategies improve operations, supply chain management and control, and product quality control. The fast improvement of predictive algorithms and big data analysis provides:

- Enormous potential in studying product behaviours.

*Corresponding author. Email: mr.maad.alnaimiy@baghdadcollege.edu.iq

- Helping to make timely health decisions.
- Addressing data security and privacy concerns.
- Protecting sensitive information for businesses and users.

The fourth industrial revolution (4IR) covers many different areas of research and key technologies such as big data, smart factories, electronic, physical systems, Internet of Things, and interoperability where the entire supply chain can be digitized [16-20]. The 4IR seeks to operate artificial intelligence techniques to transform companies into a fully automated digital environment with all public and private data and information connected to each other digitally in one system and one environment and interacting fully to make decisions [21-23]. Physical systems and human operators must work seamlessly by collaborating in accomplishing tasks, and there is very important for there to be cooperation between machines and humans. The communication process between machines and humans occurs through a smart digital environment that facilitates the communication process and achieves many benefits, including monitoring real users and effective decentralized decision-making. In other words, a smart factory that contains mechanisms for monitoring all physical and real-time operations and decentralized decision-making can be implemented with maximum efficiency while offering many advantages to the workers in this factory. The 4IR is characterized by integrating digital technologies, such as artificial intelligence, robotics, the Internet of Things (IoT), big data, and automation, to develop a digital environment that has many advantages for companies and individuals [24-26]. AI-powered robotics and automation systems streamline industrial processes and enhance the quality of their products. Artificial intelligence methods enable robots to perform complex tasks, enhancing productivity, accuracy, manufacturing efficiency, and customer satisfaction [27][28]. Machine learning is an essential component of artificial intelligence in the 4IR. Machine learning algorithms contribute to making practices that help computers learn from huge amounts of data, recognize new patterns, and make correct decisions through prediction strategies, for instance, image recognition, natural language processing, recommendation systems, medical data analysis, and others [29][30]. Artificial intelligence is making significant progress in many domains, especially with the emergence of large applications such as ChatGPT and Bard [31-37]. These applications contribute to business development, increase productivity, and grow the human mind. Artificial intelligence is a science that includes a variety of computational techniques inspired by the way humans use their nervous systems and bodies to feel, learn, reason and act. The 4IR is the period that witnesses the emergence of electronic-physical systems with new capabilities like human capabilities. This capability is linked to the technologies, applications, and infrastructure of the 3IR. The 4IR is described as the merging of digital and biological technologies, affecting many aspects of our lives [38-40]. Influencing people's relationships with technology can change production processes, employment patterns, and how and where work is accomplished.
The main contribution of this article is to concentrate on the relationship between the 4IR and artificial intelligence methods and the impact of cybersecurity on the digital environment while conducting analyses and assessments of the precautions that must be taken in this domain. In addition, reviewing the most important conclusions reached in this article and identifying actions that can contribute to growing the digital environment.

2. Industry 4.0 Technology

Industry 4.0 refers to the integration of digital technologies and automation into industrial processes and includes many advanced technologies such as artificial intelligence, robotics, big data analysis, cloud computing, 3D printing (additive manufacturing) and the Internet of Things [41-45]. The essence of industry 4.0 lies in its ability to transform and develop industries and contribute to companies' economic growth [46-50]. It increases productivity and efficiency through enhanced automation, real-time data analysis, and reduced downtime. Also, it contributes to quality control and the use of resources more efficiently, as companies can achieve higher productivity with less resources, which leads to increased economic growth for these companies, achieving competitiveness and earning client satisfaction. Moreover, industry 4.0 facilitates the digital transformation of industries by connecting machines, systems and processes together in a digital environment. This connection enables data sharing and collaboration through certain mechanisms that allow company owners to make quick judgments and improve client experiences. The establishment of smart manufacturers is one of the most critical priorities of industry 4.0, where machines and systems are linked, communicate with each other through Internet of Things sensors and analyse data in real-time. Operators can monitor equipment performance, predict maintenance needs, prevent breakdowns, reduce downtime and costs, and improve maintenance schedules. Artificial intelligence and robot methods enable adjustable production practices that can rapidly adapt and meet all changing client requirements through the use and analysis of real-time data.

Fig. 1. Cobots operate with humans in industry [downloaded from Google].

The primary purpose of industry 4.0 is to improve human capabilities and make work more efficient, less stressful, and safer. Cobots can work with humans and help improve productivity and repetitive tasks by analysing data, making more profitable decisions, and concentrating on more complex and creative tasks. Figure 1 illustrates how cobots operate with humans in industry. Industry 4.0 can contribute to sustainable development by developing efficient practices in the use of company resources, assisting in data analysis, determining energy consumption patterns, and improving processes to reduce waste and environmental impact on the company's products, thus leading to reducing emissions associated with the company's products and preserving the surrounding environment. Industry 4.0 has the considerable potential to design economic growth for companies and working individuals by enhancing productivity and creating new business models serving a large society segment. Companies seeking digital transformation can rely on industry 4.0 technologies as they will gain a serious competitive advantage in the global market (see Figure 2). Thus, they can attract investment, encourage entrepreneurship, develop new job opportunities in modern technology sectors, and cooperate with international companies to increase the company's productivity. It is vital because it revolutionises industries by enhancing productivity, enabling the workforce to work in private companies, improving sustainability, and increasing economic growth for nations and companies. Industry 4.0 relies mainly on the knowledge of superior automation, interaction and communication between manufacturing technologies, which include cyber-physical systems, the Internet of Things and cloud computing, in order to create a smart manufacturer that meets client requirements. Digital technology changed the direction of the industry and enabled the convergence between the Internet of Things and robots through the use of artificial intelligence methods.

Fig. 2. The significant of industry 4.0 [49].

The Internet of Things has found many new business models across various industries that serve communities. The Internet of Things technology refers to a network that includes physical devices embedded with sensors, software, and connectivity, which allows them to collect and exchange data in a digital environment free from gaps and preserves users' privacy. In addition, the Internet of Things has opened up opportunities for new services and applications to spread and serve companies and individuals, as IoT devices can be integrated into the infrastructure and create a network that includes a group of devices linked with each other, for instance, home automation services, smart cities, wearable devices, and healthcare monitoring systems. These devices collect and analyse data and provide accurate outcomes to help staffers make the right decisions. The Internet of Things provides opportunities to create new data-based businesses, as the considerable amount of data collected by IoT devices is analysed to create unique patterns and make appropriate decisions. It is possible to generate income from this data through various means, such as providing data analysis services, developing products, etc., and this data cannot be sold to other parties after obtaining clients' approval. Companies can take advantage of the Internet of Things to create more efficient operations, provide new services, and gain a competitive advantage in the digital environment. Companies such as Amazon, Facebook and Netflix are among the modern pioneers of the new industrial revolution. Industry 4.0 is evolving rapidly, and technology companies need to evolve over time to compete in tomorrow's world. Companies such as Amazon, Facebook and Netflix are among the modern pioneers of the new industrial revolution.

3. Artificial intelligence and Industry 4.0

Cyber systems are continuously surveyed in smart factories, and their effectiveness in decentralized decision-making via the Internet of Things is confirmed. Cyber systems communicate with each other and with individuals in real-time, inside or outside the virtual environment. In order to create an efficient industry 4.0, companies must mainly rely on artificial intelligence techniques, which will create new job opportunities as well as fill the gap between the existing workforces. Artificial intelligence techniques seek to force the industry to invest and use new skills by hiring a good workforce that has the ability to deal with artificial intelligence applications in all fields. The main objective of industry 4.0 is to create an environment that relies heavily on artificial intelligence, digitization, and the Internet. Artificial intelligence techniques can be combined with cybersecurity to create smart models to classify malware and detect cyber-attacks because computer systems are frequently exposed to cyber threats [50-56]. These technologies are used to protect the privacy of users and computer systems and to prevent unauthorized access[57-60]. Moreover, machine learning algorithms are trained to recognize new patterns and create more innovative applications capable of detecting cyber-attacks and defending the digital environment. Meanwhile, the malicious use of artificial intelligence algorithms and the ability to make attack techniques more sophisticated does not go unnoticed. In industry 4.0, artificial intelligence and cybersecurity are two related domains that have significant roles in achieving a digital environment free of loopholes, as artificial intelligence contributes to strengthening cybersecurity defences. Machine learning algorithms can analyse large amounts of data to determine patterns and cyber threats by training these algorithms to identify malicious activities and behaviours. Artificial intelligence supports security analysts in identifying potential threats and investigating malicious application practices more efficiently. Intelligent algorithms process and correlate large amounts of security data, including logs, network traffic, and user behaviour within the digital environment, and determine indicators of breaches and systems vulnerabilities. Artificial intelligence algorithms are characterized by their ability to analyse the patterns and behaviour of users within the network to identify patterns and behaviours of electronic threats. This can support companies in detecting unauthorized access or abnormal user activities. Artificial intelligence is of great importance in enhancing cyber security. Companies must implement the following steps in growing their digital assets:

- Utilising machine learning algorithms to detect modern threats and malware.
- Updating computer systems operating artificial intelligence applications to discover security vulnerabilities and verify that systems are working perfectly.
- Training machine learning algorithms to protect the privacy of users and companies and not allow unauthorized individuals to manipulate or modify them.
- Enhancing collaboration between AI researchers and cybersecurity experts in designing more uncontroversial and trustworthy algorithms.
- Report users and companies of the risks associated with artificial intelligence techniques, such as deepfakes, and enhance critical thinking skills to combat misinformation.

The growth of networks and the Internet has provided users with an interconnected, interactive, and highly opportunely online environment. Artificial intelligence techniques are applied in many sectors thanks to the power of its algorithms that have the ability to improve the performance of computer systems. Moreover, cybersecurity techniques are also being improved using AI techniques or subsets of machine learning and neural networks to create AI-enhanced cybersecurity systems capable of protecting the digital environment from cyber-attacks. It is expected that the number of workers in the

cybersecurity sector will decrease by 2025 to approximately 2 million people due to the existence of artificial intelligence techniques that will replace humans in many positions by 2030. AI can assist in alleviating concerns while empowering existing cyber workers. HR systems are built by large groups of cybersecurity and natural language processing experts. AI can do the legal work of processing and analysing data to help make decisions. In addition, providing many training programs in all domains via the Internet. Artificial intelligence practices in cybersecurity help protect companies from cyber threats and recognise malicious programs. In addition, AI-based cybersecurity systems can provide practical security standards and help develop better strategies to prevent all kinds of electronic threats and not allow unauthorized individuals to tamper with data or create hidden components inside computer systems.

4. Conclusions

Traditional cybersecurity engineers play a significant role in protecting users' privacy, preventing unauthorized access, and protecting computer systems from electronic attacks, as they are characterized by confidentiality, integrity, and non-repudiation of user data. With the advent of Industry 4.0, transformative practices such as cloud computing, artificial intelligence, Internet of Things (IoT), and system automation have emerged. This industry faces many electronic attacks and cyber threats because it contains big data for many users and companies and is characterized by the rapid transfer of information and data between computer systems. Thus, vital cybersecurity techniques are required to protect electronic data from electronic operations and attacks and to ensure that this data is not stolen or tampered with. Cybersecurity engineers must familiarize themselves with the latest technologies and benefit from them in creating an electronic environment free of loopholes and not allowing electronic attacks to enter computer systems and control the data of users or companies. Continuous monitoring of this environment with attack prevention measures must be implemented to ensure the stability and security of digital ecosystems in industry 4.0. In the digital environment, cloud computing allows storing and processing huge amounts of data, and artificial intelligence works to enable systems to make smart decisions. Also, the existence of the Internet of Things connects computers with each other, creating a highly interconnected virtual system. Eventually, cybersecurity techniques need to implement robust systems control mechanisms, use encryption protocols to protect data in transit and implement intrusion detection and prevention systems to identify and block malicious activities. In the future, more articles will be made on the importance of Industry 4.0 and cyber security based on AI technologies.

Funding

Non.

Conflicts of Interest

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] Syam N. and Sharma A., “Waiting for a sales renaissance in the fourth industrial revolution: Machine learning and artificial intelligence in sales research and practice,” *Industrial Marketing Management*, vol.69, pp:135-146, February 2018. https://doi.org/10.1016/j.indmarman.2017.12.019

[2] Dimiduk D. M., Holm E. A., and Niezgoda S. R., “Perspectives on the Impact of Machine Learning, Deep Learning, and Artificial Intelligence on Materials, Processes, and Structures Engineering," *Integrating Materials and Manufacturing Innovation*, vol. 7, pp:157–172, August 2018. https://doi.org/10.1007/s40192-018-0117-8

[3] Mijwil M. M., Ali G., and Sadıkoğlu E., “The Evolving Role of Artificial Intelligence in the Future of Distance Learning: Exploring the Next Frontier,” *Mesopotamian Journal of Computer Science*, vol.2023, pp:98-105, May 2023. https://doi.org/10.58496/MJCSC/2023/012

[4] Zhang Z. and Lu Y., “Study on artificial intelligence: The state of the art and future prospects,” *Journal of Industrial Information Integration*, vol.23, pp:100224, September 2021. https://doi.org/10.1016/j.jii.2021.100224

[5] Dolgui A. and Ivanov D., “5G in digital supply chain and operations management: fostering flexibility, end-to-end connectivity and real-time visibility through internet-of-everything,” *International Journal of Production Research*, vol.60, no.2, pp:442-451, November 2021. https://doi.org/10.1080/00207543.2021.2002969

[6] Doshi R., Hiran K. K., Mijwil M. M., and Anand D., “To That of Artificial Intelligence, Passing Through Business Intelligence,” In Handbook of Research on AI and Knowledge Engineering for Real-Time Business Intelligence, pp:1-16, 2023. https://doi.org/10.4018/978-1-6684-6519-6.ch001.

[7] Al-mashhadani M. I., Hussein K. M., Khudir E. T., and ilyas M., “Sentiment Analysis using Optimized Feature Sets in Different Facebook/Twitter Dataset Domains using Big Data,” *Iraqi Journal For Computer Science and Mathematics*, vol. 3, no. 1, pp: 64–70, January 2022. https://doi.org/10.52866/ijcsm.2022.01.01.007

[8] Azeem M., Abualsoud B. M., and Priyadarshana D., “Mobile Big Data Analytics Using Deep Learning and Apache Spark,” *Mesopotamian Journal of Big Data*, vol.2023, pp:18–30, February 2023. https://doi.org/10.58496/MJBD/2023/003

[9] Korkmaz A., Aktürk C., and Talan T., “Analyzing the User's Sentiments of ChatGPT Using Twitter Data,” *Iraqi Journal For Computer Science and Mathematics*, vol. 4, no. 2, pp: 202–214, May 2023. https://doi.org/10.52866/ijcsm.2023.02.02.018

[10] Chen L., Zhang X., Chen A., Yao S., Hu X., and Zhou Z., "Targeted design of advanced electrocatalysts by machine learning," *Chinese Journal of Catalysis*, vol.43, no.1, pp:11-32, January 2022. https://doi.org/10.1016/S1872-2067(21)63852-4

[11] Mijwil M. M., "Deep Convolutional Neural Network Architecture to Detection COVID-19 from Chest X-ray Images," *Iraqi Journal of Science*, vol.64, no.5, pp:2561-2574, May 2023. https://doi.org/10.24996/ijs.2023.64.5.38

[12] Fei S., Hassan M. A., Xiao Y., Su X., Chen Z., et al., "UAV-based multi-sensor data fusion and machine learning algorithm for yield prediction in wheat," *Precision Agriculture*, vol.24, pp:187–212, August 2022. https://doi.org/10.1007/s11119-022-09938-8

[13] Mijwil M. M., Doshi R., Hiran K. K., Unogwu O. J., and Bala I., "MobileNetV1-Based Deep Learning Model for Accurate Brain Tumor Classification," *Mesopotamian Journal of Computer Science*, vol.2023, pp:32-41, March 2023. https://doi.org/10.58496/MJCSC/2023/005

[14] Vaishya R., Javaid M., Khan I. H., and Haleem A., "Artificial Intelligence (AI) applications for COVID-19 pandemic," *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol.14, no.4, pp:337-339, August 2020. https://doi.org/10.1016/j.dsx.2020.04.012

[15] Sivarajah U., Kamal M. M., Irani Z., and Weerakkody V., "Critical analysis of Big Data challenges and analytical methods," *Journal of Business Research*, vol.70, pp:263-286, January 2017.

[16] Oztemel E. and Gursev S., "Literature review of Industry 4.0 and related technologies," *Journal of Intelligent Manufacturing*, vol.31, pp:127–182, July 2018. https://doi.org/10.1007/s10845-018-1433-8

[17] Mijwil M. M., Hiran K. K., Doshi R., and Unogwu O. J., "Advancing Construction with IoT and RFID Technology in Civil Engineering: A Technology Review," *Al-Salam Journal for Engineering and Technology*, vol. 02, no. 02, pp:54-62, March 2023. https://doi.org/10.55145/ajest.2023.02.02.007

[18] Fanoro M., Božanić M., and Sinha S., "A Review of 4IR/5IR Enabling Technologies and Their Linkage to Manufacturing Supply Chain," *Technologies*, vol.09, no.04, pp:1-33, October 2021. https://doi.org/10.3390/technologies9040077

[19] David L. O., Nwulu N. I., Aigbavboa C. O., and Adepoju O. O., "Integrating fourth industrial revolution (4IR) technologies into the water, energy & food nexus for sustainable security: A bibliometric analysis," *Journal of Cleaner Production*, vol.363, pp:132522, August 2022. https://doi.org/10.1016/j.jclepro.2022.132522

[20] Hadjadj A. and Halimi K., "COVID-19 Patients' Health Monitoring System using Fuzzy Ontology and Internet of Things," *Iraqi Journal For Computer Science and Mathematics*, vol. 4, no. 1, pp:191–203, January 2023. https://doi.org/10.52866/ijcsm.2023.01.01.0016

[21] Nyagadza B., Pashapa R., Chare A., Mazuruse G., and Hove P. K., "Digital technologies, Fourth Industrial Revolution (4IR) & Global Value Chains (GVCs) nexus with emerging economies' future industrial innovation dynamics," Cogent Economics & Finance, vol.10, no.1, pp:1, January 2022. https://doi.org/10.1080/23322039.2021.2014654

[22] Mijwil M. M., Doshi R., Hiran K. K., Al-Mistarehi AH, and Gök M., "Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects," *Mesopotamian journal of cybersecurity*, vol.2022, pp:1-4, January 2022. https://doi.org/10.58496/MJCS/2022/001

[23] Bibby L. and Dehe B., "Defining and assessing industry 4.0 maturity levels – case of the defence sector," *Production Planning & Control*, vol.29, no.12, pp:1030-1043, September 2018. https://doi.org/10.1080/09537287.2018.1503355

[24] Shrivastava A., Krishna K. M., Rinawa M. L., Soni M., Ramkumar G., and Jaiswal S., "Inclusion of IoT, ML, and Blockchain Technologies in Next Generation Industry 4.0 Environment," *Materials Today: Proceedings*, vol.80, no.3, pp:3471-3475, 2023. https://doi.org/10.1016/j.matpr.2021.07.273

[25] Hoosain M. S., Paul B. S., and Ramakrishna S., "The Impact of 4IR Digital Technologies and Circular Thinking on the United Nations Sustainable Development Goals," *Sustainability*, vol.12, no.23, pp:10143, December 2020. https://doi.org/10.3390/su122310143

[26] Mhlanga D., "The Role of Artificial Intelligence and Machine Learning Amid the COVID-19 Pandemic: What Lessons Are We Learning on 4IR and the Sustainable Development Goals," *International Journal of Environmental Research and Public Health*, vol.19, no.3, pp:1879, February 2022. https://doi.org/10.3390/ijerph19031879

[27] Wu Y., "Cloud-Edge Orchestration for the Internet of Things: Architecture and AI-Powered Data Processing," *IEEE Internet of Things Journal*, vol.8, no.16, pp:12792 - 12805, August 2021. https://doi.org/10.1109/JIOT.2020.3014845

[28] Akter S., Hossain A., Sajib S., Sultana S., Rahman M., et al., "A framework for AI-powered service innovation capability: Review and agenda for future research," *Technovation*, vol.125, pp:102768, July 2023. https://doi.org/10.1016/j.technovation.2023.102768

[29] Ahsan M. and Siddique Z., "Machine learning-based heart disease diagnosis: A systematic literature review," *Artificial Intelligence in Medicine*, vol.128, pp:102289, June 2022. https://doi.org/10.1016/j.artmed.2022.102289

[30] Varoquaux G. and Cheplygina V., "Machine learning for medical imaging: methodological failures and recommendations for the future," *npj Digital Medicine*, vol.5, no.48, pp:1-8, April 2022. https://doi.org/10.1038/s41746-022-00592-y

[31] Mijwil M. M., Aljanabi M., and ChatGPT, "Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime," *Iraqi Journal For Computer Science and Mathematics*, vol.4, no.1, pp:65-70, January 2023. https://doi.org/10.52866/ijcsm.2023.01.01.0019

[32] Mijwil M. M., Aljanabi M., and Ali A. H., "ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information," *Mesopotamian journal of cybersecurity*, vol.2023, pp:18-21, February 2023. https://doi.org/10.58496/MJCS/2023/004

[33] Mijwil M. M., Filali Y., Aljanabi M., Bounabi M., Al-Shahwani H., "The Purpose of Cybersecurity in the Digital Transformation of Public Services and Protecting the Digital Environment," *Mesopotamian journal of cybersecurity*, vol.2023, pp:1-6, January 2023. https://doi.org/10.58496/MJCS/2023/001

[34] Mijwil M. M., Hiran K. K., Doshi R., Dadhich M., Al-Mistarehi AH , and Bala I., "ChatGPT and the Future of Academic Integrity in the Artificial Intelligence Era: A New Frontier," *Al-Salam Journal for Engineering and Technology*, vol. 2, no. 2, pp116-127, April 2023. https://doi.org/10.55145/ajest.2023.02.02.015

[35] Haque M. U., Dharmadasa I., Sworna Z. T., Rajapakse R. N., and Ahmad H., "I think this is the most disruptive technology": Exploring Sentiments of ChatGPT Early Adopters using Twitter Data," *Arxiv*, pp:1-12, December 2022. https://doi.org/10.48550/arXiv.2212.05856

[36] Rudolph J., Tan S., and Tan S., "ChatGPT: Bullshit spewer or the end of traditional assessments in higher education?," *Journal of Applied Learning and Teaching*, vol. 6, no.1, pp:1-22, January 2023. https://doi.org/10.37074/jalt.2023.6.1.9

[37] Aljanabi M., Ghazi M., Ali A. H., Abed S. A., and ChatGPT, "ChatGpt: Open Possibilities," *Iraqi Journal For Computer Science and Mathematic*s, vol. 4, no. 1, pp: 62–64, January 2023. https://doi.org/10.52866/20ijcsm.2023.01.01.0018

[38] Soh C. and Connolly D., "New Frontiers of Profit and Risk: The Fourth Industrial Revolution's Impact on Business and Human Rights," *New Political Economy*, vol.26, no.1, pp: 168-185, February 2020. https://doi.org/10.1080/13563467.2020.1723514

[39] Noble S. M., Mende M., Grewal D., and Parasuraman A., "The Fifth Industrial Revolution: How Harmonious Human–Machine Collaboration is Triggering a Retail and Service [R]evolution," *Journal of Retailing*, vol.98, no.2, pp:199-208, June 2022. https://doi.org/10.1016/j.jretai.2022.04.003

[40] Hoosain M. S., Paul B. S., Doorsamy W., and Ramakrishna S., "The Influence of Circular Economy and 4IR Technologies on the Climate–Water–Energy–Food Nexus and the SDGs," *Water*, vol.15, no.4, pp:787, February 2023. https://doi.org/10.3390/w15040787

[41] Bala I., Bhamrah M. S., and Singh G., "Capacity in fading environment based on soft sensing information under spectrum sharing constraints," *Wireless Networks*, vol. 23, pp:519–531, December 2015. https://doi.org/10.1007/s11276-015-1172-0

[42] Bala I. and Ahuja K., "Energy-efficient framework for throughput enhancement of cognitive radio network by exploiting transmission mode diversity," *Journal of Ambient Intelligence and Humanized Computing*, vol.14, pp:2167–2184, August 2021. https://doi.org/10.1007/s12652-021-03428-x

[43] Bala I., Sharma A., Tselykh A., and Kim B., "Throughput optimization of interference limited cognitive radio-based Internet of Things (CR-IoT) network," *Journal of King Saud University - Computer and Information Science*s, vol.34, no.7, pp:4233-4243, July 2022. https://doi.org/10.1016/j.jksuci.2022.05.019

[44] Mijwil M. M., Gök M., Doshi R., Hiran K. K.,and Kösesoy I., "Utilizing Artificial Intelligence Techniques to Improve the Performance of Wireless Nodes," In Applications of Artificial Intelligence in Wireless Communication Systems", pp:150-162, June 2023. https://doi.org/10.4018/978-1-6684-7348-1.ch010

[45] Yadav V. S., Singh A. R., Raut R. D., Mangla S. K., Luthra S., and Raut R. D., "Exploring the application of Industry 4.0 technologies in the agricultural food supply chain: A systematic literature review," *Computers & Industrial Engineering*, vol.169, pp:108304, July 2022. https://doi.org/10.1016/j.cie.2022.108304

[46] Saniuk S., Grabowska A., and Straka M., "Identification of Social and Economic Expectations: Contextual Reasons for the Transformation Process of Industry 4.0 into the Industry 5.0 Concept," *Sustainability*, vol.14, no.3, pp:1391, January 2022. https://doi.org/10.3390/su14031391

[47] Ching N. T., Ghobakhloo M., Iranmanesh M., Maroufkhani P., and Asadi S., "Industry 4.0 applications for sustainable manufacturing: A systematic literature review and a roadmap to sustainable development," *Journal of Cleaner Production*, vol.334, pp:130133, February 2022. https://doi.org/10.1016/j.jclepro.2021.130133

[48] Ahmad T., Zhu H., Zhang D., Tariq R., Bassam A., et al., "Energetics Systems and artificial intelligence: Applications of industry 4.0," *Energy Reports*, vol.8, pp:334-361, November 2022. https://doi.org/10.1016/j.egyr.2021.11.256

[49] HSRC, "Industry 4.0 Technologies," 2019. https://industry40marketresearch.com/blog/industry_4-0_technologies/

[50] Salem I. E., Mijwil M. M., Abdulqader A. W., Ismaeel M. M., Alkhazraji A., and Alaabdin A. M. Z., "Introduction to The Data Mining Techniques in Cybersecurity," *Mesopotamian journal of cybersecurity*, vol.2022, pp:28-37, May 2022. https://doi.org/10.58496/MJCS/2022/004

[51] Sharma D. K., Mishra J., Singh A., Govil R., Srivastava G., and Lin J. C. L., "Explainable Artificial Intelligence for Cybersecurity," *Computers and Electrical Engineering*, vol.103, pp:108356, October 2022. https://doi.org/10.1016/j.compeleceng.2022.108356

[52] Mijwil M. M., Salem I. E., and Ismaeel M. M., "The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review," *Iraqi Journal For Computer Science and Mathematics*, vol.4 no.1, pp:87-101, January 2023, https://doi.org/10.52866/ijcsm.2023.01.01.008.

[53] Naik B., Mehta A., Yagnik H., and Shah M., "The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review," *Complex & Intelligent Systems*, vol.8, pp:1763–1780, August 2021. https://doi.org/10.1007/s40747-021-00494-8

[54] Radanliev P. and De Roure D., "Advancing the cybersecurity of the healthcare system with self-optimising and self-adaptative artificial intelligence (part 2)," *Health and Technology*, vol.12, pp:923–929, August 2022. https://doi.org/10.1007/s12553-022-00691-6

[55] Radanliev P., Roure D., Maple C., and Ani U., "Super-forecasting the 'technological singularity' risks from artificial intelligence," *Evolving Systems*, vol.13, pp:747–757, June 2022. https://doi.org/10.1007/s12530-022-09431-7

[56] Mijwil M. M., Unogwu O. J., Filali Y., Bala I., and Al-Shahwani H., "Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview," *Mesopotamian journal of cybersecurity*, vol.2023, pp:57-63, March 2023. *https://doi.org/10.58496/MJCS/2023/010*

[57] A. H. Ali and M. Z. Abdullah, "A parallel grid optimization of SVM hyperparameter for big data classification using spark Radoop," Karbala International Journal of Modern Science, vol. 6, no. 1, p. 3, 2020.

[58] A. H. Ali and M. Z. Abdullah, "An efficient model for data classification based on SVM grid parameter optimization and PSO feature weight selection," International Journal of Integrated Engineering, vol. 12, no. 1, pp. 1-12, 2020.

[59] H. M. Fadhil, M. Abdullah, and M. Younis, "Innovations in T-way test creation based on a hybrid hill climbing-greedy algorithm," IAES International Journal of Artificial Intelligence, vol. 12, no. 2, p. 794, 2023.

[60] B. A. Shahal and M. N. Abdullah, "A review of localization algorithms based on software defined networking approach in wireless sensor network," Measurement: Sensors, p. 100772, 2023.