ISSN No:-2456-2165

A Review of the Prospects and Constraints for Using Artificial Intelligence for the Interpretation of Remote Sensing Data

Md. Tarek Hossain, Rumi Afrin , Mohd. Al- Amin Biswas
Department of Computer Science and Engineering
Bangladesh University of Business and Technology (BUBT

Abstract:- The abstract of a paper on the prospects and restrictions of applying artificial intelligence (AI) for remote sensing data interpretation will most likely discuss the junction of AI and remote sensing, stressing potential benefits and challenges. It may discuss advances in AI approaches and their applications in evaluating large and complicated remote sensing datasets, as well as limitations and issues that researchers and practitioners should be aware of. The abstract could underline the significance of precise remote sensing data interpretation for environmental monitoring, resource management, disaster response, and other essential applications. The rapid growth of artificial intelligence (AI) tools has changed the field of remote sensing data interpretation, creating previously unimaginable prospects for extracting useful insights from enormous and complicated datasets. This study provides an in-depth examination of the opportunities and restrictions involved with using AI to understand remote sensing data, offering insight on the revolutionary potential of this integration. This research also discusses the essential restrictions and challenges associated with AI integration in remote sensing. Some AI models are black boxes, which raises concerns about transparency, interpretability, and the possibility of biased decision-making. To ensure the ethical use of AI in remote sensing interpretation, a careful balance of algorithmic complexity and the capacity to give interpretable results that fit with domain knowledge must be struck. This article offers a comprehensive evaluation of the opportunities and restrictions associated with using artificial intelligence to understand remote sensing data. Researchers and practitioners can use AI's revolutionary potential to gain deeper insights into Earth's dynamics and contribute to a more sustainable and informed future.

Keywords:- *Artificial Intelligence, Remote Sensing, Constraints, Interpretation, Prospects.*

I. INTRODUCTION

The fast spread of remote sensing technology has changed our ability to observe and monitor the Earth's surface and atmosphere at unprecedented scales and resolutions [1]. This rush of data, however, has brought a new challenge: how to efficiently and accurately assess and extract valuable insights from massive amounts of information recorded by satellites, drones, and ground-based sensors. As a result, incorporating artificial intelligence (AI) techniques into the interpretation of remote sensing data has emerged as a possible option to address this difficulty.

Machine learning and deep learning, in particular, have the potential to transform how we analyze and interpret remote sensing data [2]. These techniques have proven their worth in a variety of applications, ranging from image classification and object detection to time series analysis and anomaly detection. Researchers and practitioners are exploring novel techniques to improve the efficiency, accuracy, and depth of information retrieved from remote sensing observations by leveraging AI's capacity to discern complex patterns and relationships within data. This paper provides a thorough examination of both the opportunities and restrictions connected with using artificial intelligence to understand remote sensing data. It dives into the revolutionary potential of AI-driven interpretation, demonstrating how these techniques have the ability to revolutionize industries such as environmental monitoring, disaster response, urban planning, and a The incorporation of AI approaches opens up a plethora of opportunities for better remote sensing interpretation [3]. AI systems excel at dealing with the inherent complexity of remote sensing data. AI-driven interpretation can give insights that human analysis may overlook by autonomously discovering subtle patterns and relationships within multispectral and hyperspectral data.

Automated Feature Extraction: Artificial intelligence (AI) can automate the feature extraction process, allowing for the detection of crucial environmental indicators such as land cover, vegetation health, and hydrological patterns. This automation speeds up data processing while decreasing the need for manual intervention [4]. Artificial intelligence-powered systems can continually monitor remote sensing data streams in real-time, discovering abnormalities, changes, or events that demand rapid action, such as natural catastrophes or pollution crises. Machine learning and deep learning techniques make it possible to build predictive models that predict future environmental conditions, which aids in climate modeling, agricultural yield predictions, and ecosystem health assessments.

This review of the opportunities and restrictions for employing artificial intelligence (AI) in remote sensing data interpretation can make numerous significant contributions to the field of remote sensing, AI research, and related applications.

II. METHODOLOGY

An assessment of the opportunities and restrictions for applying artificial intelligence (AI) for remote sensing data interpretation would comprise three important phases to thoroughly analyze and evaluate the current status of the subject. Here's a high-level overview of the methodology:

A. Problem Definition and Scope:

- Clearly explained the review's goal, which is to examine the potential and limitations of AI in analyzing remote sensing data.
- Defined the scope of the evaluation, including the types of remote sensing data (e.g., satellite imagery, LiDAR data) and specific AI techniques (e.g., machine learning algorithms, deep learning models) to be addressed [5].

B. Review of the Literature:

- Conducted a thorough literature study to discover relevant research papers, articles, and studies relating to AI applications in remote sensing data interpretation.
- Analyzed and synthesize the available literature to identify trends, difficulties, and advancements in the topic.

C. Explaining AI Techniques:

- Provided an introduced of several AI techniques typically used in remote sensing data interpretation, such as machine learning algorithms (e.g., Random Forest, Support Vector Machines) and deep learning models (e.g., Convolutional Neural Networks, Recurrent Neural Networks).
- Discussed the advantages, disadvantages, and appropriateness of these strategies for various types of remote sensing data interpretation jobs.

D. Constraints and difficulties:

- Identified and discussed the restrictions and obstacles associated with AI-based remote sensing data interpretation, such as limited labeled data, the interpretability of AI models, data preprocessing needs, and computational demands [6].
- Addressed any ethical, legal, or privacy concerns that may arise from AI-driven analysis of remote sensing data.

E. Examples of Cases:

- Provided thorough case studies demonstrating the successful application of AI approaches to remote sensing data interpretation. In each case study, emphasize the approaches employed, the results obtained, and the lessons gained.

Following this methodology, this study would provide a comprehensive assessment of the current state and future possibilities of applying AI for remote sensing data interpretation, providing significant insights for researchers, practitioners, and decision-makers in the field.

III. ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is a fast developing branch of computer science that focuses on developing systems and machines that can do activities that would normally need human intelligence. Problem-solving, decision-making, interpreting [7] natural language, identifying patterns, and learning from experiences are examples of these tasks. Machine learning, neural networks, natural language processing, and robots are examples of AI approaches and technologies.

A subset of AI is machine learning, which allows computers to learn from data and improve their performance over time without being explicitly programmed. Neural networks, which are modeled after the structure of the human brain, are used to model complex relationships in data, allowing AI systems to process and analyze vast volumes of data [8]. Natural language processing enables computers to perceive, interpret, and synthesize human language, resulting in more natural and intuitive interactions between humans and technology. AI uses range from healthcare to finance to manufacturing to entertainment and beyond. AI-powered systems may detect medical ailments, forecast financial market trends, improve supply chains, generate tailored suggestions, and even help with creative efforts such as painting and music.

As artificial intelligence technology progresses, ethical considerations, transparency, and responsible AI development become more crucial. It is critical for the successful integration of AI systems into society to ensure that they are fair, unbiased, and respect privacy [9]. While AI has already revolutionized many aspects of our lives, continued research and innovation are pushing the boundaries of what is possible, offering a future in which AI-driven solutions play a vital role in changing the world.

Traditional computational approaches have numerous advantages over ANNs [10]. An ANN composed of nonlinear parts is nonlinear in and of itself, can learn an input-output mapping from a teacher, can adjust its synaptic weights to adapt to the environment, can deal with partial information, and can deliver responses under uncertainty. It is worth mentioning that the analogy with the brain motivates or inspires ANNs, while the urge to create an artificial brain lags far behind. ANN is now viewed as a paradigm for doing computations in an effective and efficient manner, rather than an attempt to replicate a real brain [11]. To illustrate the differences between the brain and ANNs, events in silicon chips occur in nanoseconds, whereas responses in neurons occur in milliseconds. The brain performs enormous parallel computing to compensate for the speed. The human cortex contains approximately 10 billion neurons and 60 trillion synapses. In terms of power usage, the brain consumes around 10-16 joules per operation per second, whereas computers consume approximately 10-6 joules per operation per second.

IV. AI ARCHITECTURE

A neuron is a computational element that serves as the foundation of an ANN. Figure 1 depicts the most typical model of a neuron. A neuron receives x 1..., xm inputs. Different synaptic weights influence each connection from the input to the processing unit. A signal xj is multiplied by synaptic weight wkj at the input of synapse or connection j, which is coupled to neuron k. An adder adds all inputs together to generate a linear combination. The activation function is employed to limit the neuron's output [12]. Figure 1 also includes an external bias w 0, having the effect of raising or lowering the net input to the activation function.

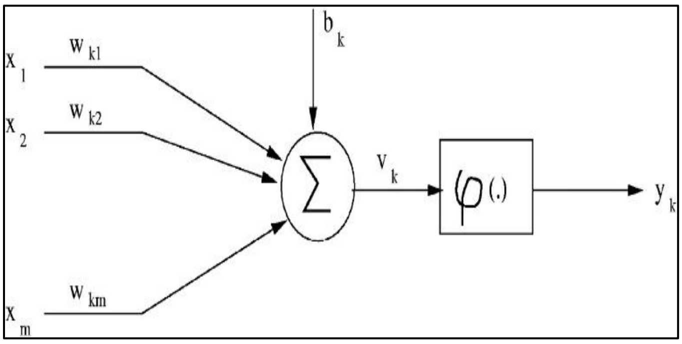

Fig. 1: Anatomy of an artificial neuron.

A neuron is described in mathematical terms by the following equations:

where w0 is the bias and x0 =1.

The network topology or architecture refers to how neurons are placed in a neural network. The learning algorithm is closely connected to the architecture used in ANNs. There are three types of ANN architectures: (i) singlelayer feedforward networks, (ii) multilayer feedforward networks, and (iii) recurrent networks. Figure 2 also shows the AI architecture [13].

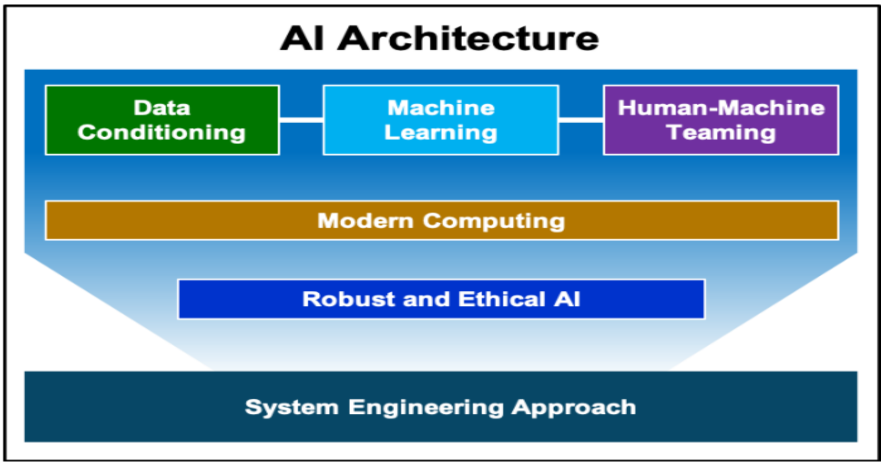

Fig. 2: Artificial Architecture

V. THE USE OF ANNS IN REMOTE SENSING

The primary tasks of remote sensing data analysis in which the application of ANNs is reported are classification, more specifically land cover classification, unmixing, and retrieval of biophysical properties of cover [14]. ANNs have also been used for change detection, data fusion, forecasting, preprocessing, georeferencing, and object recognition. Because of their ability to understand complicated relationships and patterns from vast datasets, Artificial Neural Networks (ANNs) have found significant applications in remote sensing. ANNs are a type of machine learning model that is inspired by the form and operation of the neural networks in the human brain. Here are some examples of how ANNs are utilized in remote sensing:

- **Image Classification and Object Detection**: ANNs are used in remote sensing imagery to categorize land cover, land use, and other features. Convolutional Neural Networks (CNNs), a form of ANN, excel at picture classification tasks by learning features at various levels of abstraction automatically [15]. CNNs are also used to recognize, locate, and classify individual objects inside images.
- **Semantic Segmentation**: For semantic segmentation, ANNs, particularly Fully Convolutional Networks (FCNs) and U-Net architectures, are used. This entails assigning a distinct class to each pixel in an image, allowing for precise mapping of land cover and land use patterns [16].

- **Change Detection**: ANNs can detect differences in time-series remote sensing images, assisting in the monitoring of urban development, deforestation, natural catastrophes, and other phenomena [16].
- **Analysis of Hyperspectral Data**: Hyperspectral data comprises information from hundreds of tiny, contiguous spectral bands. Based on their spectral characteristics, ANNs may analyse this data to identify materials, minerals, and other compounds [17].ANNs can improve the resolution of remote sensing photos, enhancing details and allowing for better feature recognition.
- **Land Cover Classification**: ANNs aid in the accurate classification of various land cover categories, such as forests, bodies of water, urban areas, and agricultural fields.
- **Terrain & Elevation Modelling**: ANNs can build high-resolution digital elevation models (DEMs) from remote sensing data, which can be used to aid in terrain analysis and flood modelling.
- **Weather and Atmospheric Correction**: ANNs are used to improve image quality and accuracy by correcting atmospheric impacts in remote sensing photos.
- **Feature Extraction**: ANNs are used to extract features from remote sensing data, allowing for the identification of relevant information for further study.
- **Data fusing**: ANNs enable the fusing of data from several sensors (e.g., optical, radar) to improve information accuracy and richness.
- **Quality Control and Anomaly Detection:** ANNs may detect anomalies or errors in remote sensing data automatically, improving data quality and dependability.
- **Multi-Temporal Analysis**: ANNs aid in the analysis of remote sensing data collected at various time points, allowing for the monitoring of land use changes, vegetation growth, and other phenomena.
- The application of ANNs in remote sensing necessitates proper data preparation, model architecture design, and training. Because ANNs learn from data, it is critical to gather high-quality and representative training datasets. Considerations such as model interpretability, overfitting, and generalization must also be addressed [18]. Overall, ANNs provide a robust and adaptable toolkit for deriving meaningful insights from remote sensing data in a variety of applications.

VI. TECHNIQUES OF ARTIFICIAL INTELLIGENCE FOR DATA INTERPRETATION

AI approaches have showed considerable promise in the interpretation of remote sensing data, allowing for more efficient and accurate processing of complex imagery. Here are some of the most common AI algorithms for understanding remote sensing data:

A. Machine Learning (ML):

- **Supervised Learning**: Supervised Learning entails training a model on labelled training data in order to make predictions on new, unlabelled data. Support Vector Machines (SVM), Random Forests, and Decision Trees are examples of popular algorithms [19].
- **Unsupervised Learning**: This technique is used to uncover patterns and relationships in data without the use of labeled training samples [20]. Clustering algorithms such as k-means and hierarchical clustering are examples.
- **Semi-Supervised Learning**: Semi-supervised learning combines components of supervised and unsupervised learning by combining a small amount of labelled data and a larger amount of unlabelled data.

B. Deep Learning:

- **Convolutional Neural Networks (CNN):** CNNs are well-suited for image analysis jobs because they can automatically learn hierarchical features from raw pixel data.
- **Recurrent Neural Networks (RNN)**: While useful for sequence-based data, RNNs can also be applied to time-series remote sensing data, such as satellite imagery over time.
- **GANs (Generative Adversarial Networks):** GANs may generate synthetic data that closely matches real remote sensing imagery, assisting in data augmentation and training.

C. Feature Extraction and Representation:

- **Principal Component Analysis (PCA):** Reduces the dimensionality of data by translating it into a new coordinate system.
- **Autoencoders:** Autoencoders are neural network topologies that are used for unsupervised learning of efficient data encodings.
- **Feature Fusion**: The integration of information from several sources or bands of remote sensing data to improve interpretation.

D. Detection and Segmentation of Objects:

To recognize and outline items of interest within remote sensing data, techniques such as Faster R-CNN, YOLO (You Only Look Once), and Mask R-CNN are utilized.

- **Segmentation based on semantics:** A label is assigned to each pixel in an image, allowing for detailed land cover or land use classification.

E. Learning Transfer:

Using pre-trained AI models and fine-tuning them for remote sensing tasks on huge datasets, eliminating the need for significant labelled data.

- **Methods of Ensemble:** Predictions from various AI models are combined to increase overall accuracy and resilience.
- **Analysis of Space and Time:** Using spatial and temporal information from remote sensing data to examine changes and trends across time.
- **Geographical Analysis:** Using remote sensing data in conjunction with geographic information systems (GIS) to do advanced spatial analysis.
- **XAI (Explainable AI):** Techniques aimed at improving transparency and trust by making AI model predictions interpretable and intelligible.

VII. STEPS OF INTERPRETATION OF REMOTE SENSING DATA USING AI

Interpreting remote sensing data with artificial intelligence (AI) is a sequence of procedures that use AI approaches to extract useful insights and information from data acquired by sensors, satellites, and other remote sensing platforms [21]. The following are the main steps in the interpretation process:

- **Data Acquisition and Preprocessing:** Gather remote sensing data using a variety of sensors such as satellites, drones, or ground-based equipment. Preprocess the data to remove sensor-specific distortions, atmospheric effects, noise, and other artifacts that may have an impact on the data's quality and accuracy [22].
- **Data Representation:** Convert the raw data into an analysis-ready format. This may entail translating imagery into distinct spectral bands, indices (for example, NDVI for vegetation), or other data representations that highlight specific aspects or qualities of interest [23].
- **Feature Extraction and Selection:** Use AI approaches to extract relevant features from data automatically [24]. This could include detecting textures, forms, patterns, or other distinguishing characteristics associated with specific land cover types, events, or changes.
- **Algorithm Selection:** Based on the specific interpretation task, select relevant AI algorithms. For image analysis, this could entail utilizing machine learning methods such as random forests, support vector machines, or deep learning structures such as convolutional neural networks (CNNs) [25].
- **Preparation of Training Data:** Make a labelled dataset with examples of the classes or phenomena you want to investigate. This dataset is used to train the AI model to recognize and categorize various features in remote sensing data.
- **Model Training:** Use the prepared training dataset to train the AI model. The model learns to recognize patterns and correlations between data features and their corresponding classes.
- **Validation and Evaluation:** Assess the performance of the trained AI model using validation datasets. Metrics such as accuracy, precision, recall, and F1-score are used to measure the model's ability to correctly classify and interpret features.
- **Model Optimization:** Improve the performance of the AI model by fine-tuning its parameters and architecture. This step may include tweaking hyperparameters, employing data augmentation techniques, or investigating various network designs.
- **Interpretation and Classification:** For classification and interpretation, apply the trained AI model to the complete remote sensing dataset. Based on learning patterns, the model gives classifications or labels to individual pixels or regions [26].
- **Post-Processing and Visualization:** Use post-processing techniques to refine the interpreted results. Filtering out noise, removing minor artifacts, or combining pixel-level classifications into larger meaningful units could all be part of this. Use maps, graphs, or other visualization tools to visualize the interpreted data.
- **Domain Knowledge Integration:** Work with domain experts to validate and contextualize interpreted outcomes. Domain knowledge contributes to ensuring that AI-generated interpretations are accurate, relevant, and applicable to the specific environmental setting.
- **Constant Monitoring and Updating:** Interpreting remote sensing data is an ongoing effort. To maintain the quality and relevance of the interpretations, regularly update and retrain the AI model as new data becomes available or as the environment changes.

By following these procedures, academics and practitioners can use artificial intelligence to extract significant insights from remote sensing data, thereby contributing to informed decision-making, environmental monitoring, and a variety of applications across domains.

VIII. CONSTRAINTS AND CHALLENGES

Despite the attractive promises, the integration of AI into remote sensing interpretation provides some important restrictions and challenges:

- **Transparency and comprehensibility:** Many AI models, particularly deep neural networks, operate like black boxes, making it impossible to explain their decision-making processes [27]. It is critical to ensure transparency and interpretability in order to gain the trust of stakeholders and experts who rely on accurate and intelligible interpretations.
- **Data Quality and Quantity:** AI approaches rely largely on labelled training data that is of high quality. Obtaining extensive and accurate labelled datasets, especially for infrequent or dynamic occurrences, can be difficult and may have an impact on AI model performance [28].
- **Domain Expertise:** To ensure that AI-generated insights are contextually appropriate and matched with the specific intricacies of environmental dynamics, effective interpretation of remote sensing data requires domain expertise [29].
- **Ethical problems:** The employment of artificial intelligence in remote sensing interpretation presents ethical problems about prejudice, justice, and unforeseen effects. To avoid perpetuating current inequities and inaccuracies, it must be carefully considered [30].
- **Generalization to Complex Environments:** Data from remote sensing cover a wide range of ecosystems, landforms, and atmospheric conditions. To deliver accurate interpretations in a variety of environmental scenarios, AI models must generalize well across these complexities [31].
- **Scalability and computational resources:** AI models, particularly deep learning systems, can be computationally intensive [32]. It is a continuous challenge to ensure that AI-driven interpretations are computationally possible and scalable for large-scale remote sensing datasets.

IX. DISCUSSION

The incorporation of artificial intelligence (AI) tools into remote sensing data interpretation holds great promise for furthering our understanding of Earth's complicated dynamics. This fusion, however, carries with it a set of opportunities and limits that influence the potential effect and challenges of using AI in this domain [33]. AI technologies, particularly machine learning and deep learning, can automatically evaluate massive amounts of remote sensing data. These algorithms excel in detecting complex patterns, correlations, and trends that typical hand analysis may miss. Artificial intelligence-driven interpretation allows for the automatic extraction of relevant information from raw remote sensing data. This feature speeds up the detection of crucial indicators including land cover changes, urbanexpansion, and vegetation health, resulting in more efficient and accurate insights [34].

Artificial intelligence integration enables real-time monitoring of remote sensing data streams. AI-powered systems can detect abnormalities, odd events, or environmental changes quickly, allowing for early alerts and swift responses to natural catastrophes, pollution problems, and other emergent circumstances. Based on previous data, AI models can be taught to develop predictive models that estimate future environmental conditions [35]. These predicted insights help with proactive disaster preparedness, resource allocation, and climate modelling. AI may customize and contextualize its interpretation based on unique settings and aims. This versatility allows for tailored analysis for a wide range of applications, including urban planning, agriculture, forestry, and ecosystem monitoring.

Many AI algorithms, particularly massive deep neural networks, operate as "black boxes," making it difficult to explain their decision-making processes [36]. Transparency and interpretability are crucial for building trust in AI-generated interpretations and encouraging collaboration between AI experts and domain experts [37]. AI approaches rely significantly on high-quality, labelled training data. It is critical to have access to accurate, diverse, and representative datasets when developing robust and reliable AI models. Obtaining such datasets, particularly for unusual events or remote locales, remains difficult. The use of artificial intelligence into the analysis of remote sensing data has enormous potential to transform our understanding of Earth's dynamics [38]. While opportunities such as improved analysis, automation, and predictive modelling have the potential to be transformative, constraints such as openness, data availability, domain expertise, ethics, and generalization must be appropriately handled. Researchers and practitioners may use the power of AI to extract actionable insights, advance environmental monitoring, and contribute to informed decision-making for a sustainable future by navigating these difficulties and capitalizing on the opportunities [39].

X. CONCLUSION

The use of artificial intelligence into the interpretation of remote sensing data holds enormous promise for redefining how we perceive and adapt to Earth's changing dynamics. This study delves into the opportunities AI presents for improving data analysis, feature extraction, real-time monitoring, and predictive modeling. Simultaneously, it addresses the fundamental restrictions of openness, data availability, domain expertise, and ethical issues that must be managed to ensure the responsible and effective deployment of AI-driven remote sensing interpretation. By solving these issues, academics and practitioners can realize AI's full potential and contribute to more educated, sustainable, and actionable insights from remote sensing data. The successful integration of artificial intelligence with remote sensing data interpretation is dependent on interdisciplinary collaboration among AI researchers, remote sensing experts, domain specialists, and policymakers. We can harness the full potential of AI to unlock new frontiers in remote sensing applications by fostering an environment of continuous learning, adaptation, and innovation, resulting in more sustainable resource management, improved disaster preparedness, and a deeper understanding of our dynamic planet.

REFERENCES

[1.] Zhang, L., & Zhang, L. (2022). Artificial intelligence for remote sensing data analysis: A review of challenges and opportunities. IEEE Geoscience and Remote Sensing Magazine, 10(2), 270-294.

[2.] Shirmard, H., Farahbakhsh, E., Müller, R. D., & Chandra, R. (2022). A review of machine learning in processing remote sensing data for mineral exploration. Remote Sensing of Environment, 268, 112750.

[3.] Bohr, A., &Memarzadeh, K. (2020). The rise of artificial intelligence in healthcare applications. In Artificial Intelligence in healthcare (pp. 25-60). Academic Press.

[4.] Ahmad, T., Zhang, D., Huang, C., Zhang, H., Dai, N., Song, Y., & Chen, H. (2021). Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities. Journal of Cleaner Production, 289, 125834.

[5.] Chakraborty, A., Alam, M., Dey, V., Chattopadhyay, A., &Mukhopadhyay, D. (2018). Adversarial attacks and defences: A survey. arXiv preprint arXiv:1810.00069.

[6.] Chakraborty, A., Alam, M., Dey, V., Chattopadhyay, A., &Mukhopadhyay, D. (2021). A survey on adversarial attacks and defences. CAAI Transactions on Intelligence Technology, 6(1), 25-45.

[7.] Rawal, A., Rawat, D., & Sadler, B. M. (2021). Recent advances in adversarial machine learning: status, challenges and perspectives. Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III, 11746, 701-712.

[8.] Rawal, A., Rawat, D., & Sadler, B. M. (2021). Recent advances in adversarial machine learning: status, challenges and perspectives. Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III, 11746, 701-712.
[9.] Walter, M. J., Barrett, A., Walker, D. J., & Tam, K. (2023). Adversarial AI testcases for maritime autonomous systems. AI, Computer Science and Robotics Technology.
[10.] Kim, J., & Park, N. (2020). Blockchain-based data-preserving AI learning environment model for AI cybersecurity systems in IoT service environments. Applied Sciences, 10(14), 4718.
[11.] Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on artificial intelligence enhancing internet of things security: A survey. Ieee Access, 8, 153826-153848.
[12.] Ebers, M. (2021). Standardizing AI-The Case of the European Commission's Proposal for an Artificial Intelligence Act. The Cambridge handbook of artificial intelligence: global perspectives on law and ethics.
[13.] Walter, M. J., Barrett, A., Walker, D. J., & Tam, K. (2023). Adversarial AI testcases for maritime autonomous systems. AI, Computer Science and Robotics Technology.
[14.] Liu, P., Xu, X., & Wang, W. (2022). Threats, attacks and defenses to federated learning: issues, taxonomy and perspectives. Cybersecurity, 5(1), 1-19.
[15.] Zhou, S., Liu, C., Ye, D., Zhu, T., Zhou, W., & Yu, P. S. (2022). Adversarial attacks and defenses in deep learning: From a perspective of cybersecurity. ACM Computing Surveys, 55(8), 1-39.
[16.] Nguyen, H., Di Troia, F., Ishigaki, G., & Stamp, M. (2023). Generative adversarial networks and image-based malware classification. Journal of Computer Virology and Hacking Techniques, 1-17.
[17.] Devagiri, J. S., Paheding, S., Niyaz, Q., Yang, X., & Smith, S. (2022). Augmented Reality and Artificial Intelligence in industry: Trends, tools, and future challenges. Expert Systems with Applications, 118002.
[18.] Costa, J. C., Roxo, T., Proença, H., &Inácio, P. R. (2023). How Deep Learning Sees the World: A Survey on Adversarial Attacks & Defenses. arXiv preprint arXiv:2305.10862.
[19.] Kaviani, S., Han, K. J., &Sohn, I. (2022). Adversarial attacks and defenses on AI in medical imaging informatics: A survey. Expert Systems with Applications, 198, 116815.
[20.] Bhandari, K., Kumar, K., &Sangal, A. L. (2023, May). Artificial Intelligence in Software Engineering: Perspectives and Challenges. In 2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC) (pp. 133-137). IEEE.
[21.] Giachos, I., Papakitsos, E. C., Savvidis, P., &Laskaris, N. (2023). Inquiring Natural Language Processing Capabilities on Robotic Systems through Virtual Assistants: A Systemic Approach. Journal of Computer Science Research, 5(2), 28-36.
[22.] Michel, A., Jha, S. K., &Ewetz, R. (2022). A survey on the vulnerability of deep neural networks against adversarial attacks. Progress in Artificial Intelligence, 1-11.
[23.] Alshahrani, E., Alghazzawi, D., Alotaibi, R., &Rabie, O. (2022). Adversarial attacks against supervised machine learning based network intrusion detection systems. Plos one, 17(10), e0275971.
[24.] de Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. Electronics, 12(8), 1920.
[25.] Conti, M., Li, J., Picek, S., & Xu, J. (2022, November). Label-only membership inference attack against node-level graph neural networks. In Proceedings of the 15th ACM Workshop on Artificial Intelligence and Security (pp. 1-12).
[26.] Kaviani, S., Han, K. J., &Sohn, I. (2022). Adversarial attacks and defenses on AI in medical imaging informatics: A survey. Expert Systems with Applications, 198, 116815.
[27.] Liang, H., He, E., Zhao, Y., Jia, Z., & Li, H. (2022). Adversarial attack and defense: A survey. Electronics, 11(8), 1283.
[28.] Qian, Z., Huang, K., Wang, Q. F., & Zhang, X. Y. (2022). A survey of robust adversarial training in pattern recognition: Fundamental, theory, and methodologies. Pattern Recognition, 131, 108889.
[29.] Chen, Y., Zhang, M., Li, J., &Kuang, X. (2022, July). Adversarial attacks and defenses in image classification: A practical perspective. In 2022 7th International Conference on Image, Vision and Computing (ICIVC) (pp. 424-430). IEEE.
[30.] Liang, H., He, E., Zhao, Y., Jia, Z., & Li, H. (2022). Adversarial attack and defense: A survey. Electronics, 11(8), 1283.
[31.] Esterhuizen, J. A., Goldsmith, B. R., &Linic, S. (2022). Interpretable machine learning for knowledge generation in heterogeneous catalysis. Nature Catalysis, 5(3), 175-184.
[32.] Alanazi, A. (2022). Using machine learning for healthcare challenges and opportunities. Informatics in Medicine Unlocked, 30, 100924.
[33.] Yang, J., Zhang, W., Liu, J., Wu, J., & Yang, J. (2022). Generating de-identification facial images based on the attention models and adversarial examples. Alexandria Engineering Journal, 61(11), 8417-8429.
[34.] Zhou, N. R., Zhang, T. F., Xie, X. W., & Wu, J. Y. (2023). Hybrid quantum–classical generative adversarial networks for image generation via learning discrete distribution. Signal Processing: Image Communication, 110, 116891.
[35.] Nguyen, N. B., Chandrasegaran, K., Abdollahzadeh, M., & Cheung, N. M. (2023). Re-thinking Model Inversion Attacks Against Deep Neural Networks. In Proceedings of the IEEE/CVF Conference on

Computer Vision and Pattern Recognition (pp. 16384-16393).
[36.] Zhang, R., Hidano, S., &Koushanfar, F. (2022). Text revealer: Private text reconstruction via model inversion attacks against transformers. arXiv preprint arXiv:2209.10505.
[37.] Amerirad, B., Cattaneo, M., Kenett, R. S., & Luciano, E. (2023). Adversarial Artificial Intelligence in Insurance: From an Example to Some Potential Remedies. Risks, 11(1), 20.
[38.] Xu, L., Zheng, X., Li, X., Zhang, Y., Liu, L., & Ma, H. (2022, September). WiCAM: Imperceptible Adversarial Attack on Deep Learning based WiFi Sensing. In 2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON) (pp. 10-18). IEEE.
[39.] Amirkhani, A., Karimi, M. P., &Banitalebi-Dehkordi, A. (2022). A survey on adversarial attacks and defenses for object detection and their applications in autonomous vehicles. The Visual Computer, 1-15.