DeepScience
Open Access Books

Chapter 2

Techniques and optimization algorithms in machine learning: A review

Nitin Liladhar Rane [1], Suraj Kumar Mallick [2], Ömer Kaya [3], Jayesh Rane [4]

[1] *Vivekanand Education Society's College of Architecture (VESCOA), Mumbai 400074, India*
[2] *Shaheed Bhagat Singh College, University of Delhi, New Delhi 110017, India*
[3] *Engineering and Architecture Faculty, Erzurum Technical University, Erzurum 25050, Turkey*
[4] *Pillai HOC College of Engineering and Technology, Rasayani, India*
[1] *nitinrane33@gmail.com*

Abstract: Machine learning (ML) has transformed different sectors by allowing for data-based decision-making and forecasting analysis. This study explores the most recent techniques and algorithms that are influencing the direction of machine learning. The research investigates different supervised learning techniques, such as advanced versions of decision trees, support vector machines, and ensemble methods like XGBoost and random forests. Unsupervised learning involves the study of clustering algorithms like k-means++, hierarchical clustering, and density-based spatial clustering of applications with noise (DBSCAN), which are used for anomaly detection and customer segmentation. An overview of convolutional neural networks (CNNs) for image recognition and recurrent neural networks (RNNs) and their advanced form, long short-term memory (LSTM) networks, for time-series analysis and natural language processing address deep learning, a subset of ML. The study highlights the progress of generative adversarial networks (GANs) and transformer models, showcasing notable improvements in generative tasks and language models, respectively. Moreover, the research delves into reinforcement learning, with an emphasis on recent advancements in deep reinforcement learning and how it is utilized in autonomous systems and playing games. Also covered are new developments like federated learning, which tackles data privacy issues by allowing ML models to be trained on decentralized devices, and quantum machine learning, which uses quantum computing to improve algorithm performance. This thorough review is designed to give a complete understanding of modern ML techniques and algorithms, providing insights into their practical use and potential for future innovation in different industries.

Keywords: Artificial intelligence, Machine learning, Deep learning, Techniques, Convolutional neural networks, Recurrent neural networks, Algorithms.

2.1 Introduction

Artificial intelligence (AI) includes machine learning (ML), which has emerged as a game-changing technology with the potential to revolutionise a number of industries, including manufacturing, transportation, healthcare, and finance (Dhiman et al., 2022; SS & Shaji, 2022; Aljabri et al., 2022). Advanced machine learning (ML) approaches and algorithms have grown in popularity and use due to the rapid advancement of computer power and the amount of data (SS & Shaji, 2022; Mahesh, 2020; Kumbure et al., 2022). These developments let robots to learn from data, see patterns, and make judgements with little assistance from humans, ultimately increasing production and efficiency across a range of industries. The rise of data-centric applications in the modern digital age has necessitated the development of powerful machine learning algorithms that can handle complex datasets (Mijwil et al., 2023; Dhall et al., 2020; Tanveer et al., 2020). The ML paradigm relies heavily on techniques like supervised learning, unsupervised learning, and reinforcement learning, each of which offers unique approaches to model training and prediction. Unsupervised learning techniques identify hidden patterns in data without labels, whereas supervised learning algorithms require labelled data to train models to make predictions on fresh data (Syeda et al., 2021; Saha & Manickavasagan, 2021). However, by experimenting with various actions and using rewards and penalties as guidance, models can learn the optimal behaviours through reinforcement learning (Mahesh, 2020; Mijwil et al., 2023; Zhang et al., 2020; Greener et al., 2022). Beyond automation, machine learning's significance lies in its ability to draw insightful conclusions from data and apply those conclusions to make well-informed decisions. ML algorithms play a crucial role in healthcare by aiding in predictive analytics, identifying diseases, and customizing treatment plans (Tanveer et al., 2020; Fatima et al., 2020; Cifuentes et al., 2020; Bhatore et al., 2020). In the financial sector, they aid in identifying fraud, evaluating risk, and conducting algorithmic trading. Additionally, ML methods are crucial in improving customer satisfaction via recommendation systems, natural language processing, and computer vision.

Table 2.1 Different types of ML algorithm

Machine Learning Type	Category	Algorithm
Supervised	Classification	Naive Bayes
Supervised	Classification	Logistic Regression
Supervised	Classification	K-Nearest Neighbor (KNN)
Supervised	Classification	Random Forest
Supervised	Classification	Support Vector Machine (SVM)
Supervised	Classification	Decision Tree

Supervised	Regression	Simple Linear Regression
Supervised	Regression	Multivariate Regression
Supervised	Regression	Lasso Regression
Unsupervised	Clustering	K-Means Clustering
Unsupervised	Clustering	DBSCAN Algorithm
Unsupervised	Clustering	Principal Component Analysis
Unsupervised	Clustering	Independent Component Analysis
Unsupervised	Association	Frequent Pattern Growth
Unsupervised	Association	Apriori Algorithm
Unsupervised	Anomaly Detection	Z-score Algorithm
Unsupervised	Anomaly Detection	Isolation Forest Algorithm
Semi-Supervised	Classification	Self-Training
Semi-Supervised	Regression	Co-Training
Reinforcement	Model-Free	Policy Optimization
Reinforcement	Model-Free	Q-Learning
Reinforcement	Model-Based	Learn the Model
Reinforcement	Model-Based	Given the Model

Table 2.1 classifies different machine learning algorithms according to their learning types and specific categories. The table includes four main types of learning: Supervised Learning, Unsupervised Learning, Semi-Supervised Learning and Reinforcement Learning. This table provides a systematic understanding of various algorithms in the field of machine learning and presents from an academic perspective which learning types and categories these algorithms belong to Bhat et al., (2023); Latif et al., (2023); and Topuz & Alp (2023).

This research seeks to give a thorough explanation of the techniques and algorithms that support ML. We aim to explore the current ML methodology landscape by conducting a thorough review of literature, focusing on their applications, strengths, and limitations. The examination will cover different aspects of ML, such as selecting models, engineering features, and evaluating metrics, providing a comprehensive understanding of the field.

The main contribution of this study include:

- A comprehensive analysis of available literature on machine learning methods and algorithms, offering a critical summary of current understanding and highlighting areas for further research.
- Identifying and examining key terms and how they appear together in literature to reveal common themes and trends in machine learning research.

- An in-depth cluster analysis to classify and illustrate the connections between different ML techniques and algorithms, aiding in a better comprehension of the industry's organization and development.

2.2 Methodology

This research employs a systematic methodology to examine various machine learning techniques and algorithms. A survey of the existing literature served as the fundamental step for the investigation. A thorough search was conducted using a number of scholarly resources, including Google Scholar, IEEE Xplore, SpringerLink, and ScienceDirect. Peer-reviewed literature, conference proceedings, and freshly published review papers were all included in the search parameters. Publications that particularly discuss machine learning algorithms and methodologies were given special attention. The objective of the literature review was to gather a wide variety of perspectives and findings in order to arrive at a thorough understanding of the subject. Following a survey of the literature, the most often used terms and phrases related to machine learning algorithms and methodologies were identified by a keyword analysis. Keywords were identified by analyzing the titles, abstracts, and keywords sections of the chosen papers. This procedure included utilizing text mining tools and software VOSviewer to measure the occurrence and significance of particular terms. The aim was to identify the main themes and ideas that are prevalent in discussions within the field of machine learning research.

The subsequent stage included conducting co-occurrence analysis to explore the connections among keywords in the chosen literature. This analysis uncovers the interconnectedness of different concepts and techniques in machine learning by pinpointing common pairs of keywords in documents. Network analysis software was used to visualize the co-occurrence network, enabling the identification of key clusters and subfields in the machine learning domain. In the end, cluster analysis was carried out to classify the research articles into different groups according to their thematic similarities. Hierarchical clustering techniques were used on the keyword co-occurrence data to accomplish this. The clustering process assisted in identifying distinct areas of emphasis in machine learning research, including supervised learning, unsupervised learning, reinforcement learning, and deep learning. Each group was then examined to comprehend its distinct qualities and impacts on the field.
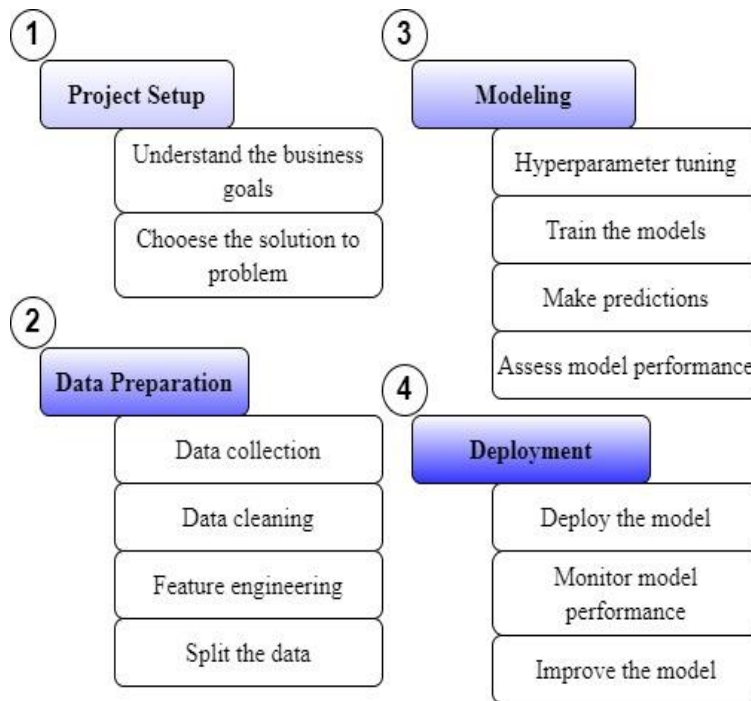
Fig. 2.1 Machine learning workflow

Machine learning (ML) processes require systematic planning and execution of projects and evaluation of results. These processes generally proceed within the framework of certain steps, and each step contributes significantly to the success of the project. Fig. 2.1 shows the machine learning workflow in general.

The machine learning workflow consists of specific steps that must be followed from the beginning to the end of projects. This workflow includes basic stages such as determining the objectives of the project, preparing the data, creating and distributing the models. Each step is critical to the overall success of the project and must be executed with care. This structured approach ensures that machine learning projects are completed efficiently, effectively and consistently.

2.3 Results and discussions

Co-occurrence and cluster analysis of the keywords used in ML techniques

The network diagram (Fig. 2.2) displays a intricate network of terms associated with machine learning methods, demonstrating how they appear together and group together in a significant collection of academic papers. This kind of visualization aids in grasping

the interconnectedness of various concepts in machine learning and their common occurrence in literature. The diagram shows clusters that group together keywords related to each other and appear together often, highlighting specific research areas and themes within the wider field of machine learning. In the diagram's focal point, "machine learning" and "learning systems" are the main nodes, showing their significance in the discussion. The nodes' size indicates they are the terms mentioned most often, serving as central points from which other related terms extend. This importance emphasizes that machine learning is a fundamental concept that different techniques, applications, and related fields are centered around. A prominent group in the chart, highlighted in green, focuses on machine learning applications related to security. Key terms like "cyber security," "network security," "anomaly detection," and "intrusion detection" are significant in this group. This suggests a large amount of research has been conducted on how machine learning can improve security, identify irregularities, and safeguard networks against cyber dangers. The existence of phrases such as "privacy-preserving techniques" and "federated learning" in this group shows continuous endeavors to tackle privacy issues while utilizing machine learning for security objectives.

In addition to this cluster, which emphasises security, there is another significant cluster that focusses on machine learning algorithmic approaches and techniques and is indicated in blue.Words like "decision trees," "adaptive boosting," "random forest," and "feature selection" are important and demonstrate a serious focus on improving machine learning algorithms through research. This group embodies the technical aspects of machine learning, focussing on optimising feature extraction methods, boosting algorithm performance, and increasing predicting accuracy. Machine learning applications in the medical and healthcare domains are highlighted by the red cluster, which also features phrases like "random forest," "prediction," "classification," and "controlled study." The terms "illnesses," "identification," "central nervous system," and "coronavirus" illustrate how frequently machine learning techniques are used in medical research to forecast disease outcomes, examine brain activity, and analyse medical images. This group highlights how machine learning, a field that utilizes computational methods, spans across different disciplines to tackle challenging issues in healthcare and medicine.

Key phrases like "convolutional neural network," "image segmentation," "image processing," and "computer vision" are highlighted by the yellow group, which specialises in image processing and computer vision jobs. This indicates that using deep learning techniques to analyse visual data is highly important. Terms like "convolution" and "feature extraction" suggest that the emphasis is on developing sophisticated models for precisely processing and comprehending images, which is crucial in fields like surveillance, medical imaging, and autonomous driving. The purple-highlighted group is

another important one that focusses on sentiment analysis and natural language processing (NLP). Phrases like "emotion analysis," "NLP," "online education," and "data protection" indicate that machine learning is being used extensively in research to understand and analyse human speech. This grouping emphasizes the significance of NLP methods in different areas such as e-learning platforms, customer feedback sentiment analysis, and privacy-preserving techniques in text data analysis.
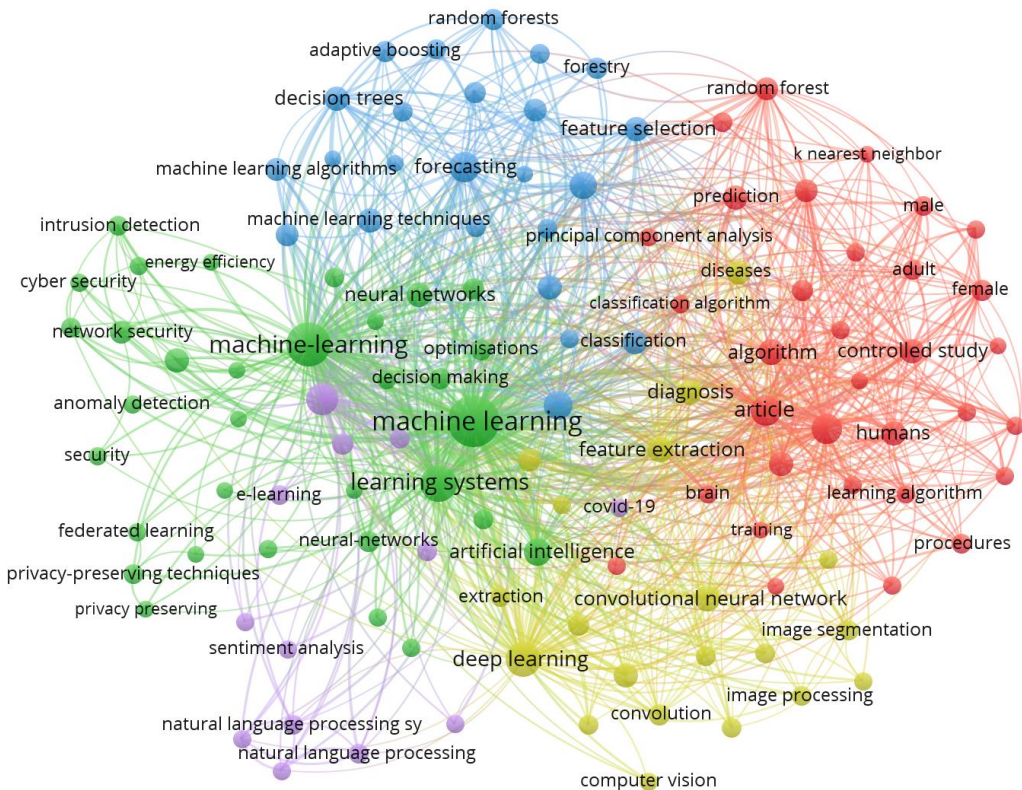

Fig. 2.2 Co-occurrence analysis of the keywords used in ML techniques

The interconnected clusters show the various uses of machine learning across different disciplines. As an example, even though the green cluster emphasizes security, it is connected to the blue cluster, indicating that progress in algorithmic techniques is vital for enhancing security applications. Likewise, the red cluster centered on medical aspects is linked with the yellow cluster emphasizing image processing, demonstrating the intersection of medical imaging and computer vision methods.We can better grasp the latest developments and important fields of research in the field of machine learning thanks to the keywords' simultaneous appearance in both of these categories. For example, "privacy-preserving techniques" are frequently used with terminology related to security and natural language processing (NLP), suggesting that data privacy is becoming more

and more important in a variety of sectors. It is possible, therefore, that future research will continue to focus on developing techniques that combine the benefits of machine learning with the need to protect user privacy. Moreover, the relevance of terms like "deep learning" and "neural networks" across several clusters proves their basic use across a range of machine learning uses. Numerous novel solutions, such as advances in image processing methods, cybersecurity, and medical diagnostics, are based on neural networks and deep learning models.

Advanced machine learning algorithms

There are three main types of machine learning algorithms: supervised, unsupervised, and reinforcement learning (Dhall et al., 2020; Navarro et al., 2021; Houssein et al., 2021; Nwanosike et al., 2022). Sophisticated methods are frequently used in advanced algorithms to combine different types and improve performance and adaptability (Dhall et al., 2020; Tanveer et al., 2020; Gedam & Paul, 2021; Shaukat et al., 2020). These sophisticated algorithms have the ability to analyze and process data with unparalleled precision, proving to be invaluable in various industries like healthcare, finance, and autonomous systems (SS & Shaji, 2022; Dhall et al., 2020; Seo et al., 2020; Hernandez-Matheus et al., 2022; Aliramezani et al., 2022).

Deep Learning and Neural Networks

Neural networks with multiple layers, or "deep" networks, are used in deep learning, a kind of machine learning, to examine complex patterns in data. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are two notable examples. CNNs are particularly good at image and video recognition applications because of their ability to record spatial hierarchies. However, RNNs are particularly good at analysing sequential data, such time series and natural language processing (NLP). Generative Adversarial Networks (GANs) are the latest advances in deep learning. GANs are composed of two neural networks competing to generate real data. Remarkable results have been achieved by GANs in producing high-quality photos, music, and videos. Transformer models, such as BERT and GPT, have transformed natural language processing by allowing for contextually aware comprehension and creation of text.

Reinforcement Learning

Reinforcement learning (RL) involves teaching agents to perform desirable actions in order to assist them in making decision sequences. When a certain outcome is unknown but may be determined by trial, this type of learning is highly advantageous. Reactive learning (RL) has inspired the development of sophisticated AI systems for games,

robotics, and autonomous vehicles. Recent advances in reinforcement learning combine deep learning to create Deep Reinforcement Learning (DRL). Proximal Policy Optimisation (PPO) and Deep Q-Networks (DQN) are two techniques that have demonstrated significant progress in handling difficult jobs. Robust trading systems and robotic control, as well as advancements in gaming such as AlphaGo, have been made possible by DRL's ability to learn from large amounts of data, including video frames.

Transfer Learning

Transfer learning is building a model for a different task using an existing model for the first task as a basis. This strategy, which builds on the knowledge from the first task to improve outcomes, is extremely helpful when there is little data available for the second task. The advent of pre-trained models, such ImageNet for computer vision and BERT for natural language processing, has propelled the growth of transfer learning. These models are designed to reduce training time and resource requirements while maintaining high performance, as they have been fine-tuned for specific tasks after being trained on large datasets.

Explainable AI (XAI)

The more complicated machine learning models get, the more crucial it is to comprehend their decision-making processes, especially in delicate industries like finance and healthcare. The goal of explainable AI (XAI) is to make AI systems more understandable and comprehensible for people. The most advanced techniques for explaining how models predict results are SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-agnostic Explanations). The move towards XAI is being driven by regulatory requirements as well as the need for trust and accountability in AI systems. Ensuring the interpretability of AI models is crucial for assisting stakeholders in ensuring equity, impartiality, and compliance with moral principles.

Federated Learning

A sophisticated technique called federated learning uses multiple decentralised devices or servers, each with local data samples, to train a global model. By storing data on separate devices and only exchanging model changes, this technique protects data security and privacy. In industries where protecting data privacy is crucial, like healthcare and mobile apps, the use of federated learning is growing. Federated learning is used by Apple's Siri and Google's Gboard to improve user experience while maintaining data security. This approach is also gaining popularity in cooperative research with different organisations.
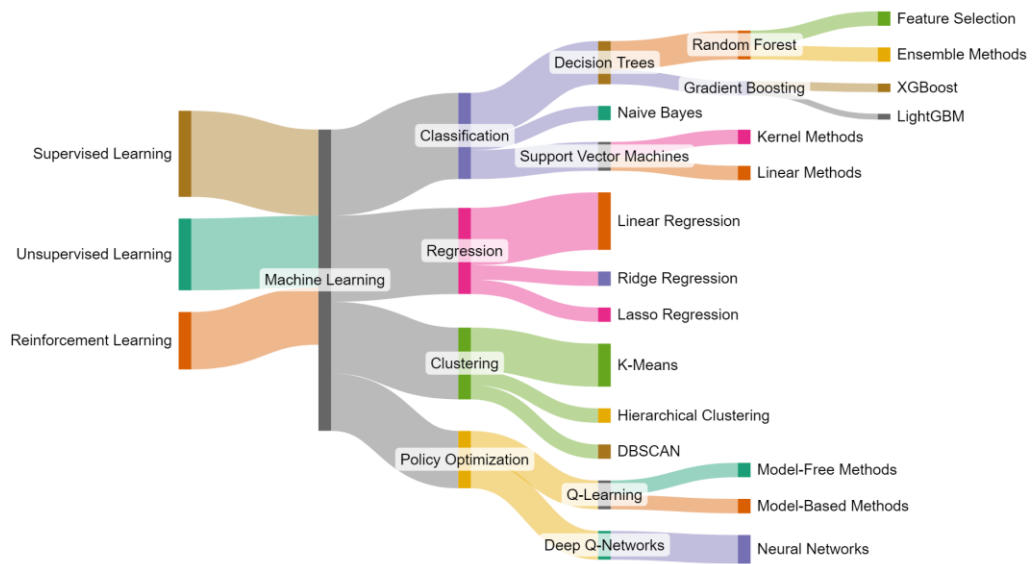
Fig. 2.3 Sankey diagram of advanced ML algorithms

Self-Supervised Learning

In the emerging field of self-supervised learning, an algorithm generates a self-monitoring signal by analysing the incoming data. This method reduces the need for large annotated datasets, which are usually expensive and time-consuming to create. In self-supervised learning, techniques like Contrastive Learning and Masked Language Modelling (seen in models like BERT) are setting the standard. These methods, which build robust representations from unannotated data, have produced remarkable results in computer vision and natural language processing, setting new benchmarks.

AutoML and Neural Architecture Search (NAS)

The method of creating models is being revolutionised by AutoML and NAS. AutoML handles every step of the machine learning implementation process, from selecting the right model to adjusting hyperparameters, all in a more efficient manner. Conversely, the main focus of NAS is to automate the construction of neural network architectures. These developments are levelling the playing field for AI, making it accessible to those without specialised knowledge, and significantly accelerating the creation process. Leading platforms in this industry include open-source tools like NASNet and AutoKeras, as well as platforms like Google AutoML.

Graph Neural Networks (GNNs)

Graph-structured data, which is frequently present in social networks, recommendation systems, and molecular biology, is the target application for GNNs. Because GNNs are able to capture the relationships and interactions between nodes, they are useful for tasks like node classification, link prediction, and graph classification. Graph Convolutional Networks (GCNs) and Graph Attention Networks (GATs) are recent additions to the GNN family that enhance its ability to process complex graph data. These models are being actively researched and used for a variety of purposes, from fraud detection to medication discovery.

Quantum Machine Learning

The exciting field of quantum machine learning is created when machine learning and quantum computing combine. Because quantum computers can compute exponentially faster than classical computers, they have the potential to solve hard machine learning issues that are now unsolvable. Researchers are looking into quantum versions of classical algorithms, such as quantum neural networks and quantum support vector machines. Quantum machine learning, though still in its infancy, has the potential to revolutionise fields that require large amounts of computational power, such as materials science, encryption, and optimisation problems.

The depiction of advanced machine learning algorithms on the Sankey diagram (Fig. 2.3) shows the movement and connections between different ML methods and individual algorithms. The classification of ML starts by dividing it into three primary categories: Supervised Learning, Unsupervised Learning, and Reinforcement Learning. Supervised Learning can be divided into Classification and Regression, which are important for making predictions using labeled data. Classification can be broken down into Decision Trees, Support Vector Machines (SVM), and Naive Bayes. Decision Trees can be divided into subcategories such as Random Forest and Gradient Boosting, while SVM includes Kernel and Linear Methods. Regression is divided into Linear Regression, Ridge Regression, and Lasso Regression, demonstrating different methods for modeling connections between variables. Unsupervised Learning leads to Clustering, a technique for organizing data points without predefined tags. Clustering divides into K-Means, Hierarchical Clustering, and DBSCAN, each showcasing distinct methods for recognizing natural clusters in data. Policy optimization is a result of reinforcement learning and involves methods such as Q-Learning and Deep Q-Networks. Q-Learning can be further divided into two categories: Model-Free and Model-Based Methods, which highlight the difference between algorithms that directly learn policies and those that create a model of the environment. Deep Q-Networks demonstrate how deep learning can be applied in reinforcement tasks by connecting directly to Neural Networks.

Emerging techniques in machine learning

Self-supervised learning (SSL) is among the most revolutionary new methods in the field of machine learning (Al-Shaaby et al., 2020; Bertolini et al., 2021; Mishra, 2021). In contrast to conventional supervised learning, SSL uses a significant amount of unlabeled data instead of labeled data to develop valuable representations (Albahri et al., 2020; Musa et al., 2020; Hooda et al., 2022). This method is especially beneficial considering the limited availability and high expense of annotated datasets. SSL has demonstrated impressive achievements in the fields of natural language processing (NLP) and computer vision. For example, BERT and GPT, both built on SSL, have achieved new standards in NLP tasks like translating languages, analyzing sentiments, and generating text. In the field of computer vision, methods such as contrastive learning within semi-supervised learning have enhanced the performance of image recognition and classification algorithms by allowing them to extract features from large quantities of unlabelled images.

Few-shot learning is a developing method that is becoming more popular (Kumbure et al., 2022; Mijwil et al., 2023; Dhall et al., 2020; Cifuentes et al., 2020). This technique tackles the issue of training models when data is scarce. Few-shot learning models are able to extrapolate information from a limited amount of instances, making them extremely beneficial in situations where gathering data is challenging or costly. This method is especially useful in medical analysis, as it can be difficult to acquire extensive labeled datasets. Few-shot learning models are capable of recognizing diseases with only a small number of labeled medical images, which helps speed up the implementation of AI in the healthcare industry. Within the domain of neural network structures, transformers have completely transformed the way models manage sequential data. Initially developed for NLP duties, transformers have surpassed conventional RNN and CNN in diverse uses. Transformers' significant advancement lies in their self-attention mechanism, enabling models to dynamically assess the significance of various parts of the input data. This has resulted in advancements not just in NLP, but also in areas such as protein folding, utilizing transformers to forecast the 3D configuration of proteins, assisting in drug development and comprehending biological functions.

Graph neural networks (GNNs) are gaining traction as effective resources for understanding information from graph-based data (Aliramezani et al., 2022; Al-Shaaby et al., 2020; Bertolini et al., 2021; Hooda et al., 2022). GNNs are highly effective in tasks where connections between entities are essential, like social network analysis, recommendation systems, and molecular chemistry. GNNs can make more precise and informative predictions by representing data in graph form, which allows them to capture intricate relationships and connections. In drug discovery, GNNs predict molecular

properties and interactions to help identify possible drug candidates. Federated learning is tackling privacy issues in the field of machine learning. Conventional machine learning models need data to be stored in a centralized manner, leading to concerns about privacy and security. On the contrary, federated learning enables training models on multiple decentralized devices without the need to share raw data. This method is especially important for use in fields that deal with confidential data, like healthcare and finance. Through keeping data in specific locations, federated learning improves privacy and still benefits from collective learning across varied data sources. Google's use of federated learning in the Gboard app, where the model learns from user typing behavior without sending the data to central servers, demonstrates its real-world use.

The field of explainable AI, or XAI, is becoming more and more important (SS & Shaji, 2022; Aljabri et al., 2022; Mahesh, 2020; Aliramezani et al., 2022). It gets more difficult to understand and justify the decisions made by machine learning models as their complexity rises (Bertolini et al., 2021; Mishra, 2021; Albahri et al., 2020). The objective of XAI approaches is to improve the interpretability and transparency of models so that users can trust AI systems and use them effectively. Methods like SHAP and LIME highlight the characteristics that influence decisions by revealing the elements influencing model predictions. For reasons of responsibility and trust, it is particularly critical to understand the logic underlying AI-generated decisions in sectors like healthcare and finance. Within machine learning, there is another method known as "learning to learn," or meta-learning. Meta-learning algorithms use prior information and experience to improve the efficacy and efficiency of learning processes. This technique is particularly useful in environments where activities are added or changed often. Thanks to meta-learning, robots in robotics may quickly adapt to new tasks with little training, increasing their usefulness and adaptability. An advanced technique for automating the construction of neural network architectures is called neural architecture search, or NAS. The traditional method of creating models is based on human experience and knowledge, which can be laborious and inefficient. NAS employs algorithms to investigate and enhance neural network architectures, resulting in the identification of superior and more effective models. This method has resulted in the creation of cutting-edge models that surpass manually created structures in different benchmarks, from image recognition to language processing.

Reward learning (RL) is still evolving as a result of deep reinforcement learning (DRL) advancements (SS & Shaji, 2022; Aljabri et al., 2022; Mahesh, 2020; Houssein et al., 2021). Through experimentation, DRL combines the principles of reinforcement learning with deep neural networks to enable agents to learn complex abilities. Impressive outcomes have been demonstrated by this technique in autonomous systems, robotics, and

games. Proximal Policy Optimisation (PPO) and Soft Actor-Critic (SAC) algorithms have improved DRL's stability and efficacy, opening up more practical and extensible applications. DRL has been instrumental in training agents to be proficient in complex games like Dota 2. Significant progress has also been made in the development of GAN. GANs are made up of a pair of neural networks - one generator and one discriminator - which compete in generating authentic data samples. This method has transformed fields such as image creation, data enhancement, and aesthetic transformation. Recent advancements in GANs, like StyleGAN and BigGAN, have generated incredibly lifelike visuals, expanding the limits of creative and visual possibilities. Researchers are also investigating the usage of GANs for creating artificial data to enhance training sets, solving problems related to lack of data and prejudice. Quantum machine learning (QML) is a developing area that merges quantum computing with machine learning. QML algorithms harness quantum mechanics principles to handle information in ways that classical computers are unable to, which could result in significant speed increases for specific tasks. Even though QML is still in its early stages, it shows potential for addressing challenging optimization issues, modeling quantum systems, and improving cryptographic protocols. Scientists are currently conducting research to investigate the capabilities of quantum algorithms in speeding up machine learning processes. Initial tests have indicated promising results particularly in quantum support vector machines and quantum neural networks.

Optimization algorithms in machine learning

Optimization algorithms play a crucial role in machine learning by facilitating the efficient and successful training of models (Tanveer et al., 2020; Syeda et al., 2021; Albreiki et al., 2021; Saha & Manickavasagan, 2021; Albahri et al., 2020). These algorithms are created to reduce or increase a particular objective function by modifying the model's parameters (Aljabri et al., 2022; Mahesh, 2020; Tanveer et al., 2020; Cifuentes et al., 2020). In machine learning, optimization usually consists of reducing the error or loss function, which evaluates the discrepancy between predicted and actual outputs (Fatima et al., 2020; Cifuentes et al., 2020; Bhatore et al., 2020; Navarro et al., 2021). As the field progresses, new optimization algorithms and techniques keep appearing, tackling different obstacles and enhancing the efficiency of machine learning models.

Gradient-Based Optimization

The basis of machine learning remains gradient-based optimisation approaches. Reducing the loss in one direction while increasing the gain in another relies on estimating the gradient of the loss function with respect to the model parameters. Because of its

simplicity and efficiency, stochastic gradient descent (SGD) and its variants are widely used. Compared to using the entire dataset, SGD drastically reduces the computing cost by updating the model's parameters using a mini-batch of data. The focus of recent developments has been on increasing the stability and rate of convergence of gradient-based approaches. The Adam algorithm—also referred to as Adaptive Moment Estimation—has gained a lot of traction. It merges the advantages of AdaGrad and RMSProp by calculating personalized learning rates for individual parameters. Adam is suitable for problems with sparse gradients and non-stationary objectives, as it utilizes estimates of first and second moments of the gradients. Its strength and effectiveness have caused it to become the standard selection in numerous deep learning platforms.

Second-Order Methods

Second-order approaches use the Hessian matrix information to capture the curvature of the loss function, in contrast to first-order methods that use gradients, like SGD. A well-known second-order optimisation strategy that converges faster than first-order methods, especially when it comes close to the optimum, is Newton's Method. However, for large problems, the Hessian matrix computation and storage may be prohibitively expensive. Quasi-Newton Methods, such as the Broyden-Fletcher-Goldfarb-Shanno (BFGS) algorithm, estimate the Hessian matrix rather than compute it directly in order to address this problem. L-BFGS is a scalable version that may be applied to high-dimensional optimisation issues because it only requires a minimal number of vectors to approximate the Hessian.

Optimization in Deep Learning

Particularly deep neural networks pose unique optimisation challenges due to their complex loss landscapes, multiple local minima, and saddle points. Learning Rate Schedulers are becoming essential for deep network optimisation. Techniques like Cosine Annealing and Cyclical Learning Rates modify the learning rate during training to help the model avoid local minima and arrive at better solutions. The optimisation of deep learning has been transformed by the technique known as batch normalisation. By normalising each layer's input, batch normalisation reduces internal covariate shift, which helps to stabilise and accelerate training. It lessens reliance on the original parameter values and permits faster learning rates.

Evolutionary Algorithms

Natural selection and genetic evolution serve as models for evolutionary algorithms (EAs). Because they can explore a large range of solutions and avoid becoming stuck at local minimum points, these population-based algorithms have gained popularity in the

field of machine learning. Two prominent examples of well-known techniques in the field are Particle Swarm Optimisation (PSO) and Genetic Algorithms (GAs). Neural architecture searches and hyperparameter optimisation are two areas where EAs excel. One such method is the NeuroEvolution of Augmenting Topologies (NEAT) program, which finds novel, efficient configurations without human intervention by evolving the weights and structures of neural networks. These algorithms can be used with other optimisation strategies to get better performance, and they have a strong potential for parallelisation.

Bayesian Optimization

Based on probabilistic models, Bayesian optimisation is an effective technique for optimising black-box functions, which are challenging to evaluate because of their high cost and lack of gradient data. In order to estimate the objective function, it builds a surrogate model, typically a Gaussian process, and uses it to identify the location of the subsequent sampling. This method works particularly well for fine-tuning machine learning model hyperparameters. Bayesian optimisation, as opposed to grid or random search, finds the optimal hyperparameters with fewer evaluations by focussing on promising regions inside the search space. Its capacity and effectiveness have been improved recently, making it suitable for challenging optimisation issues with lots of noise and large dimensions.

Gradient-Free Optimization

Gradient-free optimisation techniques offer useful choices in scenarios when gradient information is either unavailable or unreliable. Traditional examples include Nelder-Mead Simplex and Simulated Annealing (SA). These strategies can handle noisy and non-differentiable objective functions, albeit at a lower efficiency than gradient-based methods. Recent research has looked into the use of methods for Zero-Order Optimisation, in which function evaluations are the only source of information used to determine gradients. Techniques like Derivative-Free Optimisation (DFO) and Random Search with Learning Automata (RSLA) have shown promise in high-dimensional function optimisation without the need for gradient data.

Advances in Regularization Techniques

In optimisation, regulation techniques are crucial because they prevent overfitting and improve generalisation. In order to encourage sparsity and reduce complexity, L1 and L2 regularisation are frequently used to apply penalties to the loss function based on the size of the model parameters. As a kind of regularisation known as "dropout," units in a neural network are randomly removed during training in order to promote the network's learning

of a variety of representations and increase its stability. Two new innovations are Shake-Shake Regularisation, which introduces randomness in both the forward and backward passes to increase regularisation, and DropConnect, which randomly removes connections rather than units.

Optimization in Reinforcement Learning

Because finding a balance between exploration and exploitation and the sequential nature of decision-making present unique optimisation challenges for reinforcement learning (RL). Policy gradient methods compute gradients of the predicted reward in order to optimise the policy. Nowadays, RL's top techniques include Proximal Policy Optimisation (PPO) and Trust Region Policy Optimisation (TRPO), which offer improved stability and efficiency over traditional methods. To obtain optimal strategies, Q-Learning and its enhanced form, Deep Q-Networks (DQN), improve the action-value function. More recently, techniques like Double DQN and Duelling DQN have improved the stability and performance of Q-learning algorithms by addressing issues like overestimation bias.

Optimization for Federated Learning

Federated learning is a novel approach to training models collaboratively across several devices while maintaining data privacy. The optimisation of federated learning is further complicated by disparate data distributions and limited communication capabilities. A popular approach called FedAvg averages the model parameters over time while doing local updates on each device. The focus of current research has been on adopting adaptive learning rates and reducing communication overhead through the use of techniques like Federated Stochastic Variance Reduction (FedSVRG) in order to improve the efficiency and convergence of federated learning algorithms.

2.4 Conclusions

Research into methods and algorithms in machine learning has demonstrated the quick progression and extensive use of these technologies in different sectors. One of the most significant trends is the emergence of deep learning algorithms, specifically CNN and RNN, which have transformed areas like image recognition, natural language processing, and speech synthesis. These progressions have been made possible due to the presence of vast amounts of data and the rapid increase in computing capabilities, allowing for more intricate models to be efficiently trained. Another important advancement involves combining reinforcement learning and unsupervised learning methodologies. Reinforcement learning, such as Deep Q-Networks (DQNs) and Proximal Policy

Optimization (PPO), has demonstrated impressive achievements in domains that involve sequential decision-making, such as robotics and autonomous driving. Unsupervised learning, utilizing methods such as GAN and self-organizing maps, has expanded the possibilities for exploring data and recognizing patterns without the need for labeled data, making machine learning more widely applicable.

Moreover, the emphasis on clarity and understanding of machine learning models has become more important. XAI methods are being created to enhance the transparency of complex models' decision-making processes, aiming to improve trust and reliability in important fields like healthcare and finance. This pattern is essential for tackling moral issues and following rules and regulations. Furthermore, the way data privacy is upheld is being transformed by the adoption of federated learning. Federated learning enables models to be trained on decentralized devices without transferring raw data, safeguarding user privacy and tapping into collective knowledge. This method is especially important in delicate areas such as medical studies and individual finances. The ongoing integration of cutting-edge algorithms and approaches offers the potential to discover new opportunities, fueling progress and advancement in this ever-evolving industry.

References

Albahri, A. S., Hamid, R. A., Alwan, J. K., Al-Qays, Z. T., Zaidan, A. A., Zaidan, B. B., ... & Madhloom, H. T. (2020). Role of biological data mining and machine learning techniques in detecting and diagnosing the novel coronavirus (COVID-19): a systematic review. Journal of medical systems, 44, 1-11.

Albreiki, B., Zaki, N., & Alashwal, H. (2021). A systematic literature review of student'performance prediction using machine learning techniques. Education Sciences, 11(9), 552.

Aliramezani, M., Koch, C. R., & Shahbakhti, M. (2022). Modeling, diagnostics, optimization, and control of internal combustion engines via modern machine learning techniques: A review and future directions. Progress in Energy and Combustion Science, 88, 100967.

Aljabri, M., Altamimi, H. S., Albelali, S. A., Al-Harbi, M., Alhuraib, H. T., Alotaibi, N. K., ... & Salah, K. (2022). Detecting malicious URLs using machine learning techniques: review and research directions. IEEE Access, 10, 121395-121417.

Al-Shaaby, A., Aljamaan, H., & Alshayeb, M. (2020). Bad smell detection using machine learning techniques: a systematic literature review. Arabian Journal for Science and Engineering, 45(4), 2341-2369.

Bertolini, M., Mezzogori, D., Neroni, M., & Zammori, F. (2021). Machine Learning for industrial applications: A comprehensive literature review. Expert Systems with Applications, 175, 114820.

Bhat, P., Behal, S., & Dutta, K. (2023). Machine learning and deep learning techniques for detecting malicious android applications: An empirical analysis. Proceedings of the Indian National Science Academy, 89(3), 429-444.

Bhatore, S., Mohan, L., & Reddy, Y. R. (2020). Machine learning techniques for credit risk evaluation: a systematic literature review. Journal of Banking and Financial Technology, 4(1), 111-138.

Cifuentes, J., Marulanda, G., Bello, A., & Reneses, J. (2020). Air temperature forecasting using machine learning techniques: a review. Energies, 13(16), 4215.

Dhall, D., Kaur, R., & Juneja, M. (2020). Machine learning: a review of the algorithms and its applications. Proceedings of ICRIC 2019: Recent innovations in computing, 47-63.

Dhiman, B., Kumar, Y., & Kumar, M. (2022). Fruit quality evaluation using machine learning techniques: review, motivation and future perspectives. Multimedia Tools and Applications, 81(12), 16255-16277.

Fatima, N., Liu, L., Hong, S., & Ahmed, H. (2020). Prediction of breast cancer, comparative review of machine learning techniques, and their analysis. IEEE Access, 8, 150360-150376.

Gedam, S., & Paul, S. (2021). A review on mental stress detection using wearable sensors and machine learning techniques. IEEE Access, 9, 84045-84066.

Greener, J. G., Kandathil, S. M., Moffat, L., & Jones, D. T. (2022). A guide to machine learning for biologists. Nature reviews Molecular cell biology, 23(1), 40-55.

Hernandez-Matheus, A., Löschenbrand, M., Berg, K., Fuchs, I., Aragüés-Peñalba, M., Bullich-Massagué, E., & Sumper, A. (2022). A systematic review of machine learning techniques related to local energy communities. Renewable and Sustainable Energy Reviews, 170, 112651.

Hooda, R., Joshi, V., & Shah, M. (2022). A comprehensive review of approaches to detect fatigue using machine learning techniques. Chronic Diseases and Translational Medicine, 8(1), 26-35.

Houssein, E. H., Emam, M. M., Ali, A. A., & Suganthan, P. N. (2021). Deep and machine learning techniques for medical imaging-based breast cancer: A comprehensive review. Expert Systems with Applications, 167, 114161.

Kumbure, M. M., Lohrmann, C., Luukka, P., & Porras, J. (2022). Machine learning techniques and data for stock market forecasting: A literature review. Expert Systems with Applications, 197, 116659.

Latif, S. D., & Ahmed, A. N. (2023). A review of deep learning and machine learning techniques for hydrological inflow forecasting. Environment, Development and Sustainability, 25(11), 12189-12216.

Mahesh, B. (2020). Machine learning algorithms-a review. International Journal of Science and Research (IJSR).(Internet), 9(1), 381-386.

Mijwil, M., Salem, I. E., & Ismaeel, M. M. (2023). The significance of machine learning and deep learning techniques in cybersecurity: A comprehensive review. Iraqi Journal For Computer Science and Mathematics, 4(1), 87-101.

Mishra, M. (2021). Machine learning techniques for structural health monitoring of heritage buildings: A state-of-the-art review and case studies. Journal of Cultural Heritage, 47, 227-245.

Musa, U. S., Chhabra, M., Ali, A., & Kaur, M. (2020). Intrusion detection system using machine learning techniques: A review. In 2020 international conference on smart electronics and communication (ICOSEC) (pp. 149-155). IEEE.

Navarro, C. L. A., Damen, J. A., Takada, T., Nijman, S. W., Dhiman, P., Ma, J., ... & Hooft, L. (2021). Risk of bias in studies on prediction models developed using supervised machine learning techniques: systematic review. bmj, 375.

Nwanosike, E. M., Conway, B. R., Merchant, H. A., & Hasan, S. S. (2022). Potential applications and performance of machine learning techniques and algorithms in clinical practice: a systematic review. International journal of medical informatics, 159, 104679.

Saha, D., & Manickavasagan, A. (2021). Machine learning techniques for analysis of hyperspectral images to determine quality of food products: A review. Current Research in Food Science, 4, 28-44.

Seo, H., Badiei Khuzani, M., Vasudevan, V., Huang, C., Ren, H., Xiao, R., ... & Xing, L. (2020). Machine learning techniques for biomedical image segmentation: an overview of technical aspects and introduction to state-of-art applications. Medical physics, 47(5), e148-e167.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, 13(10), 2509.

SS, V. C., & Shaji, E. (2022). Landslide identification using machine learning techniques: Review, motivation, and future prospects. Earth science informatics, 15(4), 2063-2090.

Syeda, H. B., Syed, M., Sexton, K. W., Syed, S., Begum, S., Syed, F., ... & Yu Jr, F. (2021). Role of machine learning techniques to tackle the COVID-19 crisis: systematic review. JMIR medical informatics, 9(1), e23811.

Tanveer, M., Richhariya, B., Khan, R. U., Rashid, A. H., Khanna, P., Prasad, M., & Lin, C. T. (2020). Machine learning techniques for the diagnosis of Alzheimer's disease: A review. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 16(1s), 1-35.

Topuz, B., & Alp, N. Ç. (2023). Machine learning in architecture. Automation in Construction, 154, 105012.

Zhang, J., Yin, Z., Chen, P., & Nichele, S. (2020). Emotion recognition using multi-modal data and machine learning techniques: A tutorial and review. Information Fusion, 59, 103-126.