**Overview :Machine Learning**

Vaishali Jain Shiv Kumar Tiwari

Lecturer Computer Asst. Prof. CSE

Women’s Poly. Jbp GGCT ,Jbp

vaishaliharshi@gmail.com sshiv.tiwari22@gmail.com

In the area of machine learning, which is a branch of artificial intelligence, algorithms are created to let computers learn implicitly from data. It includes analysing data, finding patterns, and then making predictions or judgements based on that analysis using statistical models and algorithms. As they are exposed to more data, machine learning algorithms may perform better and better, which enables them to automatically adapt and advance over time. Numerous applications, including speech and image identification, natural language processing, recommendation engines, and predictive analytics, heavily rely on machine learning.

“Machine learning is the science (and art) of programming computers so they can learn from data,”



Figure-1(Machine Learning)

I. Machine learning has many applications across various industries and domains, some of which include:

a. Image and speech recognition

b .Natural language processing

c. Predictive maintenance

d. Fraud detection

e. Customer segmentation and personalization

f. Stock market prediction

g. Healthcare diagnosis and treatment recommendation

h. Recommender systems

i. Predictive modeling for climate change and weather forecasting

j. Self-driving cars and autonomous vehicles.

These are only a handful of the numerous potential uses for machine learning. The particular use cases will differ based on the data and issue being addressed, the project's objectives, and the resources available. Machine learning is generally used to create predictions and suggestions, automate operations that would otherwise need to be done by people, and optimise procedures and systems.

**II.Steps of Machine Learning:**

a. Problem Definition: Define the problem you want to solve and determine the target variable.

b. Data Collection: Gather relevant data to solve the problem.

c. Data Exploration: Analyze and understand the data, including cleaning and transforming it if necessary.

d. Model Selection: Choose the appropriate model based on the problem and data.

e. Model Training: Train the model using the data.

f. Model Evaluation: Evaluate the model using appropriate metrics to determine its performance.

g. Model Deployment: Deploy the model in a production environment, integrating it with other systems if necessary.

The 7 steps of machine learning are a systematic approach to building predictive models. Firstly, the problem needs to be defined and the target variable identified. This is followed by data collection, where relevant data is gathered to solve the problem. After that, data exploration is carried out to analyze and understand the data, including cleaning and transforming it if necessary. The next step is model selection, where an appropriate model is chosen based on the problem and data. The model is then trained using the data. Following training, the model is evaluated using appropriate metrics to determine its performance. Finally, the model is deployed in a production environment and integrated with other systems if necessary. These steps ensure that machine learning models are built in a structured and repeatable manner, which leads to better results and reduces the risk of failure.



Figure-2(Steps of Machine Learning)

**III.Types of Machine Learning:**

**a. Supervised Learning:**This type of machine learning involves training a model on labeled data, where the target variable is known. The model makes predictions based on the relationships between the features and target variable.

**b. Unsupervised Learning:** This type of machine learning involves training a model on unlabeled data, where the target variable is unknown. The model discovers patterns and relationships in the data without being guided by a specific outcome.

**c. Reinforcement Learning:** This type of machine learning involves training a model to make decisions in an environment by receiving rewards or punishments based on its actions. The model learns over time to maximize its rewards.

**d. Semi-Supervised Learning:** This type of machine learning combines both supervised and unsupervised learning. It involves training a model on a combination of labeled and unlabeled data, where the model can leverage the relationships learned from the unlabeled data to make better predictions on the labeled data.

**e. Transfer Learning:** This type of machine learning involves using a pre-trained model as a starting point and fine-tuning it for a new task, rather than training a model from scratch. This can save time and resources and improve model performance.

**III.(a)Supervised Machine Learning:**

The model is trained using labelled data when the goal variable is known, which is referred to as supervised machine learning. Building a model that can predict values for the target variable based on correlations between features and the target variable is the aim of supervised learning.

In supervised learning, input data (features) and matching output data (labels) are provided to the model. The input and output data relationships are taught to the model through training. Once trained, the model may utilise the associations it discovered during training to generate predictions on new, unforeseen data.

Applications for supervised learning include sentiment analysis, fraud detection, and picture categorization. The exact problem being solved and the properties of the data will determine the model that is utilised for supervised learning. Support vector machines, decision trees, and linear regression are often used models in supervised learning.

Supervised learning is a powerful tool for making predictions by learning relationships between features and target variables in labeled data.

**(a.1)Usage of Supervised Machine Learning:**

**Image Classification:** Supervised machine learning can be used to classify images into different categories, such as animals, objects, or scenes.

**Sentiment Analysis:** Supervised machine learning can be used to analyze the sentiment of text data, such as product reviews or social media posts, to determine if they are positive, negative, or neutral.

**Fraud Detection:** Supervised machine learning can be used to detect fraudulent transactions by learning patterns in the data and flagging transactions that deviate from those patterns.

**Predictive Maintenance:** Supervised machine learning can be used to predict when equipment will fail, allowing maintenance to be performed before a failure occurs.

**Customer Segmentation**: Supervised machine learning can be used to segment customers into different groups based on their purchasing behavior, allowing for targeted marketing campaigns.

**Sales Forecasting:** Supervised machine learning can be used to forecast future sales based on historical sales data and other relevant features.

**Recommendation Systems:** Supervised machine learning can be used to recommend products or content to users based on their past behavior.

**Healthcare:** Supervised machine learning can be used to predict patient outcomes, diagnose diseases, and personalize treatment plans.

**(a.2)Types of Supervised Machine Learning**:

**a. Regression:** A continuous goal variable, like the price of a stock or the weather tomorrow, may be predicted using this kind of supervised learning. For instance, a house's price may be predicted using a linear regression model based on the home's size, location, and other characteristics.

**b. Classification:** This type of supervised learning is used for predicting a categorical target variable, such as whether a customer will buy a product or not. For example, a logistic regression model could be used to classify whether an email is spam or not.

**c. Logistic Regression:** When there are only two potential values for the target variable, binary classification issues are solved using this kind of supervised learning. A logistic regression model, for instance, may be utilised to determine if a patient has an illness or not.

**d. Decision Trees:** With the help of a succession of decisions depending on the attributes, this kind of supervised learning creates a model that resembles a tree and predicts the target variable. A decision tree model, for instance, may be used to forecast the sort of loan a consumer is most likely to pick.

**e. Random Forest:** An ensemble of decision trees, which is a supervised learning technique, is trained and assembled to provide predictions. To determine whether a consumer would leave or stay, for instance, a random forest model might be applied.

**f. Support Vector Machines (SVM):** This kind of supervised learning divides the data into classes using a boundary known as a hyper plane. An SVM model, for instance, may be used to categories pictures of handwritten numbers.

**g. Naive Bayes:** The Bayes theorem is used in this kind of supervised learning to produce predictions about the likelihood of a target variable given the attributes. A Naive Bayes model, for instance, might be used to foretell whether a movie review would be good or negative.

**h. Neural Networks:** Artificial neural networks are used in this kind of supervised learning to simulate intricate interactions between the features and the goal variable. For instance, stock price predictions might be made using a neural network model.



Figure-4(Supervised Machine Learning)

**III.(b)Unsupervised Machine Learning:**

Clustering and dimensionality reduction are the two basic categories into which unsupervised learning methods fall. While dimensionality reduction methods seek to minimize the amount of characteristics in the data while maintaining its structure, clustering algorithms seek to group comparable data points together.

Principal component analysis, hierarchical clustering, and k-means clustering are a few examples of unsupervised learning techniques. Applications for these algorithms include consumer segmentation, anomaly detection, and data visualization.

There are no right or wrong answers in unsupervised learning, and the model's utility in a given domain and the interpretability of the findings are frequently used to judge the model's quality. Unsupervised learning, however, might be more difficult than supervised learning since the model is not directed by a defined outcome, and it is more complicated to assess the model's success.

Unsupervised learning is a valuable tool in the machine learning toolbox and has numerous practical uses in spite of these difficulties. It offers important insights into the data's underlying structure and may result in the identification of fresh patterns and connections.

**(b.1)Usage of Unsupervised Machine Learning:**

**Customer Segmentation:** Grouping customers into segments based on their behavior, preferences, and purchasing habits.

**Anomaly Detection:** Detecting unusual or unexpected behavior in a data set, such as fraud detection or network intrusion.

**Data Visualization:** Reducing the dimensionality of a data set for easy visualization and interpretation.

**Recommender Systems:** Recommend products or items to users based on their past behavior and preferences.

**Image and Speech Processing:** Clustering images or speech segments to identify patterns and relationships.

**Natural Language Processing:** Grouping words into topics and identifying relationships between words.

**Fraud Detection:** Identifying unusual patterns or behavior in financial transactions that may indicate fraud.

**Text Clustering**: Grouping documents into categories based on their content.

**Image Compression:** Reducing the size of an image while preserving its features and structure.

**Gene Expression Analysis**: Identifying patterns and relationships in gene expression data for biological research.

**(b.2)Types of Unsupervised Machine Learning**:

**a. Clustering:** This type of unsupervised machine learning is used to group similar data points into clusters. For example, grouping customers into segments based on their purchasing habits.

**b. Dimensionality Reduction:** This type of unsupervised machine learning is used to reduce the number of features in a data set while preserving its structure. For example, reducing the number of variables in a high-dimensional data set for visualization or further analysis.

**c. Anomaly Detection:** This type of unsupervised machine learning is used to identify unusual or unexpected patterns in a data set. For example, detecting fraud in financial transactions.

**d. Association Rule Learning:** This type of unsupervised machine learning is used to find relationships between variables in a data set. For example, identifying items that are frequently purchased together in a grocery store.

**e. Auto encoders:** This type of unsupervised machine learning is used to learn a compact representation of a data set. For example, reducing the size of an image while preserving its features and structure.

**f. Generative Adversarial Networks (GANs):** This type of unsupervised machine learning is used to generate new data samples that are similar to a training data set. For example, generating realistic images of faces.



Figure-5(Unsupervised Machine Learning)

**III.(c)Reinforcement Machine Learning:**

An artificial intelligence technique known as reinforcement machine learning focuses on teaching models to make decisions in a given environment by getting rewards or penalties based on their behavior. The objective is to develop a policy—a mapping from states to actions—that over time maximizes a reward signal.

In reinforcement learning, an agent engages with the environment by observing its state, acting accordingly, and then being rewarded or penalized. The agent wants to maximize its cumulative benefit over time. The agent gains knowledge by trial and error, changing its strategy in response to the rewards and penalties it encounters.

Numerous industries, including gaming, robotics, and autonomous systems, use reinforcement learning. It may be used, for instance, to educate a computer to play a game by rewarding excellent performance and punishing bad play. Reinforcement learning in robotics may be used to teach robots to carry out tasks in a setting while getting rewards for accomplishment and penalties for failure.

Reinforcement learning algorithms can be broadly categorized into two categories: value-based and policy-based. Value-based algorithms learn a function that maps states to values, which represent the expected reward for being in that state. Policy-based algorithms learn a policy directly, without estimating a value function.

Reinforcement learning is an active area of research and continues to evolve, with new algorithms and techniques being developed to solve morecomplex problems.

**(c.1)Usage of Reinforcement Machine Learning:**

**Gaming:** Reinforcement learning can be used to train AI agents to play games such as chess, poker, and Go.

**Robotics:** Reinforcement learning can be used to train robots to perform tasks in real-world environments, such as grasping objects or navigation.

**Autonomous Systems**: Reinforcement learning can be used to develop autonomous systems, such as self-driving cars, that can make decisions in real-world environments.

**Finance:** Reinforcement learning can be used to develop trading algorithms for financial markets.

**Healthcare:** Reinforcement learning can be used to optimize treatment plans for patients and improve patient outcomes.

**Marketing**: Reinforcement learning can be used to optimize advertising and marketing campaigns by learning from the outcomes of past actions.

**Supply Chain Management:** Reinforcement learning can be used to optimize supply chain operations by making decisions about production, inventory, and transportation.

**(c.2)Types of Reinforcement Machine Learning:**

**a. Value-based:** Value-based reinforcement learning algorithms learn a function that maps states to values, which represent the expected reward for being in that state. An example of a value-based reinforcement learning algorithm is Q-Learning, which is used to train AI agents to play games such as chess and Go.

**b. Policy-based:** Policy-based reinforcement learning algorithms learn a policy directly, without estimating a value function. An example of a policy-based reinforcement learning algorithm is REINFORCE, which is used in robotics to train robots to perform tasks such as grasping objects or navigation.



Figure-5(Reinforcement Machine Learning)

**III.(d)Semi-Supervised Machine Learning:**

A kind of machine learning called semi-supervised uses a combination of labelled and unlabeled data to train the algorithm. The method is trained using a dataset of labelled samples in classic supervised learning, where the label represents the expected result for a certain input. In unsupervised learning, the algorithm is trained on a dataset without any labels and then left to its own devices to discover patterns in the data.

To combine the benefits of both supervised and unsupervised learning, there is semi-supervised learning. The algorithm can learn the underlying structure of the data and generate predictions for fresh, unlabeled cases by only a little quantity of labelled data. This can be especially helpful when getting labelled data requires a lot of effort, money, or time.

Semi-supervised learning algorithms can be broadly categorized into two categories: generative and discriminative. Generative algorithms model the joint distribution of the inputs and labels, while discriminative algorithms model the conditional distribution of the labels given the inputs.

In order to handle ever-more complicated datasets and scenarios, new algorithms and approaches are being created in the semi-supervised learning field, which is an active area of study.

Natural language processing tasks, such text classification and named entity identification, are some instances of semi-supervised learning in the real world where a lot of unlabeled text data may be utilised to boost performance. In order to classify photos, semi-supervised learning may also be utilised. In this case, the system is trained on both labelled and unlabeled images.

**(d.1)Usage of Semi-Supervised Machine Learning:**

**Natural Language Processing:** Semi-supervised learning is often used in NLP tasks, such as text classification, named entity recognition, and sentiment analysis. In these tasks, large amounts of unlabeled text data can be used to improve the performance of the algorithm.

**Image Analysis:** Semi-supervised learning can be used in image classification tasks, where the algorithm is trained on a combination of labeled and unlabeled images. This can be useful when labeled data is limited, as the algorithm can still learn the underlying structure of the data.

**Healthcare:** Semi-supervised learning can be used in healthcare to predict patient outcomes or diagnose diseases. In these scenarios, a small amount of labeled data can be used to make predictions for new, unlabeled patients.

**Fraud Detection:** Semi-supervised learning can be used to detect fraudulent activity in financial systems. In these systems, labeled data is often limited, but the algorithm can still learn from the vast amounts of unlabeled data to make predictions.

**Marketing:** Semi-supervised learning can be used in marketing to make predictions about customer behavior. For example, the algorithm can learn from a combination of labeled data about customers who have made a purchase and unlabeled data about customers who have not made a purchase.

**(d.2)Types of Semi-Supervised Machine Learning:**

**a. Semi-Supervised Classification:** This involves using both labeled and unlabeled data to classify a target variable.

Example: Image classification with a small labeled dataset and a large unlabeled dataset.

**b. Semi-Supervised Regression:** This involves using both labeled and unlabeled data to predict a continuous target variable.

Example: Predicting house prices based on a small labeled dataset and a large dataset of neighborhood features.

**c. Self-Training:** This involves using a small labeled dataset to train a model and then using the model's predictions on the unlabeled data to generate pseudo-labels, which can then be used to improve the model.

Example: Sentiment analysis using a small labeled dataset and a large unlabeled dataset of customer reviews.

**d. Co-Training:** This involves training two or more models on different views of the same data and using their predictions to label the unlabeled data and improve the models.

Example: Named entity recognition using two models trained on different views of the same text data.

Figure-6(Semi-Supervised Machine Learning)

**III.(e)Transfer Machine Learning:**

Transfer learning is a machine learning technique where a model trained on one task is fine-tuned on a different but related task. The idea is to transfer knowledge learned on the original task to the new task, making it easier and faster to train. This is particularly useful when the amount of data available for the new task is limited, and the model can leverage the knowledge learned from the previous task to perform well on the new task.

**(e.1)Usage of Transfer Machine Learning:**

**Computer Vision:** Transfer learning is widely used in computer vision tasks such as object detection, image classification, and semantic segmentation.

**Natural Language Processing:** Transfer learning is used in NLP tasks such as sentiment analysis, text classification, and named entity recognition.

**Healthcare:** Transfer learning has been applied in the healthcare field to diagnose diseases, predict patient outcomes, and analyze medical images.

**Speech recognition:** Transfer learning has been used in speech recognition tasks to improve the accuracy of speech-to-text models.

**Robotics:** Transfer learning has been applied in robotics to improve control systems and perception tasks.

**(e.2)Types of Transfer Machine Learning:**

**a. Instance-based transfer learning:**

Example: Using a pre-trained image classification model on ImageNet to classify objects in photographs of a specific location, like a zoo.

**b. Feature-based transfer learning:**

Example: Using a pre-trained model's intermediate layer activations as features for a new classifier trained to solve a related but different problem, like recognizing a new set of objects.



Figure-7(Transfer Machine Learning)

# REFERENCES

1. L. Yan, C. Rong, and G. Zhao, “Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5931 LNCS, pp. 167–177, 2009.
2. B. Hamlen, K., Kantarcioglu, M., Khan, L. and Thuraisingham, “Security Issues for Cloud Computing,” Proc. - 9th Int. Conf. Comput. Intell. Secur. CIS 2013, pp. 150–162, 2012.
3. M. a. AlZain, E. Pardede, B. Soh, and J. a. Thom, “Cloud computing security: From single to multi-clouds,” Proc. Annu. Hawaii Int. Conf. Syst. Sci., pp. 5490–5499, 2011.
4. C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” Proc. - IEEE INFOCOM, 2010.
5. T. Swathi, K. Srikanth, and S. R. Reddy, “Virtualization in Cloud Computing,” Int. J. Comput. Sci. Mob. Comput., vol. 35, no. 5, pp. 540–546, 2014.
6. C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, “A survey on security issues and solutions at different layers of Cloud computing,” J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.
7. S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.
8. S. K. Abd, R. T. Salih, and F. Hashim, “Cloud Computing Security Risks with Authorization Access for Secure Multi-Tenancy Based on AAAS Protocol,” IEEE Reg. 10 Conf. TENCON, pp. 1– 5, 2015.
9. H. Aljahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu, “Multi-tenancy in cloud computing,” Proc. - IEEE 8th Int. Symp. Serv. Oriented Syst. Eng. SOSE 2014, pp. 344–351, 2014.
10. N. Kshetri, “Privacy and security issues in cloud computing: The role of institutions and institutional evolution,” Telecomm. Policy, vol. 37, no. 4–5, pp. 372–386, 2013.
11. K. Hashizume, D. Rosado, E. Fernández-Medina, and E. Fernandez, “An analysis of security issues for cloud computing,” J. Internet Serv. Appl., vol. 4, no. 5, pp. 1–13, 2013.
12. F. Sabahi, “Virtualization-level security in cloud computing,” in 2011 IEEE 3rd International Conference on Communication Software and Networks, 2011, pp. 250–254.
13. S. Carlin, “Cloud Computing Security,” Artif. Intell., vol. 3, no. March, pp. 14–16, 2011.
14. R. Buyya, R. Buyya, C. S. Yeo, C. S. Yeo, S. Venugopal, S.Venugopal,J.Broberg,J.Broberg,I.Brandic,andI.Brandic,“Cloudcomputing and emerging IT platforms:Vision,hype, andreality fordeliveringcomputingasthe5thutility,”Futur.Gener.Comput.Syst.,vol.25,no.6,p.17,2009.
15. J. Kabbedijk, C.-P. Bezemer, S. Jansen, and A. Zaidman, “Defining multi-tenancy: A systematic mapping study on the academic and the industrial perspective,” J. Syst. Softw., vol. 100, pp. 139–148, 2015.
16. J. Espadas, A. Molina, G. Jim??nez, M. Molina, R. Ram??rez, and D. Concha, “A tenant- based resource allocation model for scaling Software-as-a-Service applications over cloud computing infrastructures,” Futur. Gener. Comput. Syst., vol. 29, no. 1, pp. 273– 286, 2013.
17. H. Aljahdali, P. Townend, and J. Xu, “Enhancing multi-tenancy security in the cloud IaaS model over public deployment,” Proc. - 2013 IEEE 7th Int. Symp. Serv. Syst. Eng. SOSE 2013, pp. 385–390, 2013.
18. R. Wu, G.-J. Ahn, H. Hu, and M. Singhal, “Information flow control in cloud computing,” 2010 6th Int. Conf. Collab. Comput. Networking, Appl. Work., pp. 1–7, 2010.
19. M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges,” Inf. Sci. (Ny)., vol. 305, pp. 357–383, 2015.
20. F. Zhang and H. Chen, “Security-Preserving Live Migration of Virtual Machines in the Cloud,” J. Netw. Syst. Manag., pp. 562–587, 2012.
21. W. A. Jansen, “Cloud hooks: Security and privacy issues in cloud computing,” Proc. Annu. Hawaii Int. Conf. Syst. Sci., no. iv, p. 42, 2011.
22. K. Sunil Rao and P. Santhi Thilagam, “Heuristics based server consolidation with residual resource defragmentation in cloud data centers,” Futur. Gener. Comput. Syst., vol. 50, pp. 87–98, 2015.
23. J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning, “Managing security of virtual machine images in a cloud environment,” Proc. 2009 ACM Work. Cloud Comput. Secur. - CCSW ’09, no. Vm, p. 91, 2009.
24. M. Kazim, R. Masood, and M. A. Shibli, “Securing the virtual machine images in Cloud computing,” SIN 2013 - Proc. 6th Int. Conf. Secur. Inf. Networks, pp. 425–428, 2013.
25. R. Schwarzkopf, M. Schmidt, C. Strack, S. Martin, and B. Freisleben, “Increasing virtual machine security in cloud environments,” J. Cloud Comput. Adv. Syst. Appl., vol. 1, no. 1, p. 12, 2012.
26. D. Jeswani, A. Verma, P. Jayachandran, and K. Bhattacharya, “ImageElves: Rapid and reliable system updates in the cloud,” Proc. - Int. Conf. Distrib. Comput. Syst., no. i, pp. 390–399, 2013.
27. K. Fan, D. Mao, Z. Lu, and J. Wu, “OPS: Offline patching scheme for the images management in a secure cloud environment,” Proc. - IEEE 10th Int. Conf. Serv. Comput. SCC 2013, pp. 587–594, 2013.
28. Cloud Security Alliance, “Cloud Controls Matrix Working Group,” 2014. [Online]. Available: https://cloudsecurityalliance.org/group/cloud-controls-matrix/.
29. R. Sandhu, D. Ferraiolo, and R. Kuhn, “The NIST model for role-based access control,” Proc.

fifth ACM Work. Role-based access Control - RBAC ’00, pp. 47–63, 2000.

1. H. J. Smith, S. J. Milberg, and S. J. Burke, “Information Privacy: Measuring Individuals’ Concerns about Organizational Practices,” Manag. Inf. Syst. Q., vol. 20, no. 2, pp. pp. 167–196, 1996.
2. M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, “Security and privacy in cloud computing: A survey,” Proc. - 6th Int. Conf. Semant. Knowl. Grid, SKG 2010, pp. 105–112, 2010.
3. R. Sandhu and S. Jajodia, “Integrity principles and mechanisms in database management systems,” Comput. Secur., vol. 10, no. 5, pp. 413–427, 1991.
4. SK Tiwari, DS Rajput, S Sharma, SG Neogi, A Mishra,”Cloud Virtual Image Security for Medical Data Processing”,Mathematical Modeling and Soft Computing in Epidemiology, 317-345, 2020.

[34] Tiwari, S.K., Neogi S. G., Shakya H.K., Mishra A.,Devaraju T., “ Design and Implementation of a Virtualization Security Technique for Cloud Computing”, *Computer Integrated Manufacturing Systems*, *28*(12), 114–123,2022.

[35] Tiwari, S.K., Neogi S. G., Mishra A. Securing Virtual Images in Cloud Environment”, *Mathematical Statistician and Engineering Applications*, *71*(4), 7871–7882,2023.

[36] Tiwari, S.K., Neogi, S.G., Mishra, A. (2023). Design and Implementation of Security Enhancement for Trusted Cloud Computing. In: Kumar, A., Mozar, S., Haase, J. (eds) Advances in Cognitive Science and Communications. ICCCE 2022.Cognitive Science and Technology.Springer, Singapore.

[37].Tiwari,S.K. Sao,N., Kushwaha, A.,Book Title “[Fundamental of Machine Learning](https://scholar.google.com/citations?view_op=view_citation&hl=en&user=gpoUlO4AAAAJ&citation_for_view=gpoUlO4AAAAJ:eQOLeE2rZwMC)”,lambert Publication,ISBN: 9789391265335, Oct. 2022.