Recent Trend in Machine Learning: A Comprehensive Study

Sonali Soni[1], Dr. Rachana Dubey[2]
Ph.d. research Scholar[1], Assistant Professor[2]
Department of Computer Science[1,2]
Pandit S.N. Shukla University Shahdol, (M.P.), India. [1, 2]

Abstract: *Artificial intelligence (AI) and machine learning applications in the medical sector, pattern recognition, network security, financial sector, and many more sectors can produce excellent results for persons, patients, companies, and organizations such as improved efficiency, reduced operational cost, and enhanced customer satisfaction. ML has been explained as lying at the intersection of computer science, engineering, and systems. It has been marked as a tool that can be applied to various problems, especially in areas that require data to be interpreted and processed. ML, which is categorized as supervised machine learning, unsupervised machine learning, and reinforcement machine learning, plays an important role in solving the different problem using different dataset. In this paper we present the literature review for the different machine learning classifier using in different filed.*

Keywords:- Artificial intelligence, Machine learning, Deep learning, Classification, Supervised learning.

Introduction

Machine learning is one of the most promising tools in classification. In essence; machine learning is a model that aims to discover the unknown function, dependence, or structure between input and output variables. Usually, these relations are difficult to be existed by explicit algorithms via automated learning process. Machine-learning methods are applied to predict possible confirmed cases and mortality numbers for the upcoming. Machine learning can be divided into two parts. The first part is to define the optimal weight of data fusion of multi-node perception outcomes and eliminate unusable nodes based on the genetic algorithm, while the second part is to find fault nodes through a fault recognition neural network. Machine learning is a subsection of Artificial Intelligence (AI), and it involves several learning paradigms, such as Supervised Learning (SL), Un-supervised Learning (UL), and Reinforcement Learning (RL). Typical ML models consist of classification, regression, clustering, anomaly detection, dimensionality reduction, and reward maximization. The ML algorithms are trained in the SL paradigm, on labeled data sets, meaning that they exist to a ground-truth output (continuous or discrete) for every input. Conversely, in UL there is no ground-truth output, and the algorithms normally attempt to discover patterns in the data. Reinforcement Learning aims to raise the cumulative reward so that it is more suitable for sequential decision-making tasks. Supervised learning has regression and classification; unsupervised learning includes cluster analysis and dimensionally reduction, also Reinforcement Learning (RL) includes classification and control, as illustrated in below figure.

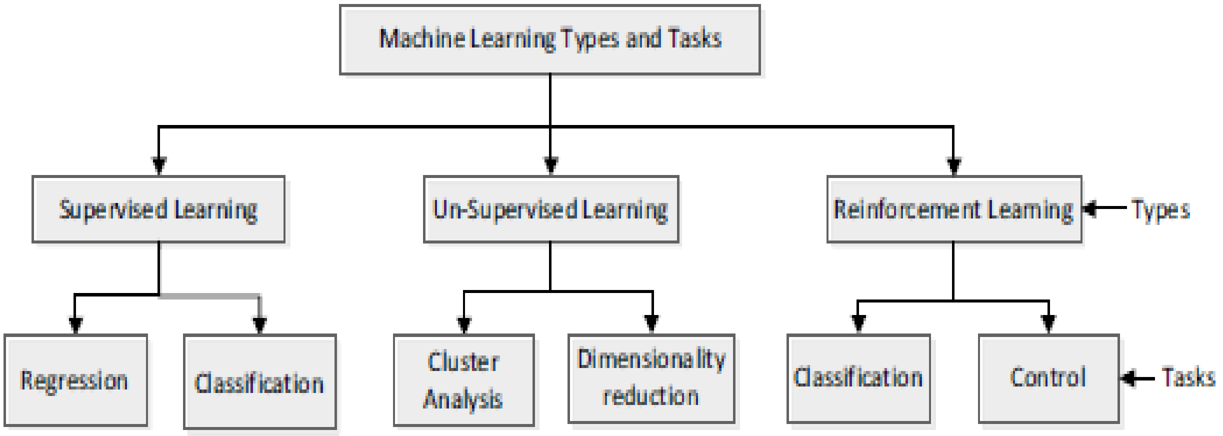

Fig. 1: Overview of machine learning types and tasks.

There are two broad classes of machine learning techniques, supervised learning and unsupervised learning. Supervised learning takes a set of feature/label pairs, called the training set. From this training set the system induces a generalized model of the relationship between the set of descriptive features and the target features in the form of a program that contains a set of rules. The objective is to use the output program produced to predict the label for a previously unseen, unlabelled input set of features, i.e. to predict the outcome for some \new" data. The features correspond to the input named \data".

Data with known labels, which have not been included in the training set, are classified by the generated model and the results are compared to the known labels. This dataset is called the test set. The accuracy of the predictive model can then be calculated as the proportion of the correct predictions the model labeled out of the total number of instances in the test set.

Unsupervised learning is the second form of machine learning and also takes a dataset of descriptive features, but without labels, as a training set. The goal now is to create a model that finds some hidden structure in the dataset, such as natural clusters. The promise of machine learning is that it can solve complex problems automatically, faster and more accurately than a manually specified solution, and at a larger scale. Over the past few decades, many machine learning algorithms have been developed by researchers, and new ones continue to emerge and old ones modified.

MACHINE LEARNING APPLICATIONS

Machine learning techniques, including deep learning, have been widely employed in the construction of credit card fraud detection models [7]. Existing research in this area predominantly utilizes supervised machine learning methodologies to develop fraud classifiers. These classifiers are built based on the experiences and knowledge gained from previous transactions, which include both legitimate and fraudulent samples. However, many challenges are faced in constructing effective detection models, including class imbalance, concept drift, features engineering, real-time requirements, class overlap, and lack of public datasets. The class imbalance problem, which is the focus of this study, has received much attention from researchers because it leads to biased classification toward the majority class. The minority instances are ignored by the classifiers, leading to a low detection rate and a high number of false alarms. ML has been explained as lying at the intersection of computer science, engineering, and systems. It has been marked as a tool that can be applied to various problems, especially in areas that require data to be interpreted and processed. ML, which is categorized as supervised machine learning, unsupervised machine learning, and reinforcement machine learning, plays an important role in solving the imbalanced dataset.

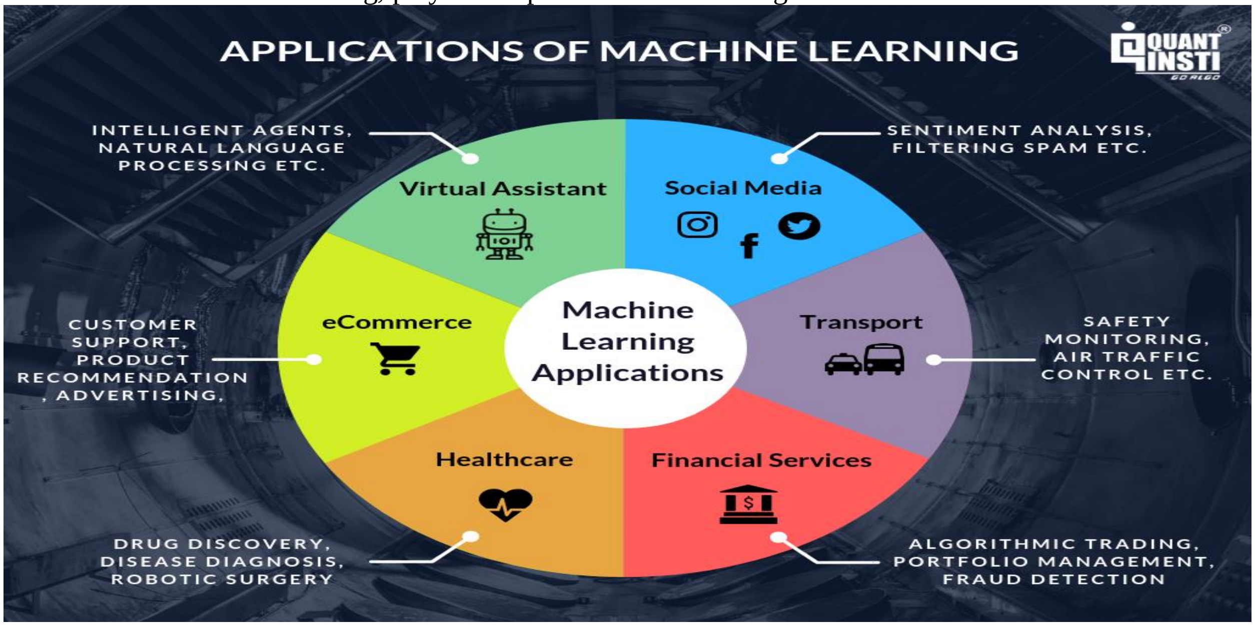
APPLICATIONS OF MACHINE LEARNING
QUANT INSTI
INTELLIGENT AGENTS, NATURAL LANGUAGE PROCESSING ETC.
SENTIMENT ANALYSIS, FILTERING SPAM ETC.
Virtual Assistant
Social Media
eCommerce
Machine Learning Applications
Transport
CUSTOMER SUPPORT, PRODUCT RECOMMENDATION , ADVERTISING,
SAFETY MONITORING, AIR TRAFFIC CONTROL ETC.
Healthcare
Financial Services
DRUG DISCOVERY, DISEASE DIAGNOSIS, ROBOTIC SURGERY
ALGORITHMIC TRADING, PORTFOLIO MANAGEMENT, FRAUD DETECTION

Fig. 2: Applications of machine learning.

➢ Emotion Recognition

Emotion recognition may be a method utilized in software that allows a program to “examine” the emotions on a person's face by utilizing sophisticated image dispensation. Firms are testing with an amalgamation of advanced formulas with image processing practices that have materialized within the last decade to understand more regarding what a video or a picture of an individual’s face tells us concerning how they're feeling. With current innovation, emotion identification software has developed very adeptly. Moreover, its aptitude to trace first facial looks for emotions like happiness, sadness, surprise, anger, etc., emotion detection software also can capture what specialists describe as “micro-expressions” or restrained cues of visual communication which may reveal a person’s feelings barren of their knowledge. Emotion recognition also concurs with other sorts of face recognition technologies and bio-metric image identification. These two sorts of technologies are often applied in many sorts of security cases. For instance, authorities can utilize emotion recognition software to further investigation efforts concerning someone at some point in an interview or interrogation. Emotion detection continues to travel forward on par with other innovations like tongue processing and these signs of progress are for the foremost part made probable by the blending of ever more dominant processors, the scientific growth of complex algorithms, and other associated technologies.

Facial expressions play a key role in understanding and recognizing emotions. Even the term "interface" suggests the importance of the face in communication between two entities. Studies have shown that reading facial expressions can dramatically alter the interpretation of what is being said and control the flow of conversation. A person's ability to interpret their emotions is very important for effective communication. The proportion of up to 93% of communication used in a normal conversation depends on the emotion of an entity. For ideal human machine interfaces (HCI), it would be desirable for machines to be able to read human emotions. This research focuses on how computers can correctly detect the emotions of their various sensors. This experience was used as a face image as a means of reading human emotions. Research on human emotions dates back to Darwin's pioneering work and has since attracted many researchers to the field. Seven basic emotions are universal for humans. Namely, neutral, angry, disgusted, fearful, happy, sad and surprised, and these basic emotions can be identified from a person's facial expression. This study suggests an effective way to identify these four emotions using the neutral, happy, sad and surprising frontal facial emotions. Various methods of recognizing emotions have been proposed in recent decades. Many algorithms have been proposed to develop system applications capable of very well detecting emotions. Computer applications could communicate better by altering reactions in various interactions depending on the emotional state of human users. A person's emotions can be determined by the tongue, face, or even gesture. The work presented in this article examines the recognition of facial expressions. For facial emotion recognition, the traditional approaches usually consider a face image that is distinguished from an information picture, and facial segments or milestones are recognized from the face districts. After that, different spatial and worldly highlights are separated from these facial segments. At last dependent on the separated highlights a classifier, for example, Keras library, random forest, is trained to produce recognitions results.

However, in practice, the structure of real- world FER datasets results in a significant constraint: the dataset may not contain images of every facial expression for every subject. Actually, we may not need to compare a query facial expression with any other class of facial expressions. According to some psychology and anatomy research [8] , the muscle activities of different facial expressions initiate from the neutral face as illustrated schematically in below figure . This is also the fundamental principle underlying the action units (AUs) and Facial Action Coding System (FACS) proposed by Ekman [2]. Since the expressive classes are naturally more discriminative from each other than from the neutral face, in the training stage, we may want to emphasize the neutral- expressive distance more than requiring large distance between those expressive classes. The neutral face images can be the ideal hard samples which can improve the learning efficiency of metric learning. However, expressive-neutral face image pairs of every person may not be always available in real world applications and in some FER image datasets.

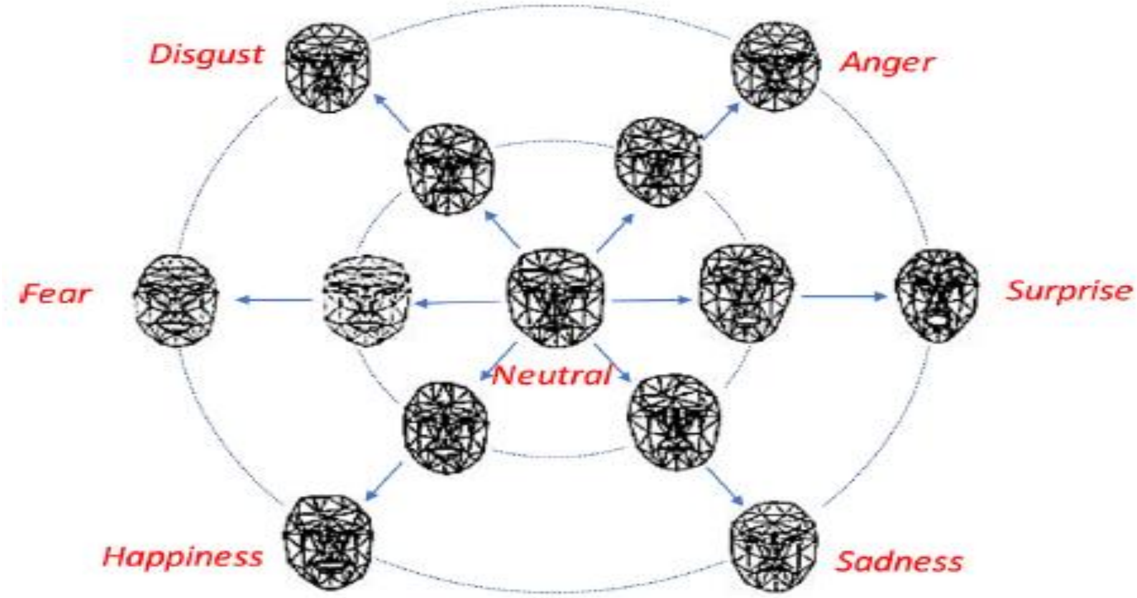

Fig. 3: A schematic depicting the 6 basic facial expressions and their relationships to the neutral face. Representations in the outer ring correspond to higher-intensity facial expressions compared to those in the inner ring.

- **Network Security**

The Intrusion Detection System (IDS) is a critical component of network and data protection. Because of the rapid evolution of network technology, identification of attacks based on contextual knowledge processing can be unique to particular apps and networks. Such a challenge can be solved with the aid of a hybrid intrusion detection system (IDS) [1]. DoS attacks are typically focused on packet flooding with the aim of overburdening the victim's infrastructure. These attacks are now capable of disrupting networks of almost any scale. One of the major testing obstacles for developing high-performance hybrid IDS is dealing with huge volumes of records with a large number of features. A large number of features can make it difficult to identify malicious patterns, resulting in a long training and testing process, increased resource demand, and a low detection rate. Computer security is characterized as the defense of computing systems from threats in order to preserve resource confidentiality, integrity, and availability. An intrusion is described as any series of acts that attempt to compromise network resources and the victim server. The Intrusion Detection System (IDS) is primarily used for tracking incidents that occur in computer systems/networks, analyzing data, identifying, preventing, or reporting to the system administrator so that appropriate action can be taken. The increase in the number of attacks launched by attackers has increased users' skepticism about the Internet. Denial of Service is an effective security assault (DoS). An intrusion detection system (IDS) is a monitoring system that tracks computer networks and network traffic and analyzes it for potential aggressive attacks from outside the organization as well as system abuse or attacks from inside the organization. In layman's words, an intrusion detection device is similar to a burglar detector. A car's lock system, for example, prevents it from burglary. However, if anyone cracks the lock mechanism and attempts to rob the vehicle, the burglar detector senses the broken lock and alarms the owner by raising an alarm sound. Similarly, IDS will function as an alert in a system/network to detect incidents and notify if any malicious behavior occurs. Attackers [1] continue to devise new ways to hack the host/network and conduct illegal operations. The Internet's scale and sophistication, as well as the operating systems on end hosts, make it more vulnerable to vulnerabilities. Because of these problems, existing Internet best practices depend on evidence of detecting attacking trends, monitoring security vulnerabilities, and closing them as soon as possible. Existing intrusion detection systems are seeing an increase in false alarms. Computational Intelligence (CI) components in IDS can be streamlined to minimize these. Many CI strategies were implemented by the researchers, and their accuracy was also measured using benchmark datasets. The Intrusion Detection System (IDS) is a multi colored technique that inspects both inbound and outbound network traffic, detects unusual patterns, and discards them. IDS are made up of three major components: a data base, an analysis engine, and a response manager [6]. The primary component of any IDS, also known as an event driver, is the data base. Host-based monitors, network-based monitors, application-based monitors, and target-based monitors are the four types of data sources.

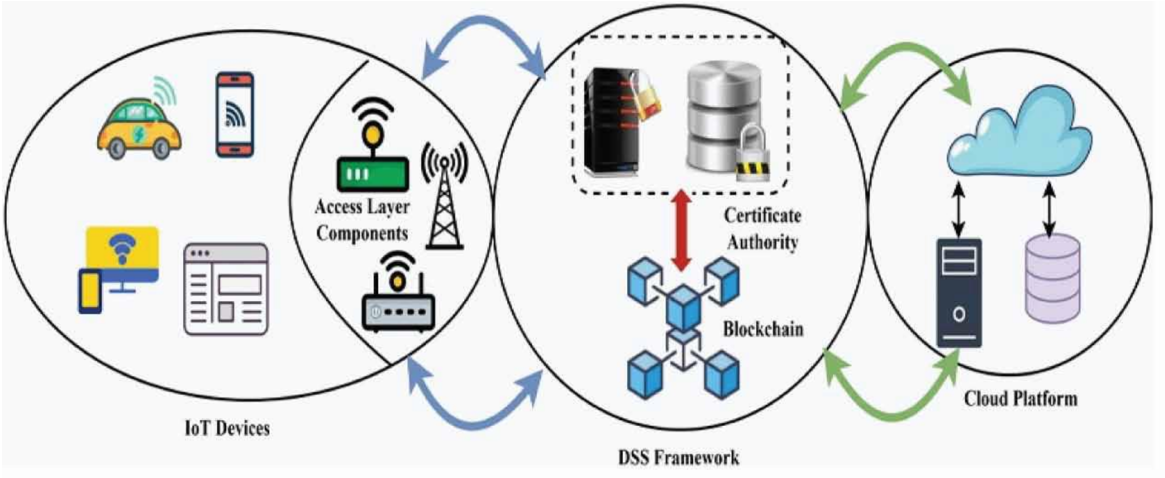

Fig. 4: IDS monitoring [11].

➢ Health Care

The human body contains various organs the heart is one of them, heart is a vital organ of the human body because it is functions to provide and pumping blood to all other remaining human body parts, therefore human life is completely dependent on the efficient operation of the heart. If the heart is not functioning properly, it will affect the other human body organs, such as the mind and kidneys with overall human body organs. Technology is increasing day by day everywhere; the healthcare sector is one of them. In the healthcare sector, artificial intelligence Approach with their subset like machine learning and, deep learning approaches are help’s the various disease diagnosis systems for patients.

AI applications are considered to play a key role in further establishing and supporting a decentralized rehabilitation model in which intelligent connected tools will be employed to assist clinical decision-making, and health outcomes monitoring. Many AI-based methods and solutions have been proposed in recent years to support the future challenge of enabling assisted physical therapy and assessments in a minimally supervised and decentralized manner, ideally at the patient's home. However, to the best of the authors' knowledge, no published works provided a comprehensive review of machine learning methods and applications used for remote monitoring and assistance in the rehabilitation context. Some existing works in literature have provided an overview of the role of machine learning algorithms combined with specific technologies used for rehabilitation issues, such as wearable sensors and vision-based motion capture technologies.

Clinical Research on AI and Machine Learning Applications The evaluation of progress has its own set of problems. In traditional clinical research, when progress takes the form of a new drug for a definable condition, the standards for testing and accepting the drug as an advance are well established. When the intervention is an AI and machine-learning algorithm rather than a drug, the medical community expects the same level of surety, but the standards for describing and testing AI and machine-learning interventions are far from clear. What are the standards to which AI and machine learning–based interventional research should be held, if an app is going to be accepted as the standard that will shape, reform, and improve clinical practice? That research has three components. First, the research must be structured to answer a clinically meaningful question in a way that can influence the behavior of the health professional and lead to an improvement in outcomes for a patient. Second, the intervention must be definable, scalable, and applicable to the problem at hand. It must not be influenced by factors outside the domain of the problem and must yield outcomes that can be applied to similar clinical problems across a wide range of populations and disease prevalence's. Can AI and machine learning–driven care meet these standards ones that we demand from a novel therapeutic intervention or laboratory-based diagnostic test or do we need to have a unique set of standards for this type of intervention? Third, when the results of the research are applied in such a way as to influence practice, the outcome must be beneficial for all patients under consideration, not just those who are similar to the ones with characteristics and findings on which the algorithm was trained. This raises the question of whether such algorithms should include consideration of public health (i.e., the use of scarce resources) when diagnostic or treatment recommendations are being made and the extent to which such considerations are part of the decision-making process of the algorithm. Such ethical considerations have engaged health professionals and the public for centuries.8 Use of AI and Machine-Learning Applications in Conducting Clinical Research AI and machine learning have the potential to improve and possibly simplify and speed up clinical trials through both more efficient recruitment and matching of study participants and more comprehensive analyses of the data. In addition, it may be possible to create synthetic control groups by matching historical data to target trial enrollment criteria. AI and machine learning may also be used to better predict and understand possible adverse events and patient subpopulations. It seems possible that AI could generate "synthetic patients" in order to simulate diagnostic or therapeutic outcomes. But the use of AI and machine learning applications and interventions introduces a set of uncertainties that must be dealt with both in protocols and in reporting of clinical trials.

➢ Credit card fraud detection

In today's era, the people of smart societies are paying more money using debit/credit cards while purchasing something online/off-line because it is heavy and uneasy to carry the wallet with huge amount of money and this is becoming the basic reason for drastic increase in the rate of fraud. In real life it is not easy to track the transaction done by the fraudulent because the technique used are very simple like pattern matching techniques. Due to this reasons now banks and other transaction partners are going for the better option and imperative methods for detecting the frauds in transactions. In present scenario the people are more curious towards ethical hacking and studding the cloud server based data transactions in IoT environment so that they can easily complete transactions related tasks by themselves. Since, the numbers of ethical hackers are increasing in our society day-by-day. So, these ethical hackers have now started their own business of hacking the cloud servers and executing frauds in the fake names like bank persons, big bazaar persons, Government officers, income tax officers and charity persons etc. Hence, exponential increase in the numbers of debit/credit card transactions related frauds are happening. Further, it observed that the fraudulent persons are preferring credit cards for executing frauds rather than debit cards because the debit cards may have limited amount of money at a particular time and on the other hand the credit cards may have extended limits and hence a huge amount of money can be withdrawn at any moment. This may bring the credit card holder in bankruptcy state.

On the basis of types of frauds done by the fraudulent, the researchers have divided the frauds related things into three types. In the first type of fraud, the persons with small intentions of normal type of fraud are included and these persons usually don't have any previous criminal history. These types of activities are done by fraudulent when the offender is in urgent need of money to fulfil his day-to-day needs and gets some opportunities to get the money. In the 2nd type of frauds, the person with criminal activities called criminal offenders are indulge in executing frauds related to debit/credit cards based illegal transactions. These criminal minded people use someone credit/debit card by becoming self-defined bank officers or big bazaar managers to purchase the goods and other things which are luxuries or criminal activities. In the 3rd type of fraud the organized crime related people indulge them in executing frauds by taking higher level of risks. These people are highly skilled in using the debit/credit cards for online transactions in cloud-IoT based environment and may take out all money in few seconds after getting the chance to carry out frauds. The diversified types of frauds happening in day-to-day work of bank account related transactions can be further divided into four categories namely Bankruptcy frauds, Theft frauds, Application frauds, and Behavioural frauds. In the cases of bankruptcy frauds, the fraudulent uses the information from the bureau as the prime source of information to take out/transfer the money from the card and exercises all the possibilities to implement the bankruptcy model. This is one of the highest levels of frauds happening in the government/private banks and the victims are able to know about the happening of frauds after many months of its actual execution. In the theft type of fraud, the owners debit/credit cards are being stolen or cloned by the fraudulent people who are taking out whole money before the actual owner of the card blocks it through bank or any other legal agencies. The application fraud is happening in banks or other corporate offices when a person is applying for fresh application and he/she gives all erroneous information about him and on later after becoming responsible official he/ she withdraws huge amount of money from companies account [11].

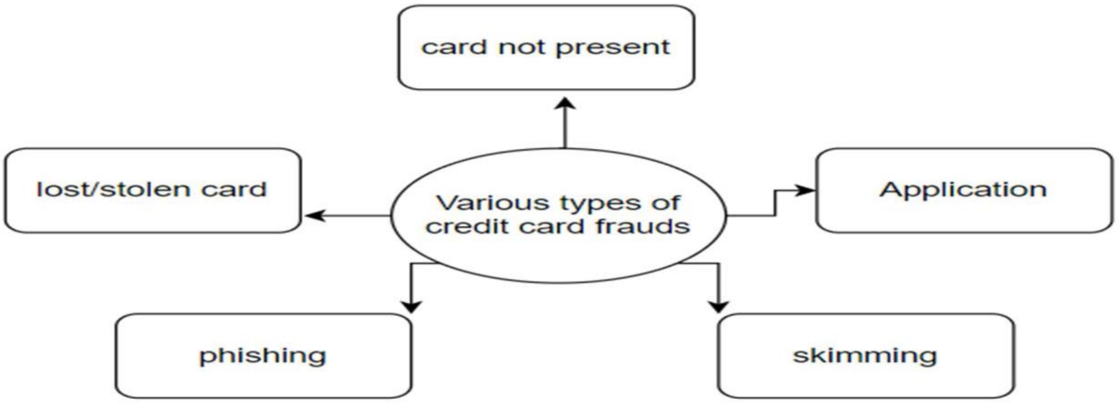

Fig. 5: Different forms of credit card scams.

MACHINE LEARNING TECHNIQUES

ML has many branches, and each branch can deal with different learning tasks. However, ML learning has different framework types. The ML approach provides a solution for CCF, such as random forest (RF). The ensemble of the decision tree is the random forest [3]. Most researchers use the RF approach. To combine the model, we can use (RF) along with network analysis. This method is called APATE. Researchers can use different ML techniques, such as supervised learning and unsupervised techniques. ML algorithms, such as LR, ANN, DT, SVM and NB, are commonly used for CCF detection.

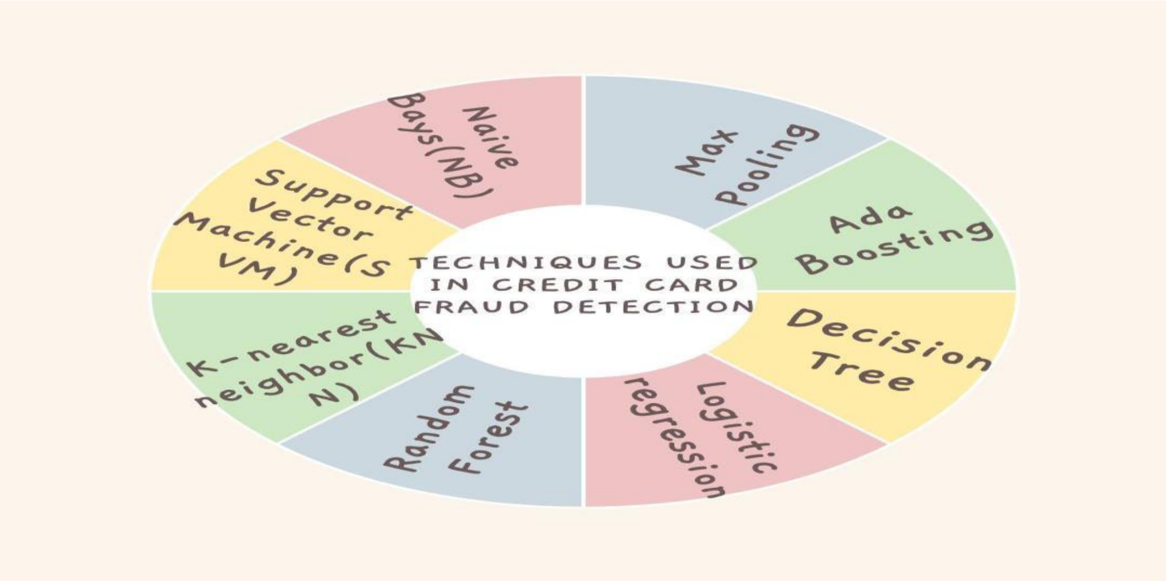

Fig. 6: Machine learning algorithms [12].

➢ **Random Forest Classification**

The RF algorithm is a classification method that is based on trees and involves the production of several trees that are then integrated using an equally weighted majority vote. During the process of training each individual tree, a third of the initial dataset that was used for training is omitted at random. RF is an ensemble learning classifier that has achieved efficient classification results in a variety of applications. Random Forest classifier is a supervised learning algorithm. Random Forest classifier generates decision trees from randomly chosen data samples, obtain predictions from each tree, and vote on the best solution. Space is divided into classes depending on the training data classification; in this case, there are two classes: normal and abnormal. The testing images are classified as Cataract or Normal based on their resemblance to two groups. The RF classification is an ensemble technique that continuously uses bootstrapping, averaging, and bagging to train many decision trees. By employing distinct subsets of accessible characteristics, numerous independent decision trees can be constructed simultaneously on different segments of the training samples. Bootstrapping guarantees that any decision tree inside the random forest is distinct, lowering the RF variance. RF classification combines numerous tree decisions for the final judgment; as a result, the RF classifier has a strong generalization. The RF classifier aims to consistently outperform almost all other classifier techniques in terms of precision without difficulties of imbalanced datasets and overfitting. This classifier also handles missing values in the data, unlike other machine learning. Another advantage is the ability to deal with high-dimensional and complex data.

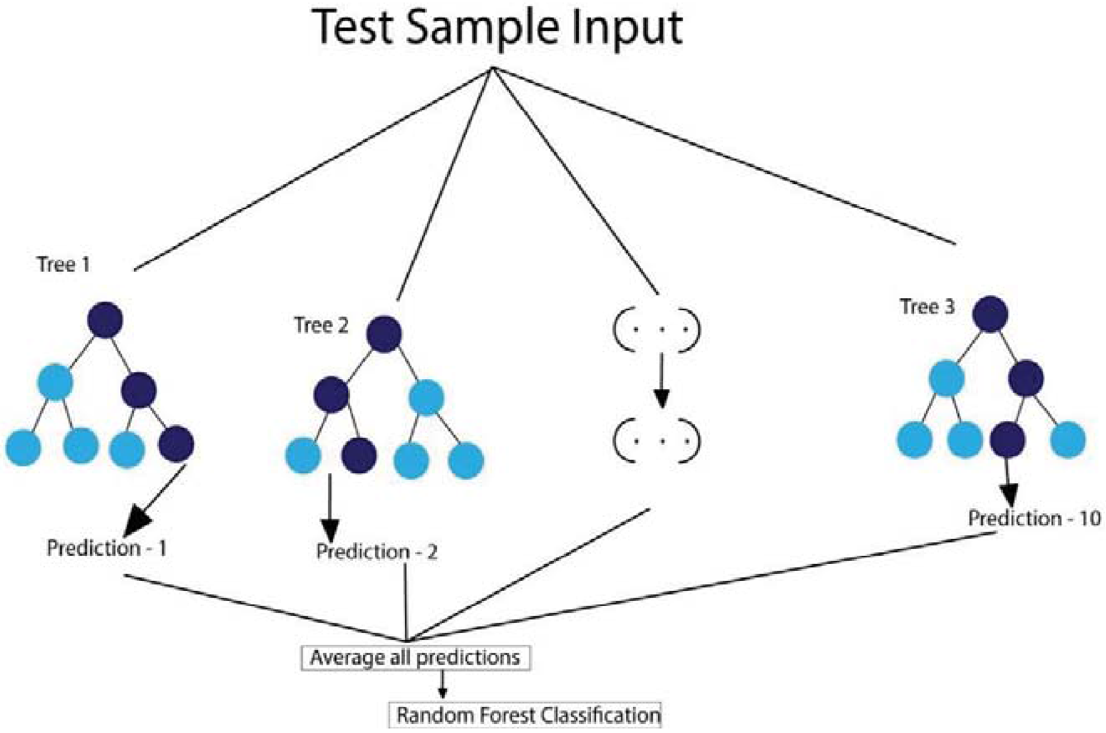

Fig. 7: This picture shows the classification using random forest.

The classifier worked on the dataset by creating multiple different decision trees. Then, it trained each decision tree on multiple divergent samples where the sampling was done through replacements. The process, in turn, aided in having a better interpretation of the bias and variance.

➢ **Decision tree classifier**

A decision tree is a tool that uses a decomposition using a tree of decisions and their outcome, including multiple outcomes, such as resource costs, and utility. The approach is to make splits so that a significant impact on a tree's accuracy would be observed. Regression and classification trees have different a pre-defined decision criterion. To decide whether to divide a node into two or more sub-nodes, we can use a variety of techniques for building a decision tree. The homogeneity of newly formed sub-nodes is increased by a sub-node creation. Formally speaking, we can say that the node's homogeneity improves in regard to the desired variable. Accordingly, the DT divides the nodes based on all variables that are accessible before choosing the branching that results in the least heterogeneous sub-nodes. The nature of target variables is considered when choosing an algorithm. However, choosing which attribute to put at the root of the tree or at various levels as internal nodes is a difficult step if the dataset has N attributes. The problem cannot be resolved by simply choosing any node at random to be the root. A random technique could produce odd outcomes with little accuracy. In this context, researchers found out different approaches to this attribute selection. Accordingly, they recommend employing measures like: Entropy, Information Gain that is related to Entropy, Gini index, etc. In this paper, we use Gini index as criteria as it is offered in the employed Python package that we will use for implementation [13].

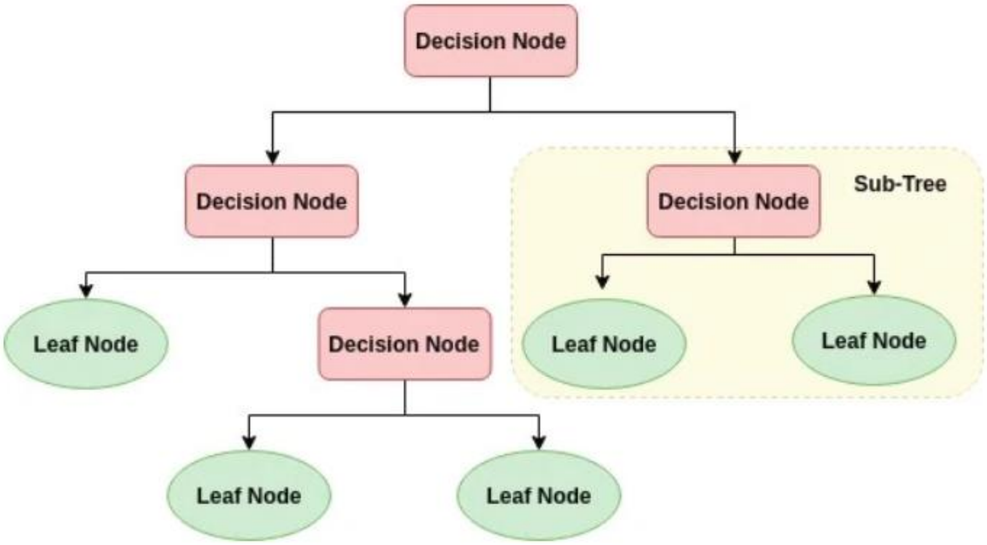

Fig. 8: The above picture represents the decision tree classifier.

➢ **Gradient Boosting Decision Trees**

Boosting algorithms, as a class of ensemble learning methods, have become very popular in data classification, owing to their strong theoretical guarantees and outstanding prediction performance. However, most of these boosting algorithms were designed for static data, thus they cannot be directly applied to on-line learning and incremental learning. Gradient boosting decision tree (GBDT) [1] is a widely-used machine learning algorithm, due to its efficiency, accuracy, and interpretability. GBDT achieves state-of-the-art performances in many machine learning tasks, such as multi-class classification, click prediction, and learning to rank. In recent years, with the emergence of big data (in terms of both the number of features and the number of instances), GBDT is facing new challenges, especially in the tradeoff between accuracy and efficiency. Conventional implementations of GBDT need to, for every feature, scan all the data instances to estimate the information gain of all the possible split points.

In gradient boosting decision trees, we combine many weak learners to come up with one strong learner. The weak learners here are the individual decision trees. All the trees are connected in series and each tree tries to minimize the error of the previous tree. Due to this sequential connection, boosting algorithms are usually slow to learn, but also highly accurate. In statistical learning, models that learn slowly perform better.

The weak learners are fit in such a way that each new learner fits into the residuals of the previous step so as the model improves. The final model aggregates the result of each step and thus a strong learner is achieved. A loss function is used to detect the residuals. For instance, mean squared error (MSE) can be used for a regression task and logarithmic loss (log loss) can be used for classification tasks. It is worth noting that existing trees in the model do not change when a new tree is added. The added decision tree fits the residuals from the current model.

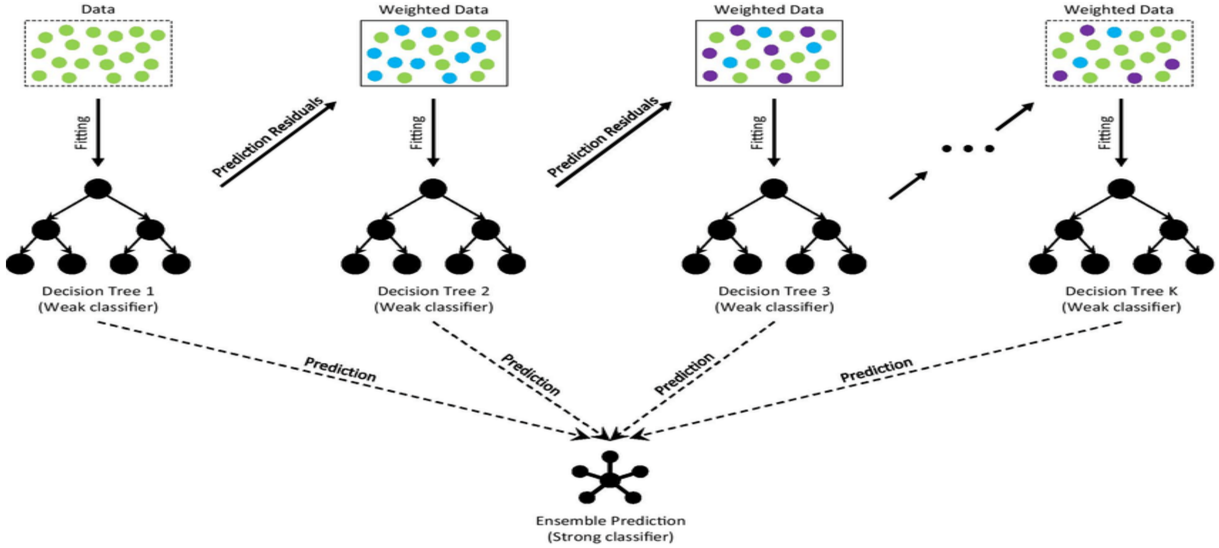

Fig. 9: This picture shows the data classification model using gradient boost decision tree.

➢ **Artificial Neural Network (ANN)**

Machine learning in neural networks includes artificial neural networks. The functioning of ANNs is compared to that of the human brain. It is built to mimic a human neuron cell in that it learns from data, classifies, and anticipates output in the same manner as a cell receives input and responds [28]. The statistical architecture used to find sophisticated problem-solving is non-linear. As illustrated in Figure 5, an ANN structure comprises a data input layer, one or more hidden layers, and an output layer with many nodes that resemble neurons in the human brain. Nodes in an ANN function as the input of the input layer, taking information from the output world and feeding it to the hidden layer, like how neurons interact. After some data processing, the hidden layer finds the pattern. The concealed layer may have one or more layers. Multi-Layer Perceptron (MLP), which we shall explore in the next point, is an ANN with several hidden layers and backpropagation. Once everything has been processed, it sends the categorized data to the output layer. An activation function is used to transform an input function into an output function; there are many distinct activation functions, including logistic, sigmoid, tanh, and linear. Recently, ANNs have gained more popularity and are utilized in various industries, including medicine, image identification, speech recognition, and facial recognition. However, employing the proper activation function and ANN parameters may provide significantly superior predictions.

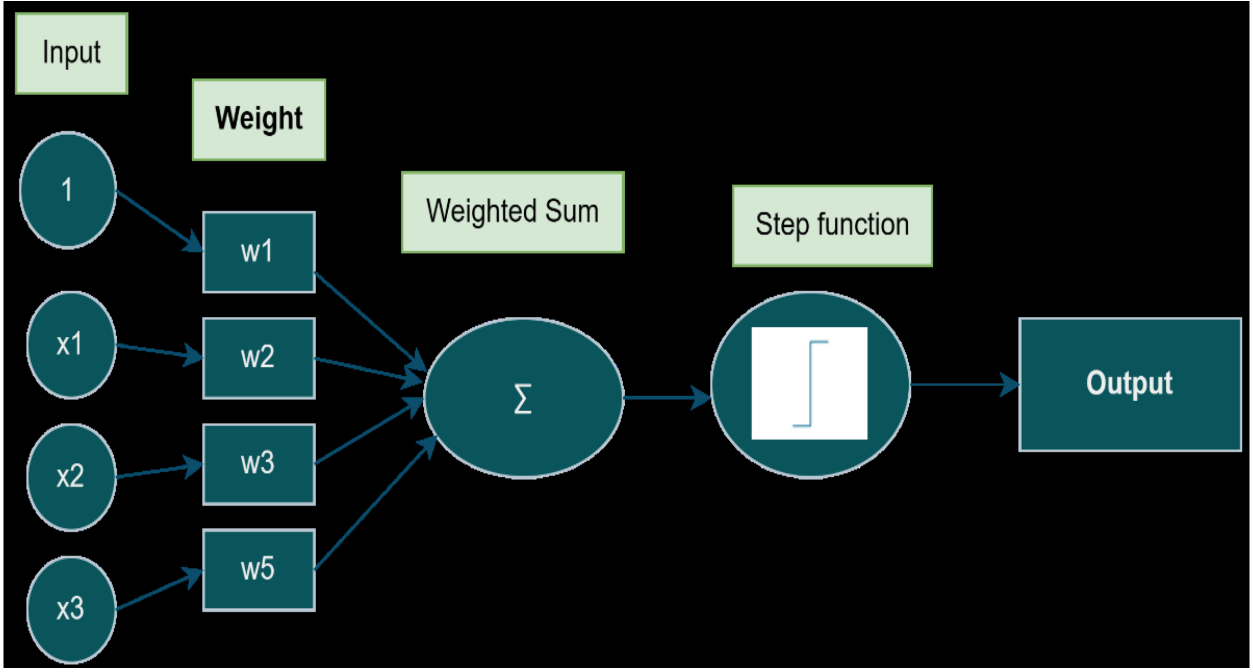

Fig. 10: The basic structure of ANN.

IV. Conclusion and Future Scope

In effect, with machine learning we have programs using data to create new programs. This is in contrast to the traditional way that programs have been generated by human programmers in which they encode the rules that the computer follows in a programming language in order to produce a solution to a specified problem. Technological innovation has drastically altered how we interact with our surroundings through the artificial intelligence and machine learning technologies. From simple tasks like browsing the web to complex tasks like diagnosing patients, and pattern recognition the artificial intelligence has highly influenced peoples' daily lives. Here we discuss different machine learning techniques for different application in future we plan to create a machine learning based model for different applications and improve the existing model.

References

[1] Ripon Patgiri, Udit Varshney, Tanya Akutota, and Rakesh Kunde, "An Investigation on Intrusion Detection System Using Machine Learning", IEEE 2018, pp 1684-1691.

[2] Shone, N, Tran Nguyen, N, Vu Dinh, P and Shi, "A Deep Learning Approach to Network Intrusion Detection", IEEE Transactions on Emerging Topics in Computational Intelligence, 2017, pp 1-11.

[3] Chuanlong Yin , Yuefei Zhu, Jinlong Fei, Xinzheng He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks", IEEE 2017, pp 21954-21961.

[4] James Brown, Mohd Anwar, Gerry Dozier, "An Evolutionary General Regression Neural Network Classifier for Intrusion Detection", IEEE 2016, Pp 1-5.

[5] Longjie Li , Yang Yu, Shenshen Bai, Jianjun Cheng, Xiaoyun Chen, "Towards Effective Network Intrusion Detection: A Hybrid Model Integrating Gini Index and GBDT with PSO", Journal of Sensors, 2018, Pp 1-10.

[6] Yanqing Yang, Kangfeng Zheng, Chunhua Wu, Xinxin Niu, Yixian Yang, "Building an Effective Intrusion Detection System Using the Modified Density Peak Clustering Algorithm and Deep Belief Networks", Applied Science Journal, 2019, Pp 1-25.

[7] Malek Al-Zewairi, Sufyan Almajali, Arafat Awajan, "Experimental Evaluation of a Multi-Layer Feed-Forward Artificial Neural Network Classifier for Network Intrusion Detection System", International Conference on New Trends in Computing Sciences, IEEE 2017, pp 167-173.

[8] M. Mazhar Rathore, Faisal Saeed, Abdul Rehman, Anand Paul, Alfred Daniel, "Intrusion Detection using Decision Tree Model in High-Speed Environment", International Conference on Soft-computing and Network Security, IEEE 2018, Pp 1-5.

[9] L. Khalvati, M. Keshtgary, N. Rikhtegar, "Intrusion Detection based on a Novel Hybrid Learning Approach", Journal of AI and Data Mining, 2018, Pp 157-162.

[1] [10] Deepak Kumar Rathore, Dr. Praveen Kumar Mannepalli, “A Review of Machine Learning Techniques and Applications for Health Care”, International Conference on Advances in Technology, Management & Education, 2021, IEEE proceeding, 978-1-7281-8586-6/21.

[11] Ban Salman Shukur1, Maad M. Mijwil, “Involving machine learning techniques in heart disease diagnosis: a performance analysis”, International Journal of Electrical and Computer Engineering, 2023, pp. 2177-2185.

[12] Belal Abuhaija, Aladeen Alloubani, “A comprehensive study of machine learning for predicting cardiovascular disease using Weka and SPSS tools”, International Journal of Electrical and Computer Engineering, 2022, pp. 1891-1902.

[13] Huru Hasanova, Muhammad Tufail, Ui-Jun Baek,Jee-Tae Park, Myung-Sup Kim.“A novel blockchain-enabled heart disease prediction mechanism using machine learning”, Computers and Electrical Engineering, 2022, pp. 1-13.

[14] Deepak Kumar Rathore, Praveen Kumar Mannepalli, “Recent Trends in Machine Learning for Health Care Sector”, International Journal of Innovative Research in Technology and Management, Vol-5, Issue-2, 2021.

[15] GhulabNabi Ahmad, Hira Fatima, Shafiullah, “Efficient Medical Diagnosis of Human HeartDiseases Using Machine Learning TechniquesWith and Without Grid SearchCV”, IEEE Access, 2022, pp. 80151-80173.

[16] AlaaMenshawi, Mohammad Mehedi Hassan, “A Hybrid Generic Framework for Heart Problem DiagnosisBased on a Machine Learning Paradigm”, Sensors 2023, pp. 1-17.

[17] Rubini PE, C.A.Subasini, “A Cardiovascular Disease Prediction using Machine Learning Algorithms”, 2021 , pp. 904-912.

[18] Anna MarkellaAntoniadi, Yuhan Du, “Current Challenges and Future Opportunities for XAI in Machine Learning-Based Clinical Decision Support Systems: A Systematic Review”, Appl. Sci. 2021, pp. 1-23.

[19] Baptiste Vasey, MMed; Stephan Ursprung, “Association of Clinician Diagnostic Performance With Machine Learning–Based Decision Support Systems A Systematic Review”, JAMA Network, 2021, pp. 1-15.

[20] Rajkumar S. Jagdale, Vishal S. Shirsat, Sachin N. Deshmukh, “Sentiment Analysis on Product Reviews Using Machine Learning Techniques”, Springer Nature Singapore Pte Ltd. 2019, pp. 639-648.

[21] Ahmed S. Abdullah, Majida Ali Abed, Israa Al_Barazanchi, “Improving face recognition by elman neural network using curvelet transform and HSI color space”, Periodicals of Engineering and Natural Sciences, 2019, pp.430-437.

[22] Zahra Mortezaie, Hamid Hassanpour, “A Survey on Age-Invariant Face Recognition Methods”, Jordanian Journal of Computers and Information Technology, 2019, pp. 87-97.

[23] Muhammad Sajjad, Sana Zahir Amin Ullah, Zahid Akhtar, Kha, n Muhammad, “Human Behavior Understanding in Big Multimedia Data Using CNN based Facial Expression Recognition”, Mobile Networks and Applications, Springer 2019, pp 1-11.

[24] R Dubey, D Rathore,, “An empirical study of intrusion detection system using feature reduction based on evolutionary algorithms and swarm intelligence methods”, International Journal of Applied Engineering Research 12 (19), 2017. pp. 8884-8889.

[25] Xiaofeng Liu, B.V.K. Vijaya Kumar, Ping Jia, Jane You, “Hard negative generation for identity-disentangled facial expression recognition”, Pattern Recognition, 2019, pp. 1-12.

[26] Tata Sutabri, Pamungkur, Ade Kurniawan, Raymond Erz Saragih, “Automatic Attendance System for University Student Using Face Recognition Based on Deep Learning”, International Journal of Machine Learning and Computing, 2019, pp. 668-674.

[27] Emmanuel Ileberi, Yanxia Sun, Zenghui Wang, “Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost”, IEEE Access, 2021, pp. 165286-165295.

[28] Ebenezer Esenogho, Ibomoiye Domor Mienye, “A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection”, IEEE Access, 2022, pp. 16400-16408.

[29] Wei Zhou, Xiaorui Xue, “Credit card fraud detection based on self-paced ensemble neural Network”, ITCC 2022, pp. 92-99.

[30] Tzu-Hsuan Lin, Jehn-Ruey Jiang, “Credit Card Fraud Detection with Autoencoder and Probabilistic Random Forest”, Mathematics 2021, pp. 1-16.

[31] Gayan K. Kulatilleke, “Credit Card Fraud Detection Classifier selection Strategy”, 2022, pp. 1-17.

[32] Konduri Praveen Mahesh, Shaik Ashar Afrouz, “Detection of fraudulent credit card transactions: A comparative analysis of data sampling and classification techniques”, Journal of Physics: Conference Series, 2021, pp. 1-9.

[33] Dileep M R, Navaneeth A V, "A Novel Approach for Credit Card Fraud Detection using Decision Tree and Random Forest Algorithms", IEEE, 2021, pp. 1025-1028.

[34] Mosa M. M. Megdad, Bassem S. Abu-Nasser, " Fraudulent Financial Transactions Detection Using Machine Learning", International Journal of Academic Information Systems Research, 2022, pp. 30-39.

[35] Shubham Shah, Dhairya Shah, "Credit Card Fraud Detection System using Machine Learning", International Journal of Research in Engineering and Science, 2022, pp. 9-14.

[36] Appala Srinuvasu Muttipati, SangeetaViswanadham, "Recognizing Credit Card Fraud Using Machine Learning Methods", Turkish Journal of Computer and Mathematics Education, 2021, pp. 3271-3278.

[37] Akhil Songa, Sri Teja Kumar Reddy Tetali, Naga Sai Tanmai Raavi, "Credit Card Fraud Detection using Various Machine Learning Algorithms", International Journal for Research in Applied Science & Engineering Technology, 2022, pp. 1174-1185.

[38] Ashu Kumar, Amandeep Kaur, Munish Kumar, "Face detection techniques: a review', Artificial Intelligence Review, Springer 2018, pp. 1-22.

[39] Deepak Rathore, "Diseases Prediction and Classification Using Machine Learning Techniques", AIP Conference Proceedings 2424, 070001 (2022); https://doi.org/10.1063/5.0076768.

[40] Amit Kumar, Naveen Tewari, Rajeev Kumar, "Study towards the Analytic Approach for Human Computer Interaction using Machine Learning", The International journal of analytical and experimental modal analysis, 2019, pp. 1-11.

[41] Michele Merler, Nalini Ratha, Rogerio Feris, John R. Smith, "Diversity in Faces", 2019, pp. 1-29.

[42] Awais Mahmood, Shariq Hussain , Khalid Iqbal, Wail S. Elkilani, "Recognition of Facial Expressions under Varying Conditions Using Dual-Feature Fusion", Hindawi Mathematical Problems in Engineering, 2019, pp 1-13.