International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

Data Poisoning Attacks on Machine Learning Model Reliability

[1]Prasetha N

Department of Computer Science and Engineering

Bannari Amman Institute of Technology

prasetha.cs19@bitsathy.ac.in

[2]Indirani A

Department of Artificial intelligence and Machine Learning

Bannari Amman Institute of Technology

indirania@bitsathy.ac.in

Abstract

Data poisoning attacks on machine learning model reliability, is to identify poisoned attacks in a data set and support clinicians for their future study. A data set is a collection of related sets of information composed of separate items, which can be processed as a unit by a computer. Healthcare data sets include a vast amount of medical data gathered from various healthcare data sources. The healthcare data sets need to be always kept secured, since they can be used further by the doctors or researchers. The chosen healthcare data sets are first run through an ML algorithm called Bayesian Neural Network, which determines the dataset's accuracy. The data set's accuracy can be used to determine whether the data set is poisoned or not. Following that, the dataset is pre-processed, and then the three algorithms named Random Forest, Support Vector Machine and Logistic Regression are used. The highest accuracy producing algorithm is chosen as the best. The best algorithm is chosen as Support Vector Machine due to its high accuracy and is then used to help doctors in the further study of the patient's health condition.

Keywords **- Data poisoning, Bayesian Neural Network, Random Forest, Support Vector Machine, Logistic Regression**

I.INTRODUCTION

Any information "relating to health issues, reproductive results, causes of mortality, and quality of life" for a person or population is considered to be health data. Clinical measurements and relevant environmental, socioeconomic, and behavioral data are all included in health data, which also contains clinical metrics. There are two types of health data: structured and unstructured. Health information systems can exchange standardized, structured health data with ease. For instance, structured data formats can be used to store information like a patient's name, birthdate, or blood test results. Contrary to structured data, unstructured health data is not standardized. Unstructured health data includes things like emails, audio recordings, and doctor's notes regarding a patient. The complexity of health data has prevented uniformity in the healthcare business even as developments in health information technology have increased collection and usage. The global healthcare industry is experiencing change as the new norm. In fact, for the foreseeable future, the clinical, operational, and financial models of the economy as a whole are undergoing a significant and fundamental transition as a result of the digitalization of health and patient data. This shift is being prompted by ageing populations and lifestyle changes, the proliferation of software applications and mobile devices, innovative treatments, a greater emphasis on care quality and value, and evidence-based medicine rather than subjective clinical decisions. These factors together are creating significant opportunities for supporting clinical decision, improving healthcare delivery, management and policy making, monitoring adverse events, and surveillant disease. The digitalization of healthcare has the potential to alter healthcare and offers many benefits, but it also presents numerous obstacles and concerns. Indeed, worries about the security and privacy of healthcare data grow yearly. A bottom-up, reactive strategy to identifying security and privacy requirements that is focused on technology was also discovered by healthcare organizations to be insufficient for safeguarding the organization and its patients.

A. Data poisoning

Attacks that poison a machine learning model require contaminating the training data. Data manipulation is referred to be an integrity attack since it prevents the model from producing accurate predictions. With a poisoning attack, the attacker's objective is to have their inputs accepted as training data, in contrast to an attack that aims to circumvent a model's prediction or classification. The length of the attack also varies depending on the model's training cycle; the attacker may need many weeks to complete their intended poisoning. Data poisoning can be accomplished either in a Whitebox scenario where the attacker gains access to the model and its private training data, possibly somewhere in the supply chain if the training data is gathered from multiple sources, or in a Blackbox scenario against classifiers that depend on user feedback to update their learning. Data poisoning's key drawback is that it's difficult to resolve. Depending on the purpose for which they are to be used and the preferences of their owners, models are retrained using newly acquired data at specific intervals. Because poisoning typically occurs over a period of time and a number of training cycles, it can be challenging to identify when prediction accuracy begins to change. To remove all the faulty data samples and undo the poisoning effects, a time- consuming historical study of the impacted class's inputs would be necessary. The model would then need to be retrained using data from before the attack began. Retraining in this manner, however, is simply not practical when dealing with vast amounts of data and numerous attacks, and the models are never fixed.

II. EXISTING SYSTEM

In the suggested system, the voice samples of the patients are recorded in different conditions like healthy, pathological and others for both male and female. Voice sounds of this database were recordings at the Caritas clinic St. Theresia in Saarbruecken by the Institute of Phonetics of the University of Saarland together with the Department of Phoniatrics and Ear, Nose and Throat (ENT). It consists of more 2000 recordings of sustained /a/, /i/ and /u/ vowels and a speech sequence. Samples, freely available, come from subjects afflicted by several voice disorders, including functional and organic pathologies. The recorded voice samples used as the data set is subsequently trained and tested using several machine learning ML techniques. A decision tree is used to represent the learned function in the decision tree category of ML techniques, which are used to classify categorical data. Decision trees are useful in the medical field because they can handle missing values, categorical and continuous data, and are simple to interpret. Several DT approaches like Random Forest, REPTree, Random Tree, Adadboost and Support Vector Machine (SVM) were analysed. Clinical voice quality evaluation is performed by using several procedures, such as the laryngeal examination, completion of self-assessment questionnaires or acoustic analysis. This consists of an estimation of appropriate acoustic parameters estimated from voice signal useful to evaluate any possible alterations of the vocal quality. The acoustic features can constitute the input data of several ML algorithms able to evaluate the voice quality. The aim of this system was to examine the behaviour of each technique in the presence of poisoned data: The obtained results show the decrease of specificity for each technique when poisoned data were tested. The presence of noise affects the ability of the algorithms to correctly identify healthy voices.

III.PROPOSED WORK

A. Proposed system

The proposed system takes health care data sets and examines them for data poisoning. The data set taken is the heart disease prediction dataset taken directly from the patients in the hospitals. The data sets can be tainted by the external intruders or can also be incorrectly entered. So, a machine learning algorithm named Bayesian Neural Network (BNN) is used for the detection of data poisoning. After the process of detection, the non-poisoned data sets are used for further examination using some of the ML techniques such as Logistic Regression, Support Vector Machine (SVM) and Random Forest. Then the accuracy of all the algorithms are calculated. The algorithm with the best level of accuracy will be researched further.

B. Modules of the project

The following tasks are performed in this project:

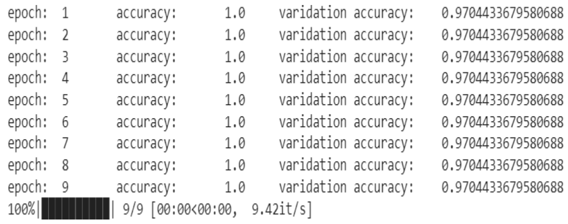
- Choosing a data set
- Removing data poisoning
- Pre-processing of the data set
- Choosing various ML algorithms
- Test-Train split
- Training the model
- Testing the model
- Performance Evaluation

C.Choosing a data set

With 17.9 million deaths per year, or 31% of all deaths worldwide, cardiovascular diseases (CVDs) are the leading cause of death worldwide. Heart attacks and strokes account for four out of every five CVD deaths, and one-third of these deaths happen before the age of 70. Heart failure is a frequent complication of CVDs, and this dataset comprises 14 variables that might be used to anticipate the development of a potential heart condition. A machine learning model can be very helpful in the early detection and management of people with cardiovascular disease or who are at high cardiovascular risk (due to the presence of one or more risk factors like hypertension, diabetes, hyperlipidaemia, or already established disease). This dataset is multivariate, which refers to multivariate numerical data analysis that provides or incorporates a number of distinct mathematical or statistical variables. Age, sex, type of chest pain, resting blood pressure, serum cholesterol, fasting blood sugar, resting electrocardiographic results, maximum heart rate reached, exercise-induced angina, old peak— ST depression caused by exercise compared to rest, slope of the peak exercise ST segment, number of major vessels, and Thalassemia are the 14 attributes that make up this factor. There are 76 attributes in this database, but only a subset of 14 of them are used in all published studies. Researchers studying machine learning have only ever used the Cleveland database. One of the main tasks on this dataset is to predict whether a patient has a heart condition based on the given attributes of the patient, and another is the experimental task to diagnose and find out different insights from this dataset which could help in understanding the problem more.

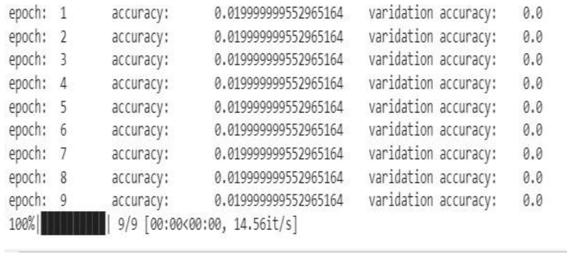
D.Removing data poisoning

Attacks that introduce malicious training samples to skew the results of tests jeopardize the integrity of machine-learning models. Bayesian Neural Networks have been used to remove data poisoning from the data set that is employed. It helps in discovering a probability distribution over potential neural networks using Bayesian inference. With a small adjustment to conventional neural network tools, it is useful in solving the inference problem. In order to prevent over-fitting, Bayesian neural networks (BNNs) are standard neural networks that have been extended with posterior inference. This BNN algorithm has been trained using mean-field variational inference to determine the level of prediction uncertainty. Clean samples are distinguished from poisoned samples using the uncertainty estimates from these methods. When determining the chance that any one of a number of potential known causes contributed to an event that already happened, Bayesian networks excel. A Bayesian network, for instance, could depict the probability connections between diseases and symptoms. Bayesian Neural network has been applied in the chosen correct and corrupted data sets and the accuracy of the datasets have been calculated. In the below given Fig.3a, the accuracy of the dataset is high. In Fig.3b, the accuracy of the dataset is low. Therefore, the dataset that has high accuracy is the correct dataset and the data set that has the lower accuracy is the corrupted dataset.



```
epoch:  1      accuracy:      1.0    varidation accuracy:    0.9704433679580688
epoch:  2      accuracy:      1.0    varidation accuracy:    0.9704433679580688
epoch:  3      accuracy:      1.0    varidation accuracy:    0.9704433679580688
epoch:  4      accuracy:      1.0    varidation accuracy:    0.9704433679580688
epoch:  5      accuracy:      1.0    varidation accuracy:    0.9704433679580688
epoch:  6      accuracy:      1.0    varidation accuracy:    0.9704433679580688
epoch:  7      accuracy:      1.0    varidation accuracy:    0.9704433679580688
epoch:  8      accuracy:      1.0    varidation accuracy:    0.9704433679580688
epoch:  9      accuracy:      1.0    varidation accuracy:    0.9704433679580688
100%|██████████| 9/9 [00:00<00:00,  9.42it/s]
```

Fig.3a Correct dataset accuracy



```
epoch:  1      accuracy:      0.019999999552965164   varidation accuracy:   0.0
epoch:  2      accuracy:      0.019999999552965164   varidation accuracy:   0.0
epoch:  3      accuracy:      0.019999999552965164   varidation accuracy:   0.0
epoch:  4      accuracy:      0.019999999552965164   varidation accuracy:   0.0
epoch:  5      accuracy:      0.019999999552965164   varidation accuracy:   0.0
epoch:  6      accuracy:      0.019999999552965164   varidation accuracy:   0.0
epoch:  7      accuracy:      0.019999999552965164   varidation accuracy:   0.0
epoch:  8      accuracy:      0.019999999552965164   varidation accuracy:   0.0
epoch:  9      accuracy:      0.019999999552965164   varidation accuracy:   0.0
100%|██████████| 9/9 [00:00<00:00, 14.56it/s]
```

Fig.3b Corrupted dataset accuracy

E. Pre - processing of the data set

Preparing raw data to be acceptable for a machine learning model is known as data preparation. In order to build a machine learning model, it is the first and most important stage. It is not always the case that there is clean and prepared data when developing a machine learning project. Additionally, any time when working with data, it must be cleaned and formatted. Therefore, data pre - processing activity can be used for this. The dataset has been collected from the Kaggle repository.

F. Data visualization

When working with data, it can be challenging to fully comprehend the data if it is just presented in tabular form. The data must be visualized or represented visually in order to fully comprehend what it means, to properly clean it, and to choose the best models for it. This makes patterns, correlations, and trends more obvious that cannot be seen in data that is presented as a table or CSV file. Data visualization is the act of using visual representations of our data to identify trends and relationships. So, a variety of Python data visualization libraries, such as Matplotlib, Seaborn, etc., can be used to do data visualization. In the below given Fig.3c, it indicates the heart disease ratio in the data set. The blue colour graph indicates that there is no heart disease and the orange colour graph shows that there is heart disease.In further, the target instance contains the values 0 and 1 which indicates that 0 shows that the person has no heart disease and 1 shows that the person has heart disease.

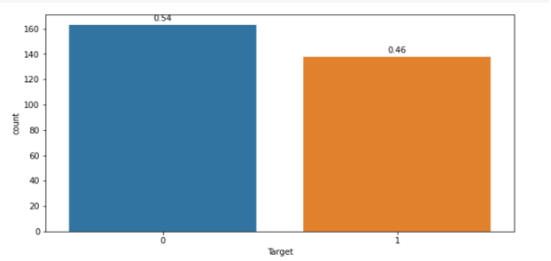


Fig.3c Data visualization of the whole dataset

The below shown Fig.5d indicates the disease probability bar plot in which the age of the person is considered as the most important factor for the plotting function.

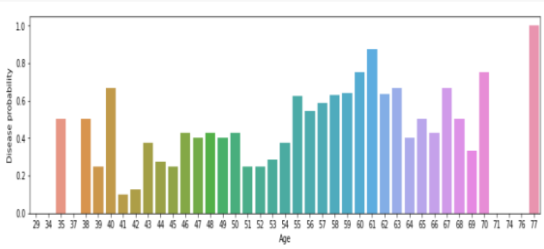


Fig.3d. Disease probability vs Age

The collected data set contains two different sorts of data as categorical data and numerical data. Therefore, the data's can be plotted as:

- Categorical Plot for categorical data
- Continuous plot for Numerical Data

1) *Categorial Plot:*

Categorical variables represent different sorts of data that can be categorised. Race, sex, age, and educational level are a few examples of categorical variables. In the collected data set, there are two attributes namely Chest Pain and Thal in which they are further classified. Chest Pain is further classified into four types as:

- typical
- nontypical
- nonangial
- asymptotic

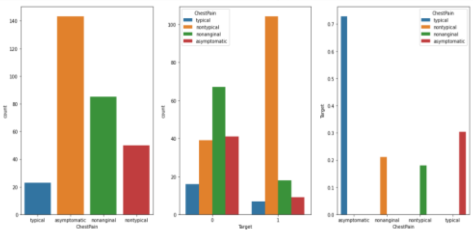


Fig.3e Chest pain bar plot

Thalassemia, a blood disorder is further classified into three types as:

- Value 0: NULL (dropped from the dataset previously)
- Value 1: fixed defect (no blood flow in some part of the heart)
- Value 2: normal blood flow
- Value 3: reversible defect (a blood flow is observed but it is not normal)

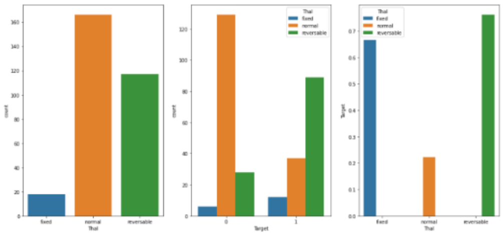


Fig.3f Thalassemia bar plot

2) *Continuous plot:*

The values that can be measured and organized logically are represented by numerical data. Height, weight, age, number of movies watched, IQ, and other numerical data are examples. The numerical data from the collected data set is age, sex (since the data set has 0 for female and 1 for male), cholesterol, RestBP, RestECG, fbs (The person's fasting blood sugar (> 120 mg/dl, 1 = true; 0 = false)), Slope (the slope of the peak exercise ST segment — 0: downsloping; 1: flat; 2: upsloping), ca(The number of major vessels (0–3)). They are plotted as continuous plot in which the graph obtained is similar to the ECG in the hospitals.

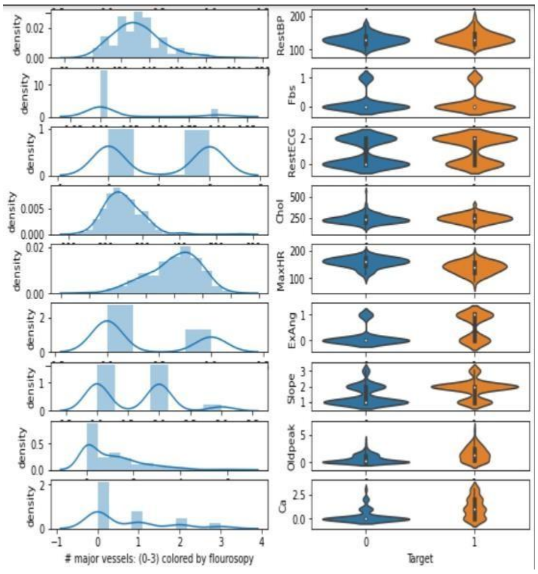


Fig.3g. Continuous plot

G. Machine learning

In the actual world, one who is surrounded by people is able to learn from their experiences thanks to their capacity for learning, and there are also computers or other robots that carry out our orders. So machine learning can be used for learn from past experiences. Machine learning is a modern innovation that has improved a wide range of industrial and professional procedures, as well as our daily lives. It is a subfield of artificial intelligence (AI) that focuses on developing intelligent computer systems that can learn from available databases using statistical approaches. Machine learning algorithms create a mathematical model with the aid of historical sample data, or "training data," that aids in making predictions or judgments without being explicitly programmed. Computer science and statistics are used with machine learning to create prediction models. Algorithms that learn from past data are created by machine learning or used in it. The performance will be higher the more information supplied.

H. Choosing various ml algorithms

For the purpose of calculating accuracy in the proposed system, various methods have been examined. The algorithm that produces the highest degree of accuracy will be chosen as the best algorithm for computing patient information in the medical profession. The three algorithms that have chosen are:

- Logistic Regression
- Support Vector Machine
- Random Forest

1) Logistic regression:

One of the most often used Machine Learning algorithms, within the category of Supervised Learning, is logistic regression. Using a predetermined set of independent factors, it is used to predict the categorical dependent variable. In a categorical dependent variable, the output is predicted via logistic regression. As a result, the result must be a discrete or categorical value. Rather than providing the exact values of 0 and 1, it provides the probabilistic values that fall between 0 and 1. It can be either Yes or No, 0 or 1, true or false, etc. One of the most often used Machine Learning algorithms, within the category of Supervised Learning, is logistic regression. Using a predetermined set of independent factors, it is used to predict the categorical dependent variable.

2) Support vector machine:

One of the most well-liked algorithms for supervised learning is called the Support Vector Machine (SVM), and it is used to solve both classification and regression issues. It is largely utilized in Machine Learning Classification issues, though. The SVM algorithm's objective is to establish the best decision boundary or line that can divide n-dimensional space into classes so that subsequent data points can be quickly assigned to the appropriate category. The term "hyperplane" refers to this optimal decision boundary.

3) Random Forest:

An effective supervised learning method is Random Forest, a well-known machine learning algorithm. Both Classification and Regression issues in ML can be solved with it. It is based on the idea of ensemble learning, which is the act of integrating different classifiers to address a complicated issue and enhance the performance of the model. Instead of depending on a single decision tree, the random forest takes the prediction from each tree and guesses the result based on the predictions that have received the most votes. An increase in accuracy and a solution to the overfitting issue are provided by the larger number of trees in the forest.

I. Test train split

The training dataset and testing dataset split is done by assigning 20 percent of the dataset in test set and 80 percent in training set. This is done to ensure maximum availability of training set that in turn increases accuracy of the model. Randomization of the whole dataset is essential before carrying out the split.

J. Experimental analysis

1) Environmental setup

In the existing system, Google colab have been used. The input is given in the form of CSV file. Firstly, connect the runtime to enable browsing. Click on "Choose Files" and then select the file to upload. Then wait for the file to be 100% uploaded. After uploading the file name will be displayed. Then copy the path of the CSV file and set it as a parameter to the read_csv() in pandas to get the data frame.

2) Implementation

The uploaded dataset is first analysed using a Bayesian Neural Network to determine whether or not it has been poisoned. The accuracy will be high if the data set is correct. The accuracy will be low if the data set is tainted. The data set is then pre-processed. As a result, the null values are eliminated. In addition, the data set is being visualised. The shown data set depicts the prediction of heart disease. The data set is then examined using machine learning methods such as Logistic Regression, Support Vector Machine, and Random Forest. The accuracy of the algorithms is determined, as is the cross validated accuracy of all three algorithms. Since the highest accuracy producing algorithm is Support vector machine, this algorithm is chosen as the best algorithm and can be used for further study.

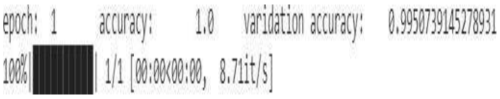
IV.RESULTS AND DISCUSSION

A. Simulation setup

A time - varying description of certain behaviour of the natural system as computed by the mathematical model. Simulation is a group of techniques that employ computers to emulate the various tasks in the real world.

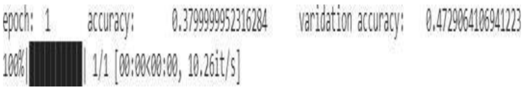
B. Dataset

The 303 instances and 14 attributes in the obtained data set is the heart disease prediction dataset. The original medical records that were retrieved from the hospitals with the aid of United Health Organizations are included in the data collection. Age, Sex, Chest Pain, RestBP, Chol, Fbs, RestECG, MaxHR, ExAng, Oldpeak, Slope, Ca, Thal and Target are the attributes in the data collection. The only categorical data are ChestPain and Thal whereas all the other values are numerical.



```
epoch: 1     accuracy:     1.0    varidation accuracy:    0.9950739145278931
100%|██████| 1/1 [00:00<00:00,  8.71it/s]
```

Fig.4a. Accuracy before data poisoning using BNN



```
epoch: 1     accuracy:     0.379999952316284    varidation accuracy:   0.472906410694122З
100%|██████| 1/1 [00:00<00:00, 10.26it/s]
```

Fig.4b. Accuracy after data poisoning using BNN

C.Performance metrics

A model approval is allowed to as the interaction where a prepared model is assessed with a testing informational index. The testing informational index is a different pair of similar informational collection from which the preparation set is derived. The reason for model approval is to check the accuracy and execution of the model in light of the past information. Metrics considered for evaluation are:

- Accuracy
- Precision
- F1 Score
- Specificity
- Sensitivity

1) Confusion Matrix:

The performance of the classification models for a certain set of test data is evaluated using a matrix called the confusion matrix. Only after the true values of the test data are known can it be determined. Although the matrix itself is simple to understand, some of the terminology used in connection with it might be. It is also referred to as an error matrix since it displays the errors in the model performance as a matrix. Confusion Matrix is a useful machine learning method which can be used to measure Recall, Precision, Accuracy, and AUC-ROC curve.

2) Precision:

Precision is defined as the ratio of correctly classified positive samples TP - True Positive to a total number of classified positive samples (either correctly or incorrectly). The precision measures the model's accuracy in classifying a sample as positive. Precision and recall are performance metrics used for pattern recognition and classification in machine learning.

Precision = True Positive / (True Positive + False Positive)(i)

3) Sensitivity:

Sensitivity is a metric that evaluates the quantity of right certain expectations made from all positive predictions that might have been made. Dissimilar precision that main remarks on the correct positive expectations out of every single positive forecast, Sensitivity gives a sign of missed positive expectations. Equation (ii) portrays the sensitivity as the proportion of genuine true positives and the addition of genuine true positive and genuine false negative.

Sensitivity = True Positives / (True Positives + False Negatives)

4) F1 Score:

The F1-score, is a proportion of a model's exactness on a dataset. The F1-score is an approach to consolidating the precision and recall of the model, and it is characterized as the consonant mean of the model's precision and recall. Hence, this score considers both misleading false positives and bogus false negatives. Naturally it isn't as straightforward as Accuracy, yet F1 is typically more valuable than exactness, particularly assuming that there is an unevenly distributed class. Equation (iii) depicts the F1 score as two times the proportion of duplication of precision and recall to the addition of precision and recall.

F1 Score = 2 * ((Precision * Recall) / (Precision + Recall)) (iii)

6) Specificity:

Specificity is characterized as the proportion of real negatives, which got anticipated as the genuine true negative. This suggests that there will be one more extent of real regret, which got anticipated as sure and could be named as false positives is known as a misleading positive rate. Equation (iv) portrays the sum of specificity and misleading positive rate would be 1 all the time. The higher Specificity of the model indicates that the model correctly identifies most of the negative results.

Specificity = True Negatives / (True Negatives + False Positives)

7) Accuracy:

Accuracy is perhaps the best-known Machine Learning model validation method used in evaluating classification problems. Accuracy is a metric that generally describes how the model performs across all classes. It is useful when all classes are of equal importance. It is calculated as the ratio between the number of correct predictions to the total number of predictions. One reason for its popularity is its relative simplicity. It is easy to understand and easy to implement. Accuracy is a good metric to assess model performance in simple cases.

Accuracy = ((TP + TN) / (TP + TN + FP + FN))

8) Cross validated Accuracy:

Cross-validation (CV) is a method for evaluating and testing the efficacy of a machine learning model (or accuracy). CV is commonly used in applied ML tasks. It entails setting aside a particular sample from a dataset on which the model has not been trained. Later, this sample is used to test the model and assess it.

V CONCLUSION

The ultimate objective of the project is to predict whether the dataset is poisoned or not, after the model has been developed and tested using the collected data. It will use a range of machine learning models to accomplish this and determine which algorithm offers the highest level of accuracy. As the only cause of death for more than 25% of people, heart disease must be anticipated. The patient's health can be improved if the disease is treated or additional therapies are given if it is identified in advance. With the three methods Support Vector Machine, Random Forest, and Logistic Regression, the data set has been trained and tested. Accuracy, a confusion matrix, and cross-validated accuracy have all been calculated as performance metrics. Support Vector Machine, with a 0.89% accuracy rate, is the most accurate machine learning algorithm. Therefore, this algorithm is deemed to be the greatest algorithm since it runs more quickly and provides greater accuracy, both of which can be used by doctors in the medical sector to conduct additional research or analysis on the heart illness of their patients. The project's future work could involve employing the most accurate and well-tested algorithm, support vector machine, in the field of medicine, where it could be applied immediately after gathering patient data from hospitals and provide a quick prediction of whether the patient would be affected by the heart disease or not.

VI REFERENCES

[1] Laura Verde, Fiammetta Marulli, Stefano Marrone, Exploring the Impact of Data Poisoning Attacks on Machine Learning Model Reliability, Procedia Computer Science, Volume 192, 2021, Pages 2624-2632, ISSN 1877-0509, https://doi.org/10.1016/ j.procs.2021.09.032.

[2] Fahri Anıl Yerlikaya, Şerif Bahtiyar, Data poisoning attacks against machine learning algorithms, Expert Systems with Applications, Volume 208, 2022, 118101, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2022.118101.

[3] Raghavan, V., Mazzuchi, T. & Sarkani, S. An improved real time detection of data poisoning attacks in deep learning vision systems. Discov Artif Intell 2, 18 (2022). https://doi.org/10.1007/s44163-022-00035-3

[4]M. Jagielski, A. Oprea, B. Biggio, C. Liu, C. Nita-Rotaru and B. Li, "Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning," 2018 IEEE Symposium on Security and Privacy (SP), 2018, pp. 19-35, doi: 10.1109/SP.2018.00057.

[5]M. Aladag, F. O. Catak and E. Gul, "Preventing Data Poisoning Attacks By Using Generative Models," 2019 1st International Informatics and Software Engineering Conference (UBMYK), 2019, pp.1-5, doi: 10.1109/UBMYK48245.2019.8965459.

[6] Dunn, Corey & Moustafa, Nour & Turnbull, Benjamin. (2020). Robustness Evaluations of Sustainable Machine Learning Models Against Data Poisoning Attacks in the Internet of Things. Sustainability. 12. 6434. 10.3390/su12166434.

[7] Ahmed, Ibrahim & Kashmoola, Manar. (2021). Threats on Machine Learning Technique by Data Poisoning Attack: A Survey. 10.1007/978-981-16-8059-5_36.

[8] Al-Dhief, F.T., Latiff, N.M.A., Malik, N.N.N.A., Salim, N.S., Baki, M.M., Albadr, M.A.A., Mohammed, M.A., 2020. A survey of voice pathology surveillance systems based on internet of things and machine learning algorithms. IEEE Access 8, 64514–64533.

[9] Amir, O., Wolf, M., Amir, N., 2007. A clinical comparison between mdvp and praat softwares: is there a difference, in: Fifth International Workshop on Models and Analysis of Vocal Emissions for Biomedical Applications, ISCA, Firenze University Press. pp. 37–40.

[10] Boyanov, B., Hadjitodorov, S., 1997. Acoustic analysis of pathological voices. a voice analysis system for the screening of laryngeal diseases.IEEE Engineering in Medicine and Biology Magazine 16, 74–82.

[11] Aghakhani, H., Eisenhofer, T., Schonherr, L., Kolossa, D., ¨ Holz, T., Kruegel, C., and Vigna, G. Venomave: Cleanlabel poisoning against speech recognition. arXiv preprint arXiv:2010.10682, 2020a.

[12] Boersma, P., Weenink, D., 2009. Praat: doing phonetics by computer (version 5.1. 05)[computer program]. retrieved may 1, 2009