



Data Breach

Team:

Sree Vandana | Swetha



About Project & Objective

- We did an implementation project on Credit card fraud Detection. Our goal was to built a model that could classify if a credit card transaction is fraudulent or not. For this we used machine learning algorithms.
- Our main objective is to focus our attention on ***identifying whether a breach occurred or not using a model creating by ML Algorithms and analyze different Algorithms and their performance.***
- “It’s important to identify a Breach in early stages, as the damaging effect increase as the time to identify them increase”

Identifying a Breach is an Important Step

- “Prevention is better than cure”. But data breaches are something unavoidable, even the most secured networks are hacked. Hackers are finding new sophisticated ways to breach the network and steal the data. In this case we say, making everything ready for treatment is a smart move. And Identification is the next immediate step that need to be focus on, after a breach.



Commonality of Data breaches

- We, are **surrounded by data breaches**. And we might be a **victim** of one and not even know about it. And this is more scary to not even realise what is happened to us
- Data breaches are more common than we think they are.
- “One massive hack after another,” this statement would probably best describe what’s happening around.



The Breach Collection Of 2020



Health Share of Oregon

February 13, 2020: The theft of an employee laptop from GridWorks IC, a third-party vendor of Health Share of Oregon, has exposed the personal and medical information of **654,000** members. The Health Share of Oregon data breach disclosed sensitive data, including names, addresses, phone numbers, dates of birth, Social Security numbers, and Medicaid ID numbers.

November 18, 2019



T-Mobile

March 5, 2020: An **one million** number of customers' sensitive information was accessed through a T-Mobile employee email account after a malicious attack of a third-party email vendor. The personal information of T-Mobile customers accessed includes names and addresses, Social Security numbers, financial account information, and government identification numbers, as well as phone numbers, billing and account information, and rate plans and features.



zoom

April 14, 2020: The credentials of over **500,000** Zoom teleconferencing accounts were found for sale on the dark web and hacker forums for as little as \$.02. Email addresses, passwords, personal meeting URLs, and host keys are said to be collected through a credential stuffing attack.

All these data breach examples are from newspapers and news articles, all these are recorded breaches but there are many breaches that are unidentified. (Companies might not know about the breach or might do this deliberately to save their reputation)

Effects Of Data Breach.




Impact

The impact of breach currently is much more damaging when compared to breaches previously.

Now a single breach can affect millions, even billions of people and multiple organisations.

Whenever a breach occurs, not only one individual is affected. Infact every entity surrounding that data will be affected which includes the individual to whom the data belongs, the organisation which stores the data, the third-part vendors or company partners etc.



Data breaches hurt individuals by compromising sensitive information, which can often lead to headaches: changing passwords frequently, enacting credit freezes or identity monitoring, and so on. Sometimes these damages can hit us for a long time.

In terms of an organisation the most damaging after-effects of the breach are Financial Losses, Reputational loss, Operational disruption, Intellectual Property loss and legal ramifications. Perhaps the biggest long-term consequence of a data breach is the loss of customer trust.

Identifying The Breach




Its Difficult

The effects of data breach can be damaging, their impact on victims, their cost, misuse of information and much more.

Which makes it an utmost necessity for us to identify it. But How?

We say a breach occurred, when we know that it occurred. But most of these breaches are unidentified for a long time.

And at the time of discovery of these breaches the damages have already happened.



All the breaches we mentioned or appeared in the news are recorded breaches.

There are many breaches which are unidentified and unrecorded (unknowingly or intentional)

So identification of the breaches becomes important. A tool is required to reduce the damaging effects of a breach. (might not prevent a breach from happening. But could reduce the after effects.)

Credit Card Fraud Detection.

We tried to automate the process of identifying the breach using ML Algorithms.



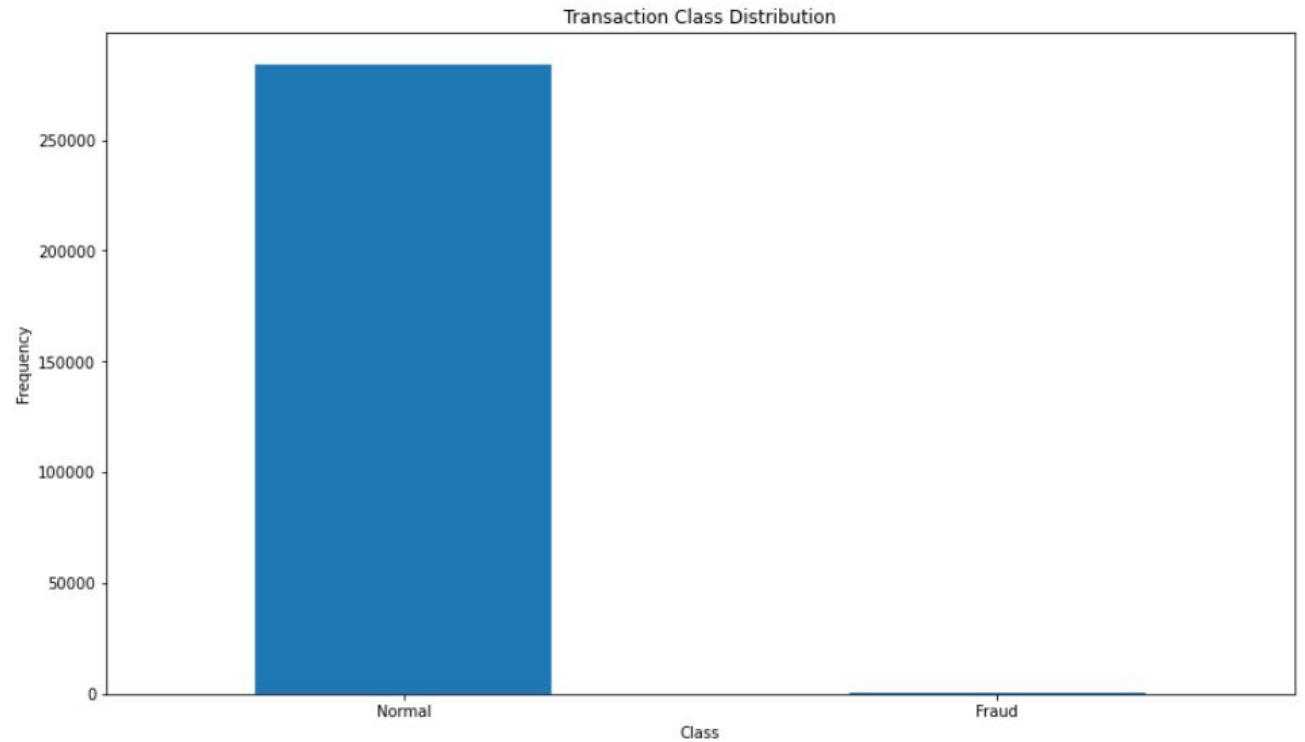
Overview Of Data Set

The datasets contains credit cards transactions that occurred in two days, which have 492 frauds out of 2,84,807 transactions.

The dataset provided in kaggles are the result of PCA transformation which generated Features V1, V2, ... V28 (to protect the original data and the only features which have not been transformed with PCA are 'Time' and 'Amount').


```
Fraud --> class = 1  
(492, 31)  
Normal --> class = 0  
(284315, 31)
```

Out[7]: Text(0, 0.5, 'Frequency')

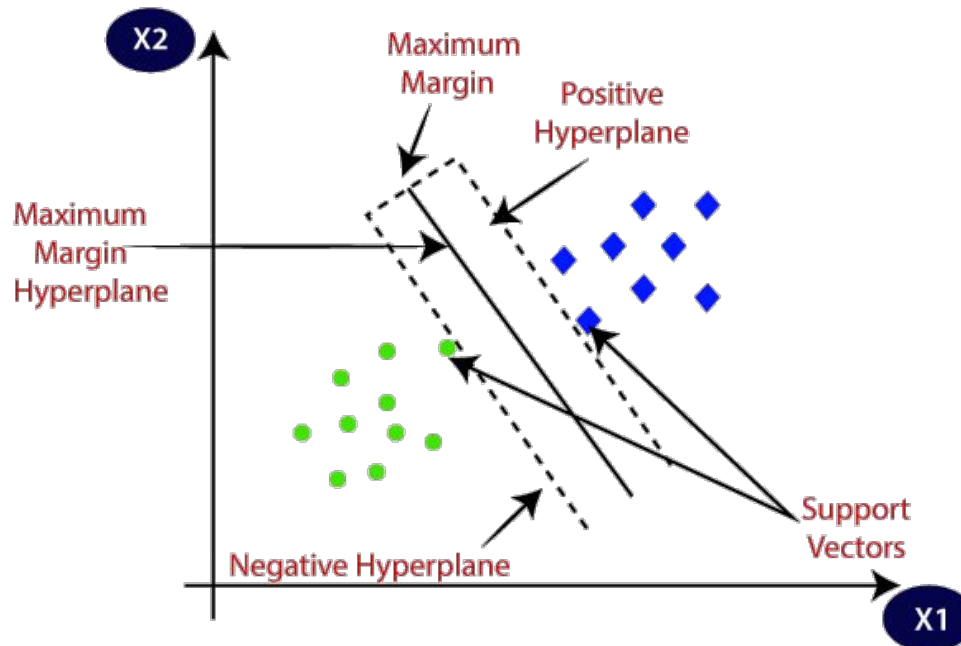




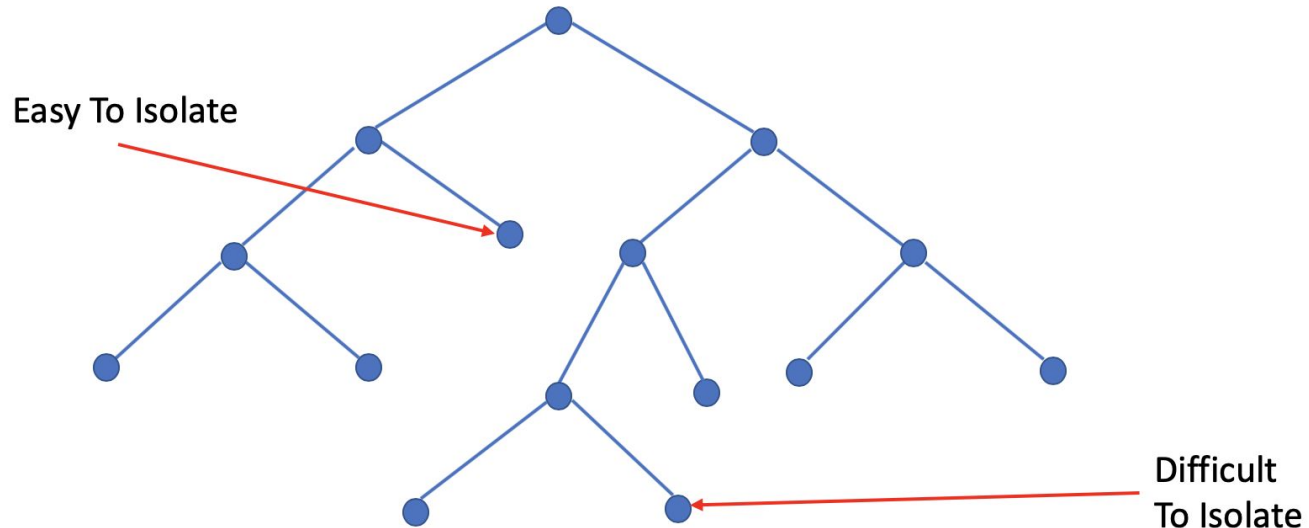
Choosing A Model

1. SVM (Support vector Machine)
2. Isolated Forest
3. Logical Regression

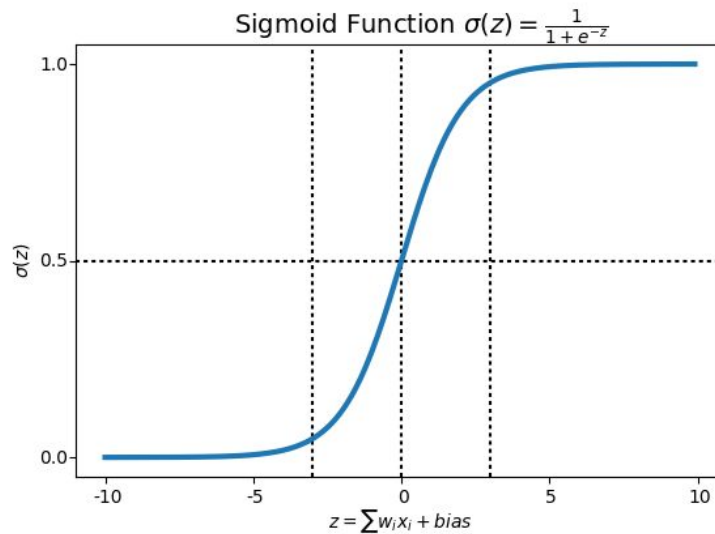
1. SVM (Support vector Machine)



2. Isolated Forest



3. Logical Regression



Performance of the models



Methods to Analyze The Performance of the Models

We cannot use Accuracy of the model's prediction to determine the models performance as this is highly imbalanced data set.

So we are going to use

1. Precision
2. Recall
3. F1 score



Definitions

1. **Precision:** Precision is the ratio of correctly predicted positive observations to the total predicted positive observations.
(it is the measure of correctness, measure of correctly identified observations from total Observations).

$$\text{Precision} = \text{TP} / \text{TP} + \text{FP}$$

2. **Recall:** Recall is the ratio of correctly predicted positive observations to the all observations in actual class
(It is a measure of correctly identified positive cases from all the actual positive cases)

$$\text{Recall} = \text{TP} / \text{TP} + \text{FN}$$

3. **F1 Score:** F1 Score is the weighted average of Precision and Recall.
(it is like a Harmonic mean of precision and recall).

$$\text{F1 Score} = 2 * (\text{Recall} * \text{Precision}) / (\text{Recall} + \text{Precision})$$

1. SVM (Support vector Machine)

Support Vector Machine: 8516

Accuracy Score :

0.7009936448860644

Classification Report :

	precision	recall	f1-score	support
0	1.00	0.70	0.82	28432
1	0.00	0.37	0.00	49
accuracy			0.70	28481
macro avg	0.50	0.53	0.41	28481
weighted avg	1.00	0.70	0.82	28481



2. Isolated Forest

Isolation Forest: 73

Accuracy Score :

0.9974368877497279

Classification Report :

	precision	recall	f1-score	support
0	1.00	1.00	1.00	28432
1	0.26	0.27	0.26	49
accuracy			1.00	28481
macro avg	0.63	0.63	0.63	28481
weighted avg	1.00	1.00	1.00	28481



3. Logical Regression

Logistic Regression:

Accuracy: 99.92 %

	precision	recall	f1-score	support
0	1.00	1.00	1.00	56892
1	0.63	0.91	0.75	70
accuracy			1.00	56962
macro avg	0.82	0.96	0.87	56962
weighted avg	1.00	1.00	1.00	56962

Observations & Conclusion.



Model Conclusion.

In our implementation project we compared, different types of models linear model(SVM), tree Structured model (Isolated Forest) and Mathematical probabilistic model (Logical regression) and analyzed their performance.

We can see that the mathematical probabilistic model worked well when compared to linear and tree structured model.

The linear model (SVM) is expected to fail, as the real world data is non-linear in fashion (mostly).



Links

1. Data Visualization Graphs & Project Code:
<https://github.com/Sree-Vandana/Data-Science/blob/master/ds%20final%20code.ipynb>
2. Research Paper for more details about Data Breach:
<https://github.com/Sree-Vandana/Data-Science/blob/master/DataBreach-ResearchReport.pdf>

Thank You :)