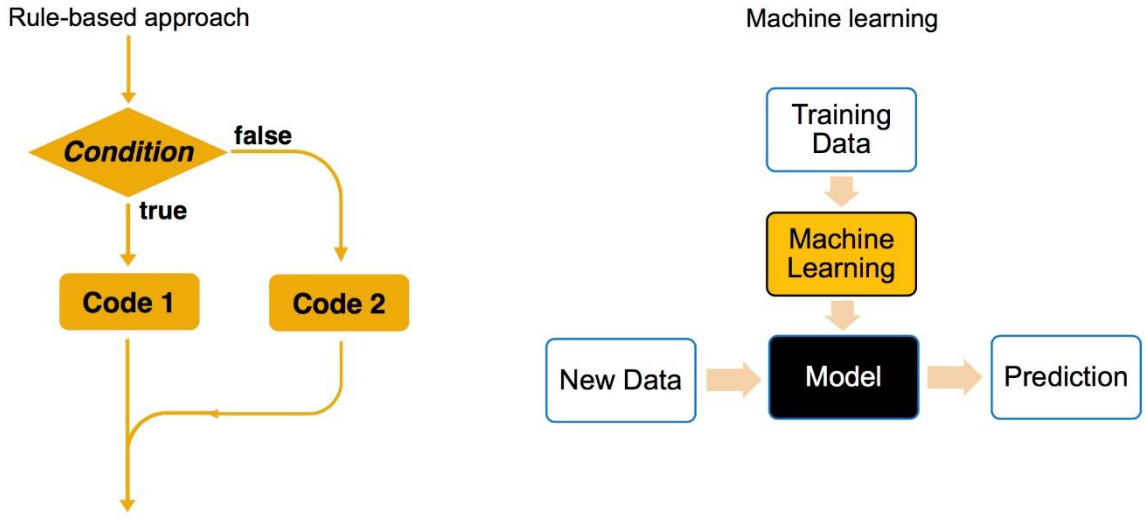
AI In Anti-Money Laundering Software (AML)

- Tanmay Pawar

1. Problem statement

Automate existing AML software by implementing ML and AI algorithms, and find the best model which accurately predicts/prevents suspicious financial transactions.

2. Market Need Assessment



The institutions' current approach is one that is focused on rules. The rule-based approach lays forth a set of standards or criteria that compliance officers can use to spot fraudulent transactions. Every financial institution keeps track of who has been involved in money laundering or who has broken their rules. This list is sometimes known as a sanction or watch list. If the following transaction does not comply with the regulations, the rule-based Anti-Money Laundering (AML) software will flag it. The compliance officer will then look into the

transactions that have been identified. This method has the advantage of making conclusions that are simple to comprehend. The rule-based approach has significant drawbacks, such as the need to introduce new rules to accommodate changes in money laundering patterns, and hence the inability to adapt to new patterns. Another disadvantage is that it makes extensive use of the bank's resources and is inefficient in terms of time. Because the negatives outnumber the benefits, this strategy must be modified to improve efficiency. As a result, it has become evident that the AML software must be automated.

3. Target Specification

AML stands for anti-money laundering software, which allows banks and other financial organizations to analyse customer data and spot questionable transactions. Transaction monitoring, customer identification authentication, and compliance management are all part of the process. Organizations can improve their security and operational efficiency by using systems that use AML software to filter information and deliver real-time alerts.

Anti-money laundering (AML) software is designed to help companies meet legal requirements to combat financial crime. Important features include the ability to monitor transactions, report currency transactions (CTR), customer identification, and compliance management.

This product is mainly designed for all banking institutions, primarily to enforce AML regulations.

4. External Search

- https://complyadvantage.com/insights/anti-money-laundering/anti-money-laundering-software/
- https://diceus.com/anti-money-laundering-in-banks/

- https://www.tcs.com/content/dam/tcs/pdf/Industries/Banking%20and%20Financial%
- **20Services/Anti-Money%20Laundering%20-%20Challenges%20and%20trends.pdf**
- https://menafn.com/1103898747/Anti-Money-Laundering-AML-Software-Solution-Market-Global-Outlook-Business-Opportunity-Upcoming-Trends-Recent-Development-Growth-Drivers-Strategy-Key-Players-Size-and-Forecast-2022-2031

5. Benchmarking

- HSBC

The AML system uses big data, analytics and contextual monitoring to “detect and disrupt crime in international trade”. It will combine bank data and external data like company ownership information to identify links between counterparties. According to HSBC, the software monitors all trade finance transactions against more than 50 different scenarios which indicate signs of money laundering. Using this technology, customer activities can be continuously assessed and scored for risk. This level of contextual monitoring improves accuracy, and decision making, while providing insight into data relationships never before possible

- SEON

SEON is becoming more popular as a compliance tool in the payments and iGaming industries, owing to its KYC capabilities. All of this is possible thanks to a robust real-time identity verification system based on alternative data checks like social media profiling. While SEON's fraud protection products aren't explicitly designed for AML compliance, they have enough features that many organisations utilise them to avoid regulatory fines. Integrations with other tools allow you to be notified of suspicious transactions, and custom rules offer you complete control over the flagging settings.

6. Applicable Patents

- Anti-money laundering system

Inventors: Yuh-Shen Song Catherine Lew Alexander Song Victoria Song

A computer system conducts transactional monitoring to detect different types of possible cases in order to prevent financial crimes and assist businesses to comply with different types of laws and regulations. The computer system derives a total risk score for each of a group of entities based on risk factors. Each of the risk factors is assigned a risk score. The computer system also detects an entity when the total risk score of the detected entity differs from a reference derived from total risk scores of the group of entities by a pre-determined margin. The computer system also assists a user to identify at least one transaction that has caused the detected entity to have a total risk score that differs from the reference derived from the total risk scores of the group of entities.

- Method and system to evaluate anti-money laundering risk

Inventors: Henry Grant, Jr. Tyler Reynolds

A method to evaluate anti-money laundering risk may include identifying a person or other legal entity to be evaluated. A country may be selected associated with the person or other legal entity. At least one financial product or financial instrument associated with the person or other legal entity may be selected. The method may also include selecting a customer type associated with the person or other legal entity. A risk rating may be determined based on responses to predetermined criteria related to the selected country,

the at least one selected financial product and the selected customer type.

7. AML Regulators in India

Financial Intelligence Unit - India (FIU-IND)

The Financial Intelligence Unit of India (FIU-IND) was established in 2004 by the Indian government to review and analyse suspicious financial transactions. The Financial Intelligence Unit of India (FIU-IND) is the organization responsible for the fight against the financial crimes of India under the Ministry of Finance. Businesses with AML obligations report to the Financial Intelligence Unit.

Reserve Bank of India (RBI)

Reserve Bank of India is the central bank of the Republic of India. It is responsible for the economic growth and economic stability of India. However, it also has some regulatory powers to prevent money laundering.

8. Applicable Constraints

Increased governance: Managing cross-border and multi-jurisdictional AML-compliance requirements, as well as ever-increasing client due diligence obligations, can be problematic for banks and financial institutions. Identifying beneficial ownership and implementing remedial procedures to resolve AML shortcomings discovered by regulatory examinations are both difficult tasks.

Lack of qualified staff: Finding qualified personnel with in-depth understanding of AML can be difficult. High onboarding durations and costs, as well as turnover, are further challenges. Organizations must also devote significant time and effort to keeping employees up to date on evolving regulatory standards.

Complicated processes and technology: AML compliance necessitates the implementation of a number of processes and technological solutions that will integrate KYC data and systems into a single repository. They must also build infrastructure for cross-channel detection of suspicious actions, increase data quality, and standardise data in order to conduct centralised fraud and financial crime analysis.

The risk level assigned during onboarding changes depending on the customer's transactions. To avoid false positives, banks must assess risks for each customer on a continuous basis and adjust risk levels accordingly. This demands ongoing transaction monitoring for each consumer, which is a huge undertaking.

9. Business Opportunity

The global anti-money laundering (AML) software solution industry is now experiencing strong growth as a result of an increase in money laundering cases around the world. Furthermore, the expanding technological development throughout the world, which includes the integration of IT technologies to increase an organization's operational efficiency, is expected to be a major factor driving the overall anti-money laundering market.

Over the projection period, the anti-money laundering (AML) software solution market is expected to grow at a CAGR of 16.0%. By 2027, it is expected to reach a market size of USD 3.5 billion. By the conclusion of the projection period, the anti-money laundering (AML) software solution market is predicted to be booming. The market is divided into three categories: deployment, kind, and industry end-use. It is divided into two categories based on deployment: on-premise and cloud. During the projected period, on-premise is expected to be the largest sub-segment. The cloud-based sub-segment, on the other hand, is expected to grow at the fastest rate during the projected period.

The increased adoption of cloud-based services by various businesses is expected to be a major factor driving the sub-growth. segment's Transaction monitoring systems, currency transaction reporting, customer identity management systems, and compliance management software are the different types of software. During the forecast period, transaction monitoring systems are expected to earn the most income.

The increased adoption of transaction monitoring systems by various financial institutions to lower the risk of money laundering is expected to be the primary driver of the sub-growth. segment's IT and telecommunications, healthcare, BFSI, transportation and logistics, manufacturing, defence and government, retail, energy and utilities, and others are the end-use industries. During the forecast period, the BFSI is expected to be the dominant sub-segment. The rising use of anti-money laundering (AML) technology in the financial services industry is expected to reduce money-related fraud.

10. **Concept Generation**

It is obvious in a materialistic world that money can buy everything. There are those who earn money legitimately by providing a service or running a business. However, some people prefer to gain money in an illegal manner and thereby disregard the law. These individuals engage in criminal activities such as drug trafficking, terrorist financing, and tax evasion, among others. By laundering the money, these criminals attempt to conceal unlawful funds and avoid the banking institutions' laws and regulations. Money laundering can be accomplished in a variety of methods, including dividing large sums of money into smaller transactions, converting into foreign currency, or investing in valuable items like diamonds or gold. As a result, the question remains as to how financial institutions detect and prevent illicit activities.

One strategy to combat money laundering through financial transactions is to force financial institutions to provide consumers with higher financial security before granting them credit. Money laundering prevention through financial institutions is simply one part of a larger strategy to combat financial crime. The adoption of anti-money laundering programmes around the world is another crucial step in the prevention of money laundering.

11. Concept Development

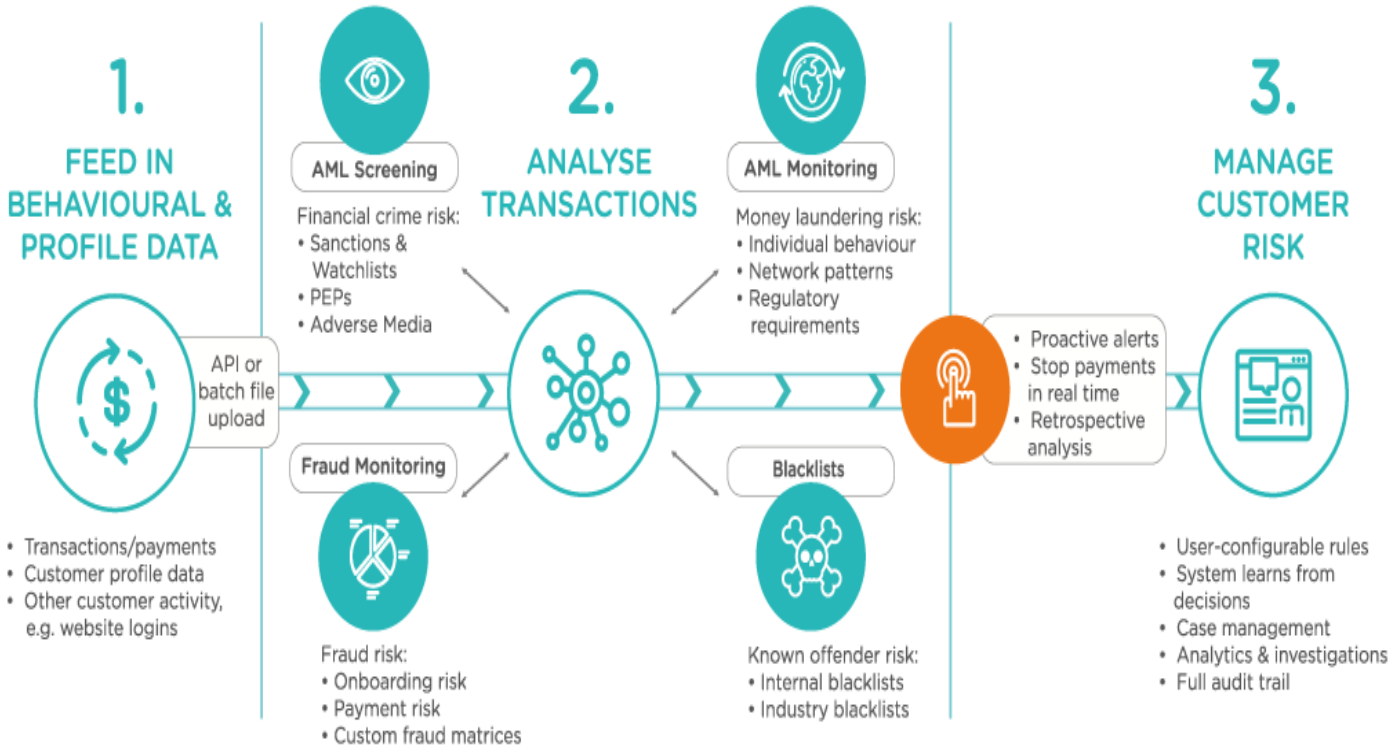
AML software performs the same function as human transaction monitoring, but it allows banks and financial institutions to automate their data analysis in real time and on an ongoing basis as part of their overall anti-money laundering/counter-terrorist financing programme. AML transaction monitoring software allows businesses to quickly and accurately build a comprehensive picture of their customers' financial behaviour, compare it to existing risk profiles, and even forecast future activity to determine whether customers pose a continuing money laundering or terror financing threat. When suspicious activity is found, transaction monitoring software can automatically notify AML teams and generate suspicious activity reports for the appropriate financial authorities.

While different platforms obviously vary in the functions and capabilities they offer, AML software tends to fall into four main categories:

- Name screening: Certain territories maintain ‘blacklists’ of high-risk customers and entities which financial institutions are prohibited from doing business with. Anti-money laundering software can be used to quickly identify blocked persons, and flag them to an institution. In addition to identifying sanctions, screening is also used to identify Politically Exposed Persons (PEPs), and individuals receiving adverse media attention.

- Transaction monitoring**:** This category of AML software focuses specifically on identifying suspicious patterns in customer transactions, using historical information and the specifics of certain account profiles. In the United States, AML software tasked with monitoring suspect transactions would be used to generate a Suspicious Activity Report (SAR) which would then be submitted to FinCen.
- Currency Transaction Reporting (CTR): Anti money laundering software can be used to spot transactions involving large amounts of cash, or multiple small transactions aggregating a large amount of cash. Under the Bank Secrecy Act, for example, transactions of over $10,000 would be flagged automatically.
- Compliance**:** Anti money laundering software can be used in the day-to-day implementation of compliance requirements. The data management capabilities of AML software can be used to keep detailed records of employee training and scheduled audits, and track reports submitted to financial authorities.

12. Product Prototype



Feed In Behavioural & Profile Data:

The first step of AML screening is to collect and organize the customer/transaction data. The transaction details, KYC, or other customer activities are collected. This process is usually fulfilled by the financial institutions. The data is then fed to AML software.

Analyse Transactions:

In this Phase we analyse the transactions on the given data and try to identify if a transaction possesses some risk. The model makes a decision based on the above conditions which include: Money Laundering risk, Fraud Risk, Financial Crime Risk and Known Offender Risk. So, to sum up this phase, the software does the following functions: AML monitoring and Screening, Fraud Monitoring and Backlist Screening.

Manage Customer Risk:

From the above phase, we get a clear understanding if the transaction possesses a risk or not. If the transaction is valid, then the software allows to transaction to proceed. If the transaction is flagged as fraud, then the transaction is blocked and given to a compliance officer for further screening. The model then can learn from the previous decisions to improve the accuracy of the model.

13. Product Details

- *Product Working Details*

  a. Monitoring Phase

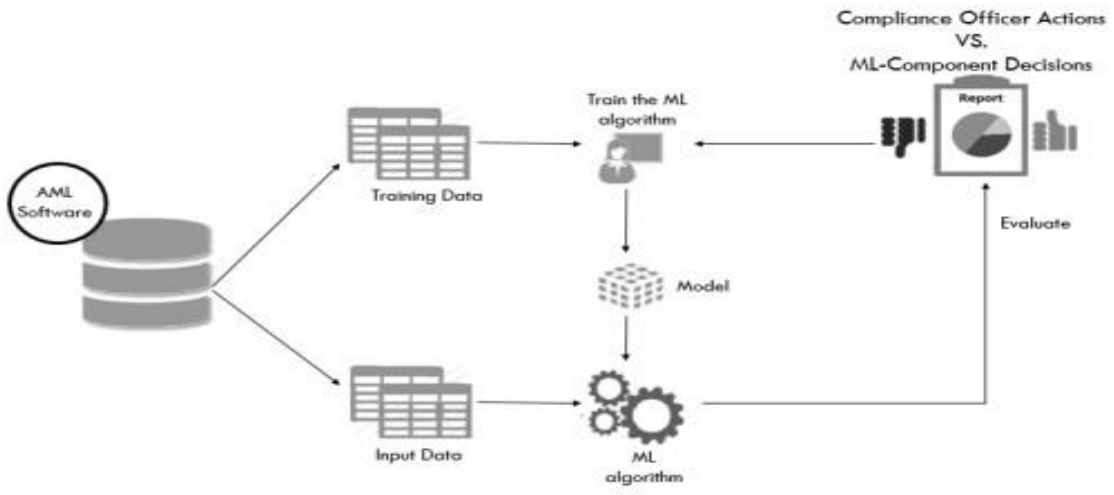


Fig 1. Monitoring Phase

The suggested ML-monitoring Component's phase is the first step, during which incoming transactions are silently monitored. Depending on the settings, the ML-Component will use a portion of the transactions as training data to tune the model. After that, it will try to predict the final conclusion for testing data (transactions) and save it in a separate database with the transaction ID. The system will generate a report that includes both the investigators and the ML-choices Component's for each transaction ID after the compliance officer makes decisions on the same test transactions.

b. Advising Phase

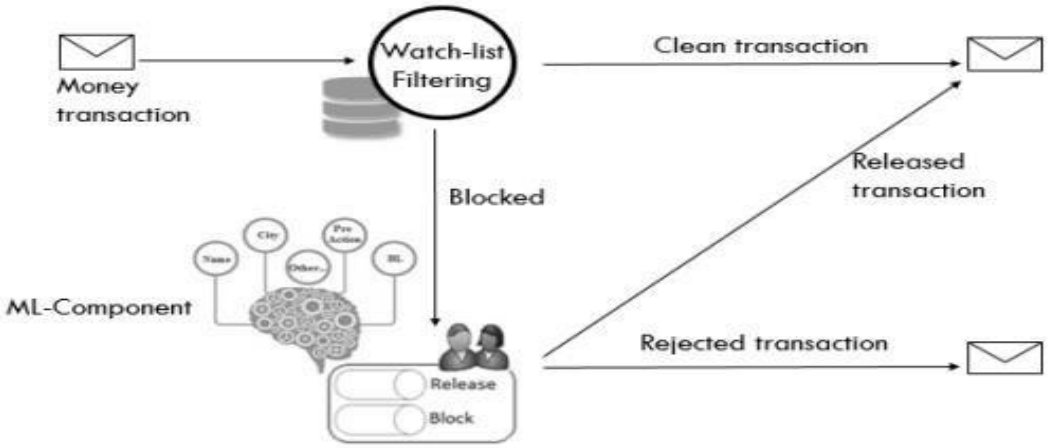


Fig 2. Advising Phase

After completing the first phase with an acceptable report indicating a perfect match between the ML-Component option and the compliance officer decision, it's time to reduce the investigative effort by putting the ML-Component into action. To limit compliance risk and monitor system behaviour, this will be done in stages so that the ML-Component does not issue a definitive decision on prohibited transactions. At this point, the ML-Component won't have entire control; it'll be able to make a decision, but it won't be the final one. As a result, human approval is necessary to finalize the transaction.

The watch-list filtering system can use the ML-Component to analyse pending transactions and offer suggestions on whether or not to release or reject blocked transactions. The system will shift the transactions to queues based on the component's recommended decision. This will reduce the amount of time the compliance officer spends investigating prohibited transactions. It will also shorten the time it takes to make a judgement, which may

result in penalties if there are a significant number of pending transactions in the queue for scrutiny.

c. Take-Action Phase

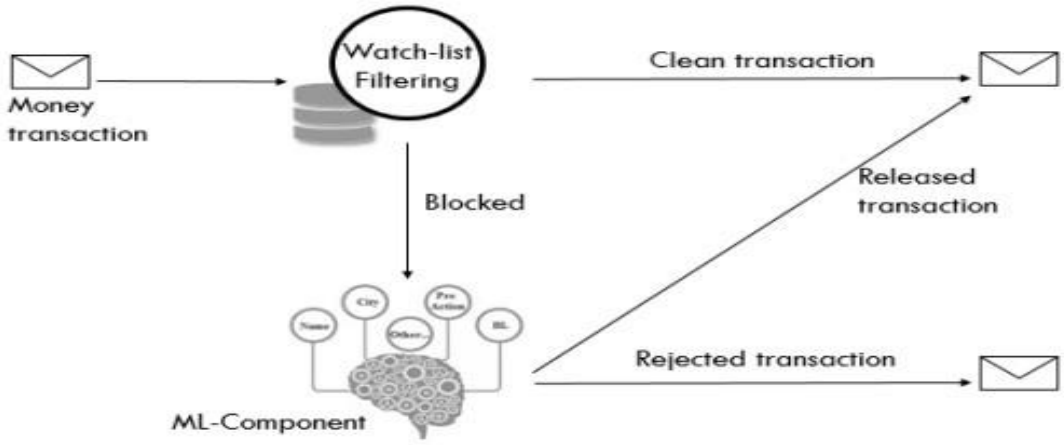


Fig 3. Take-Action Phase

In addition to the benefits of the second phase, this phase will lower the number of false positive and false-negative transactions. The ML-Component will make the final decision on whether to release or reject the blocked transaction. The compliance officer can also establish a set of rules for the system to follow, such as putting the transaction to the recommended decision queue to be manually handled. The watch-list filtering database contains a wealth of useful information, either about the transaction or the blacklisted entity it matched. While pre-processing the data set and testing the model, we can select the optimal fields to tune the ML-Component to the best conclusion. The financial transaction has a variety of data that may be used to construct the versions indicated above and fine-tune our ML-Component. Transaction information such as the sender reference,

ordering customer, and matched rank value will be used by the ML-Component.

- *Data Sources*

Every financial institution collects vast amount of data from customers that include their past and current transactions, their personal details and KYC details.

- *Algorithms*

a. Supervised Algorithms
   Decision Tree
   Random Forest
   SVM for Classification
b. Unsupervised and Deep Learning Algorithms
   K-Clustering
   ANN

- *Team Required*

   Financial Institutional Officers
   Compliance Officers
   ML Engineer
   Software Developer

14. Code Implementation (EDA)

jupyter Untitled Last Checkpoint: 14 minutes ago (unsaved changes)

Logout

File Edit View Insert Cell Kernel Widgets Help

Trusted | Python 3

Run Code

Dataset can be found at
https://www.kaggle.com/datasets/ealaxi/paysim1datasetId=1069&outputs=Visualization

In [2]:
```
import numpy as np
import pandas as pd
import seaborn as sns
import matplotlib.pyplot as plt
```

In [3]:
```
df = pd.read_csv("Transactions.csv")
df.head()
```

Out[3]:

	step	type	amount	nameOrig	oldbalanceOrg	newbalanceOrig	nameDest	oldbalanceDest	newbalanceDest	isFraud	isFlaggedFraud
0	1	PAYMENT	9839.64	C1231006815	170136.0	160296.36	M1979787155	0.0	0.0	0	0
1	1	PAYMENT	1864.28	C1666544295	21249.0	19384.72	M2044282225	0.0	0.0	0	0
2	1	TRANSFER	181.00	C1305486145	181.0	0.00	C553264065	0.0	0.0	1	0
3	1	CASH_OUT	181.00	C840083671	181.0	0.00	C38997010	21182.0	0.0	1	0
4	1	PAYMENT	11668.14	C2048537720	41554.0	29885.86	M1230701703	0.0	0.0	0	0

In [4]:
```
df.info() # Checking the dtypes of columns
```

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 6362620 entries, 0 to 6362619
Data columns (total 11 columns):
 #   Column          Dtype
---  ------          -----
 0   step            int64
 1   type            object
 2   amount          float64
 3   nameOrig        object
 4   oldbalanceOrg   float64
 5   newbalanceOrig  float64
 6   nameDest        object
 7   oldbalanceDest  float64
 8   newbalanceDest  float64
 9   isFraud         int64
 10  isFlaggedFraud  int64
dtypes: float64(5), int64(3), object(3)
memory usage: 534.0+ MB
```

jupyter Untitled Last Checkpoint: 14 minutes ago (unsaved changes)

Logout

File Edit View Insert Cell Kernel Widgets Help

Trusted | Python 3

Run Code

In [5]:
```
df.describe()
```

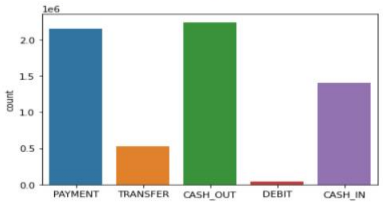
Out[5]:

	step	amount	oldbalanceOrg	newbalanceOrig	oldbalanceDest	newbalanceDest	isFraud	isFlaggedFraud
count	6.362620e+06	6.362620e+06	6.362620e+06	6.362620e+06	6.362620e+06	6.362620e+06	6.362620e+06	6.362620e+06
mean	2.433972e+02	1.798619e+05	8.338831e+05	8.551137e+05	1.100702e+06	1.224996e+06	1.290820e-03	2.514687e-06
std	1.423320e+02	6.038582e+05	2.888243e+06	2.924049e+06	3.399180e+06	3.674129e+06	3.590480e-02	1.585775e-03
min	1.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00
25%	1.560000e+02	1.338957e+04	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00
50%	2.390000e+02	7.487194e+04	1.420800e+04	0.000000e+00	1.327057e+05	2.146614e+05	0.000000e+00	0.000000e+00
75%	3.350000e+02	2.087215e+05	1.073152e+05	1.442584e+05	9.430367e+05	1.111909e+06	0.000000e+00	0.000000e+00
max	7.430000e+02	9.244552e+07	5.958504e+07	4.958504e+07	3.560159e+08	3.561793e+08	1.000000e+00	1.000000e+00

In [6]:
```
print(df.type.value_counts())
sns.countplot(x="type", data=df) # Count the number of each type of payment in dataset
```

```
CASH_OUT    2237500
PAYMENT     2151495
CASH_IN     1399284
TRANSFER     532909
DEBIT         41432
Name: type, dtype: int64
```

Out[6]:
```
<AxesSubplot:xlabel='type', ylabel='count'>
```



jupyter **Untitled** Last Checkpoint: 14 minutes ago (unsaved changes)

Logout

File Edit View Insert Cell Kernel Widgets Help

Trusted | Python 3

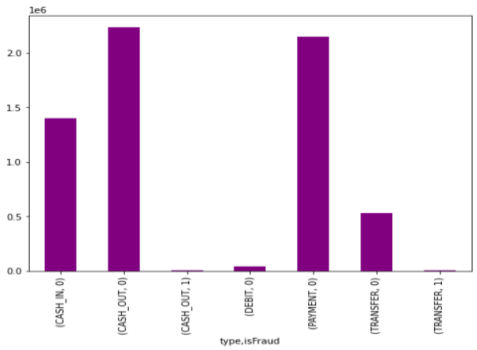
Run Code

PAYMENT TRANSFER CASH_OUT DEBIT CASH_IN

type

In [7]:
```
df.groupby(['type', 'isFraud']).size().plot(kind='bar',figsize=(8, 6), color='purple') # Count of each type of payment
                                                                                       # w.r.t isFraud coulumn
```

Out[7]: <AxesSubplot:xlabel='type,isFraud'>



In [9]:
```
df.groupby(['type', 'isFlaggedFraud']).size().plot(kind='bar',figsize=(8, 6), color='purple') # Count of each type of payment
                                                                                             # w.r.t isFlaggedFraud coulumn
```

Out[9]: <AxesSubplot:xlabel='type,isFlaggedFraud'>

jupyter **Untitled** Last Checkpoint: 14 minutes ago (unsaved changes)

Logout

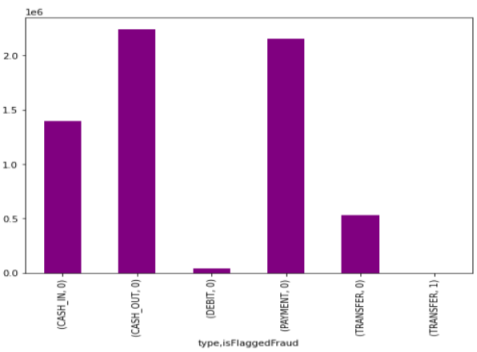
File Edit View Insert Cell Kernel Widgets Help

Trusted | Python 3

Run Code

In [9]:
```
df.groupby(['type', 'isFlaggedFraud']).size().plot(kind='bar',figsize=(8, 6), color='purple') # Count of each type of payment
                                                                                             # w.r.t isFlaggedFraud coulumn
```

Out[9]: <AxesSubplot:xlabel='type,isFlaggedFraud'>



In [8]:
```
# Increase the size of the heatmap.
plt.figure(figsize=(16, 6))
# Store heatmap object in a variable to easily access it when you want to include more features (such as title).
# Set the range of values to be displayed on the colormap from -1 to 1,
# and set the annotation to True to display the correlation values on the heatmap.
heatmap = sns.heatmap(df.corr(), vmin=-1, vmax=1, annot=True)
# Give a title to the heatmap. Pad defines the distance of the title from the top of the heatmap.
heatmap.set_title('Correlation Heatmap', fontdict={'fontsize':12}, pad=12);
```

Correlation Heatmap

jupyter Untitled Last Checkpoint: 14 minutes ago (unsaved changes)

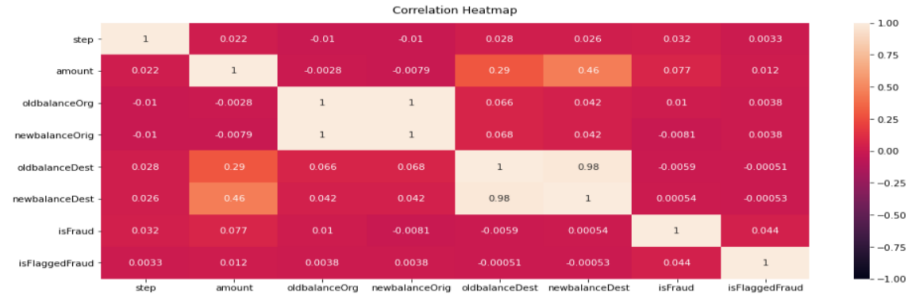
Logout

File Edit View Insert Cell Kernel Widgets Help

Trusted | Python 3

Run Code

In [8]:
```
# Increase the size of the heatmap.
plt.figure(figsize=(16, 6))
# Store heatmap object in a variable to easily access it when you want to include more features (such as title).
# Set the range of values to be displayed on the colormap from -1 to 1,
# and set the annotation to True to display the correlation values on the heatmap.
heatmap = sns.heatmap(df.corr(), vmin=-1, vmax=1, annot=True)
# Give a title to the heatmap. Pad defines the distance of the title from the top of the heatmap.
heatmap.set_title('Correlation Heatmap', fontdict={'fontsize':12}, pad=12);
```



In [ ]:

jupyter Fraud Transaction EDA (unsaved changes)

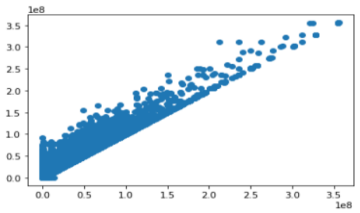
Logout

File Edit View Insert Cell Kernel Widgets Help

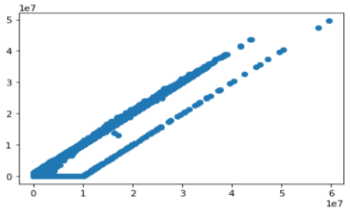
Trusted | Python 3

Run Code

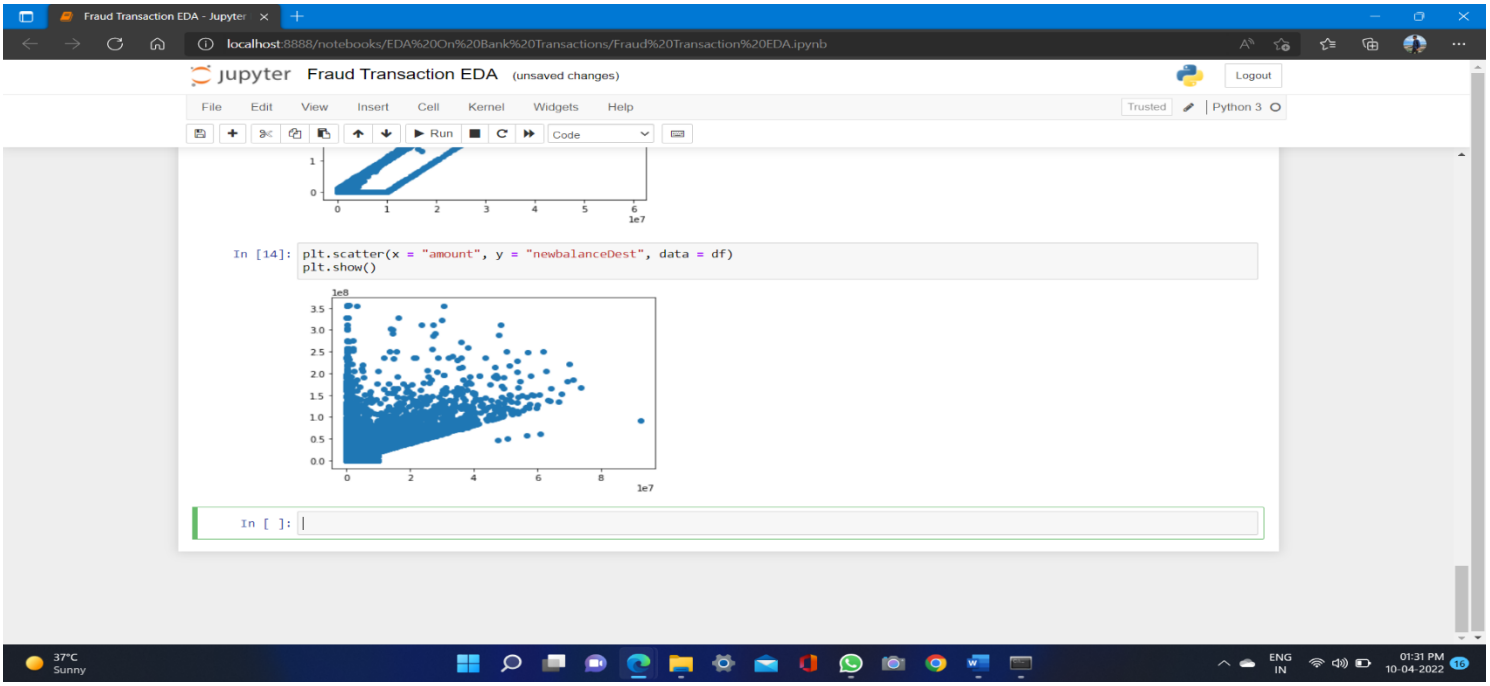
In [12]:
```
plt.scatter(x = "oldbalanceDest", y = "newbalanceDest", data = df)
plt.show()
```



In [13]:
```
plt.scatter(x = "oldbalanceOrg", y = "newbalanceOrig", data = df)
plt.show()
```



In [ ]:



GithubLink:
https://github.com/pawartanmay/Feyn_Lab_Internship.git

Conclusion:

Financial institutions are on the front lines in the fight against money laundering and terrorism financing. In addition, financial institutions must speed up the investigative process in order to reduce the "time to value," which is the time it takes to complete a transaction life cycle. As a result, adding machine learning to watch-list filtering systems that monitor financial transactions is a necessary if financial crime is to be combated more effectively and in a shorter amount of time. Many studies and investigations have been conducted to apply machine learning algorithms to AML solutions, however the industry is concerned about automating regulatory compliance areas due to the significant penalties that might be imposed if a failure occurs.