Evaluating the Financial Impact of Cyber Risk

[1]Vaidehi M Nair
Department of Computer Application
Amal Jyothi College of Engineering
Kottayam, India
vaidehimair1410@gmail.com

[2]Merin Manoj
Asst.prof Department of Computer Application
Amal Jyothi College of Engineering
Kottayam, India
merinmanoj@amaljyothi.ac.in

Abstract-- As in the context of an increase in cyber-attacks, it is critical for businesses to recognize the risk they face, even after deploying applications and implementing all security procedures. We describe a system or method for calculating an bussiness's Cyber-Value-at-Risk (CVaR). CVaR is a function that returns the loss of an organization due to cyber attcks over a particular amount of time.

Keywords — Cyber Security, Cyber-Value-at-Risk, Enterprise Security, Monte Carlo Simulations

I. INTRODUCTION

Cyber Value-at-Risk (CVaR) is created to make a study of the potential harm that can arise from cyber-treats, and the variable effectiveness of commonly-used risks controls. This will eventually lead to a better understanding of businesses' residual risk, the harms they may face in cyberspace, and the repercussions of implementing risk controls. Obtaining an in-depth associated risks that businesses face can help them make more informed risk-control decisions, that can help them lower the possibility of a cyber attack or increase their ability to mitigate various sorts of harm.

II. DESCRIPTION

Cyber Security is a necessary for any organisation, whether it is a startup or a major corporation. This is because everyone uses the internet to share essential information, thus making cyber security a must-have for everyone. It is more easy and faster to use the online method, and it's also less secure. The leakage of important information of an organization leads to huge loss of revenue results in business disruption. In such leakages small firms can even go bankrupt by paying very large amount against cyber attacks.

According to Daniel Castro, the vice-president of the Information Technology & Innovation Foundation, a cyber attack can cost anywhere between $57 to $109 B. It has being found that about, 36% of the businesses around the world to lose all of its money due to several cyber attacks. The annual loss is assumed to be an estimation of $79,841 on an average. Most people do believe that their company is too tiny to be targeted by a cyber assault, and this is where they make a mistake that turns the tables on them.

Cyber security is an economic and security concern that can better be handled by collaborating with consumers, business, and the government using private and public collaborations . Smaller firms lacked the technological and organizational abilities, along with judicial awareness, to start taking care of themself. Proper training should be provided through educational workshops so that individuals are aware of how to deal with cyber-attacks. Since they do not take any real measures to protect themselves against these dangers, small firms are more vulnerable to cybersecurity threats.
Cyber attacks frequently result in severe financial loss as a result of the following:
Information theft from a company
Financial resource theft (Eg bank details or payment card details)
Money theft wreaks havoc on the economy (eg inability to carry out transactions online)
Business or contract loss
Businesses that have had a cyber breach will almost always have to pay to fix the compromised systems, networks, and devices.

Key facts

- Risk of The portfolio is the diminishment in worth of a hazardous portfolio/asset beyond a specified period of time and confidence level is called VaR.
- Cyber Value at Risk is produced from a portfolio's or investment's value at risk.

DOI: 10.5281/zenodo.6364995

- When CVaR is used instead of only VaR, it results to a much more cautious approach to risk exposure.
- The value between VaR and CVaR isn't always evident; nonetheless, violated and engineered commitments can benefit from CVaR as a check on VaR's assumptions.

To close this gap, we created a model for calculating CVaR and tested its validity in a real-world case study. The CVaR model's aim is to assist organisations understand their residual risk, the harms they may face in cyberspace, and the repercussions of implementing risk control. The CVaR model that underpins this logic is thus the paper's fundamental contribution. The validation case study is being offered here simply as an example and is not intended for use in other research.

Data mining

Data mining is a procedure used by groups to show raw information into beneficial statistics through using some software program to search for patterns in massive batches of data, organization and teach more approximately their customers to expand greater effective advertising and marketing techniques, boom income and reduce rates. Statistics mining relies upon on the effective record in the warehouse, and laptop processing.

Data mining methods are used to create machine learning models that power applications such as search engine technology and website recommendation algorithms commonly used functionalities include Data cleansing, Artificial intelligence (AI), Association rule learning, Clustering, Classification, Data analytics, Data warehousing, Machine learning, Regression.

III. PURPOSE OF THE STUDY

This paper examines an organization's financial loss over a certain time period. It also provides a return value within a range, as well as a confidence level. After determining the variance, covariance, mean, and standard deviation of given datasets, a normal distribution curve is produced. A dataset that contains various financial records of an organization was selected for this study. For a given confidence interval, the greatest possible losses will be the VaR. For a given time frame t and a probability p, the VaR is the value that can be lost over time t with probability p. To calculate an asset's VaR, you must first identify the important metrics or variables that affect its value. VaR is determined using one of three approaches when the datasets have been found: historical simulations, delta-normal approach, or Monte Carlo simulations.

IV. METHODOLOGY

This article uses algorithms and data mining methods to estimate the return value and financial loss of an organization as a result of cyber attacks. The developing tool used is Colaboratory or Colab.

Colab

Colaboratory, or Colab in short, is a Google Research's product. Colab is a web-based Python editor that lets the user develop and run Python programmes. Machine learning, data analysis, and education are all areas where it makes it ideal. A hosted Jupyter notebook service called Colab allows free access to computational resources such as GPUs without requiring installation. Colab is a 100% free application. The availability of Colab resources is neither guaranteed or infinite, and usage limits are subject to change at any time. This is mandatory for Colab to provide free materials for users. For futher information, you can see Resource Limit. Colab Pro may be of interest to users who want more reliable access to greater resources.

Without having to download, install, or run anything, Colab allows you to utilise and share Jupyter notebooks with others. Colab notebooks can be downloaded from GitHub or saved in Google Drive. Just like Google Docs or Sheets, Colab notebooks can be shared. The software is free to use and is primarily a notebook environment based in the cloud. It offers features that allow you to edit documents in the same way that Google Docs allows you to. There are a variety of popular and high-level machine learning libraries supported by Colab that can be quickly loaded into your notebook.

Features of Google Colab

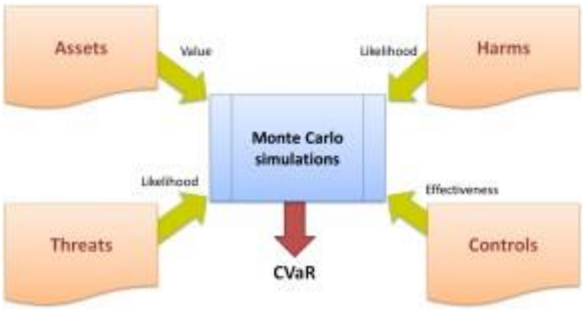
- Write and execute code in Python
- Document the code supporting the mathematical equations
- Create new notebooks
- Upload the existing notebooks

DOI: 10.5281/zenodo.6364995

- Import data from Google Drive
- Save notebooks from/to Google Drive
- Import/Publish notebooks from GitHub
- Import external datasets from Kaggle or yfinance.
- Integrate PyTorch, TensorFlow, Keras, OpenCV
- Free Cloud service with free GPU and TPU

System Architecture

This section outlines about using a CVaR computation enacted reforms, how to deploy it, and how to administer the system. Figure 1 shows the architecture of the system, with data files following the format serving as inputs and Monte Carlo simulations serving as outputs for the CVaR distribution**.**



.

Figure1: Architecture Overview

We choose to run Monte Carlo simulations in a sequential order across all layers of the model (assets, threats, controls, and harms); the system begins with an organization's assets and gradually progresses to harms. Using this method, we can produce granular results and predict events leading to catastrophic outcomes. Before analysing the numbers and distributions utilised, we first introduce the formalisation of these sequential calculations.

V. IMPLEMENTATION

Monte Carlo Simulations is used on the given data set in order to create or to make out a few useful model to find the return value in a range. Simulations of Monte Carlo algorithms are used to determine how much a company will lose and over what period of time. Once the datasets have been found, VaR is calculated using one of three methods: historical simulations, delta-normal approach, or Monte Carlo simulations.

The Value at Risk (VaR) metric is used to assess the risks of survival revenue on a venture. For instance, a Daily Value at Risk of 6.5 percent with a 95% confidence level. Means there's a 5% chance your portfolio will lose 6.5 percent or more in a single day. In contrast, we have a 95% confidence level that our portfolio will not fall by 6.5 percent in a single day.

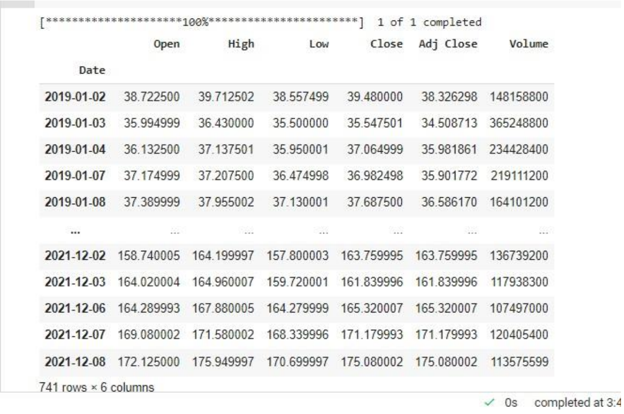
Parametric VaR (variance-covariance method): The mean, or anticipated value, and standard deviation of a portfolio are calculated first. The Confidence Interval is a range of in which we may reasonably predict our true values. We begin by constructing the portfolio and then calculating the daily returns.

Data source

Here we consider the datasets.

The datasets are downloaded from installing yfinance API of different companies in google colab.

It contains data from a particular date. The table's properties include open, close, high, low, volume, and adj close of several organisations. For example, we can learn about Apple's daily returns.



```
[*********************100%***********************]  1 of 1 completed
                 Open        High         Low       Close   Adj Close     Volume
Date
2019-01-02   38.722500   39.712502   38.557499   39.480000   38.326298  148158800
2019-01-03   35.994999   36.430000   35.500000   35.547501   34.508713  365248800
2019-01-04   36.132500   37.137501   35.950001   37.064999   35.981861  234428400
2019-01-07   37.174999   37.207500   36.474998   36.982498   35.901772  219111200
2019-01-08   37.389999   37.955002   37.130001   37.687500   36.586170  164101200
...                ...         ...         ...         ...         ...        ...
2021-12-02  158.740005  164.199997  157.800003  163.759995  163.759995  136739200
2021-12-03  164.020004  164.960007  159.720001  161.839996  161.839996  117938300
2021-12-06  164.289993  167.880005  164.279999  165.320007  165.320007  107497000
2021-12-07  169.080002  171.580002  168.339996  171.179993  171.179993  120405400
2021-12-08  172.125000  175.949997  170.699997  175.080002  175.080002  113575599
741 rows × 6 columns
```

Figure2: Financial analysis of Apple

Figure 2 depicts Apple's dataset for January 1st of 2019. Now we are finding Adj close for all the companies. The final dataset we use is the percentage change table of companies, here we use 5 companies.

DOI: 10.5281/zenodo.6364995
ISBN: 978-93-5607-317-3 @2022 MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam.

Working

Once the datasets have been found we build a portfolio and calculate daily returns. The variance covariance matrix is then found, followed by the mean and count of columns for each company. To generate a normal distribution curve, we must first determine the mean and standard deviation of a portfolio of diverse companies.

Once we know the covariance of all the stocks in the portfolio, we must calculate the portfolio's standard deviation to determine portfolio variance. To do so, we must first determine the weights or capital allocation percentages for each stock. When adding up the components in the matrix, we must remember that each component represents a percentage of the total investment. Thus, the total must equal 1 when adding up all the components.

The matrix 'W' gives the weight distribution for a portfolio with 'n' stocks

$$W = \begin{bmatrix} W_1 \\ W_2 \\ W_3 \\ W_4 \\ W_5 \\ . \\ . \\ . \\ W_n \end{bmatrix}$$

The portfolio's expected returns is given by:

Expected portfolio return = M * W

The portfolio’s variance is given by

Expected portfolio variance =

WT * (Covariance Matrix) * W

where WT represents the transpose of W matrix

Algorithm

Monte Carlo Simulation: Monte Carlo simulations are being used to depict the likelihood of forecast horizons in a mechanism that is tough to anticipate due largely to random factor interactions. This is a method for determining how risk and uncertainty affect prediction and forecasting models.

Monte Carlo simulations can improve a number of industries, notably financing, technology, order fulfillment, and astronomy. A multiple probability simulation is another name it is known by.

KEY TAKEAWAYS

- A Monte Carlo simulation is a paradigm that determines the likelihood of various possibilities, when independent variables are infused.
- Monte Carlo developed models can be used to examine the risk impact and unpredictability on forecast and prognosis statistics.
- • Monte Carlo simulations are utilized in a variety of sectors, including those of economics, manufacturing, systems integration, and academia.
- A Monte Carlo simulation is based on giving numerous values to an uncertain variable in order to generate multiple outcomes, which are then averaged to obtained is an estimate.

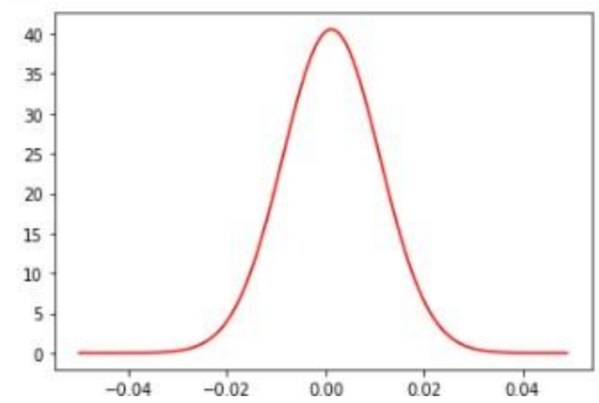


Figure3: Normal Distribution

- Monte Carlo simulations assume perfectly efficient markets.

We calculate the VaR based on the normal distribution curve, which is the probability of loss with a 5% confidence interval.

Considering the confidence level we calculate VaR which gives the loss percent in one day.

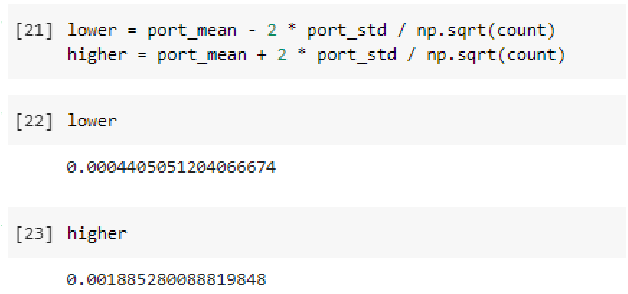
Next step is to calculate confidence interval considering a confidence level 95.5%.
Confidence level is calculated using:

$$\bar{x} \pm z_{\alpha/2} \times \frac{\sigma}{\sqrt{(n)}}$$

where z is confidence coefficient, alpha is confidence level n is sample size and zigma is standard deviation.

As we find the confidence value between a range.

The output will be:



```
[21] lower = port_mean - 2 * port_std / np.sqrt(count)
     higher = port_mean + 2 * port_std / np.sqrt(count)

[22] lower

     0.0004405051204066674

[23] higher

     0.001885280088819848
```

Figure4: Range of return value

From this we can say that 95.5% confident that the daily return of our portfolio will be between 0.0004 and 0.0018.

VI. CONCLUSION

We continue to experience an increasing threat in cyberspace, and while a variety of safeguards can avoid and lessen and the the harms caused by cyber-threats, we are nevertheless exposed to residual hazards. It is crucial that enterprises comprehend this residue risk and the range of potential losses that might arise, since this can serve to inform not only threat detection strategies, but also alter decisions on which measures should be used to reduce risk, and whether cyber- insurance should be used as a risk-sharing method.

There is a lack of systematic frameworks to aid organisations and insurance companies in calculating the full range of losses that could result from a cyber-threat, taking into account both the use and effectiveness of risk-controls, as well as the potential for harm propagation across an enterprise. We built a technique to determine an organization's Cyber-Value-at-Risk to fill this hole (CVaR)

Our CVaR model takes into account a wide portfolio of resources, how they have been likely to be interrelated, the price bracket of harms that could lead from a botnet, the funds that are highly susceptible to such a hazard, the risk assessments in necessary to secure resources and their anticipated achievement, as well as the effectiveness of risk controls. CVaR is a probability distribution for a range of potential losses, which can be estimated either by considering all harms to be in scope, or by using a specific threat intelligence and focusing on a specific threat category.

VII. REFERENCES

[1] https://www.wikihow.com/Calculate-Confidence-Interval

[2] https://blog.quantinsti.com/calculating-covariance-matrix-portfolio-variance/

[3] Albina Orlando "Cyber Risk Qualification: Investigating the Role of Cyber Value at Risk"

[4] https://www.cs.ox.ac.uk/projects/ACVAR/

[5] https://www.afponline.org/ideas-inspiration/topics/articles/Details/cybersecurity-quantifying-value-at-risk

[6] https://www.fairinstitute.org/blog/what-is-a-cyber-value-at-risk-model

[7] Young Hoon Kwak, Lisa Ingall "Exploring Monte Carlo Simulation Applications for project Management"ssss

[8] https://assignmentslab.com/financial-analysis-of-apple-inc/

[9] https://blog.quantinsti.com/calculating-covariance-matrix-portfolio-variance/