Evaluation of the Risk and Resiliency of the Amazon AWS Data Centers in the United States of America

Samriddhi
CY5250 – Decision Making in Critical Infrastructure
December 6, 2023

Contents

1 Background

1.1 CIKR Sector Background

CIKR stands for Critical Infrastructure and Key Resources. It refers to the fundamental assets and systems, both virtual and physical, that are considered to be necessary for the public health, security, and economic operations of a country. A nation may suffer grave repercussions if these critical resources and essential infrastructure sectors are disrupted or destroyed. They include a broad spectrum of businesses and services. The Department of Homeland Security (DHS) in the US has classified sixteen key infrastructure sectors, including transportation, energy, telecommunications, public health and healthcare, water and wastewater systems, and financial services, these industries are regarded as the backbone of the country, safeguarding them from dangers such as natural disasters, cyberattacks, and physical attacks is of utmost importance to national security. These industries supply the resources and services required for the well-being of society, their protection is crucial to preserving a nation's resilience and stability. To protect these important assets and guarantee their continuous functioning even in the face of diverse threats, security measures, risk assessments, and resilience planning are usually used. [1]

The Information Technology (IT) sector manufactures and offers high-assurance IT goods and services to commercial enterprises, governments, critical infrastructure sectors, and individual individuals. In an industry as big and varied as the IT sector, effective cooperation between partners in the public and commercial sectors is essential to addressing these issues and ensuring the resilience and safety of IT sector operations, which are vital to the country and sector. The goal of the IT sector is "to achieve a sustained reduction in the impact of incidents on the sector's critical functions," with the protection of critical infrastructure being the top priority. Physical assets that are easily identified and have a limited quantity make up the majority of many essential infrastructure sectors. In contrast to some other sectors, the IT sector is function-based and consists of virtual systems and networks in addition to physical assets that support critical services and capabilities in both the public and private sections. The sector's capacity to create and offer high-assurance IT goods and services for different sectors is supported by six essential functions. These tasks are necessary to uphold or reconstitute networks, including wide-area networks, local networks, the Internet, and their related services. The IT sector’s six critical functions are: 1. Provide IT products and services; 2. Provide incident management capabilities; 3. Provide domain name resolution services; 4. Provide identity management and associated trust support services; 5. Provide Internet-based content, information, and communications services; and 6. Provide Internet routing, access, and connection services. Amazon web services provides technology for running code, maintaining data, and integrating applications without the need for server management. To boost agility and save costs, serverless solutions include automatic scaling, built-in high availability, and a pay-per-use invoicing mechanism. These technologies also make infrastructure management chores such as capacity provisioning and patching obsolete. [2]

1.2 Amazon AWS US Data Centers

A subsidiary of Amazon, Amazon Web Services, Inc. (AWS) provides scalable and secure cloud computing services to a diverse range of businesses and organizations. With state-of-the-art infrastructure, AWS data centers support various services, including computing power, storage, and networking, ensuring high availability, reliability, and low-latency performance for customers across the U.S. AWS operates in four regions and sixteen availability zones in the United States.[3] The data centers from the US region are US-West-2, Oregon Data Center, Northern California, Washington, Montana, New Mexico, and Colorado on the west side, and from the east, US-East-1, Ohio Data Center, Massachusetts, Texas, Missouri, Minnesota, and Florida. [4]

1.3 Previous Attacks

A Texas man was sentenced to 10 years in federal prison for planning to blow up an Amazon Web Services data center in Virginia. [5]

A Cloudflare Network Outage in 2021 which was highly dependent on the AWS infrastructure caused a major service disruptions for many websites and platforms. [6]

A group of cybercriminals through social engineering gained internal data for several companies, including AWS. [7]

2 Methodology

2.1 Network Topology Creation

The effective functioning of the data centers is contingent upon various critical risk factors. These factors, each contributing a specific percentage to the overall risk index, include Energy Cost per Kwh (8.97%) [8], International Internet Bandwidth (Mbits/s) (23.08%) [9], Corporation Tax (6.41%) [10], Political Stability (EIU Instability Index) (12.82%) [11], Sustainability (% of energy alternatives) (8.97%) [12], Natural Disaster (15.38%) [13], Energy Security (12.18%) [14], and Water Availability per capita (6.41%) [15]. US-West-2 and Oregon Data Center: The US-West-2 region, with its centerpiece, the Oregon Data Center, exhibits a resilient operational environment. Characterized by an energy cost of $8.82 per Kwh, an impressive internet bandwidth of 39.1 Mbits/s, and a 7.6% corporation tax, this region stands out for its stability. Political stability is indexed at 13, sustainability at 24%. Energy security and water availability are both indexed at 24. The vulnerability is estimated at 20%. Consequence costs amount to $10 million, with prevention and response costs each set at $10 million and $20 million. Northern California: Moving to Northern California, this region, with an energy cost of $10.12 per Kwh and a substantial internet bandwidth of 37.2 Mbits/s, maintains a 7.4% corporation tax. Political stability stands at 15, sustainability at 22%. Energy security and water availability are both indexed at 22. This region's vulnerability of 25%. Consequence costs are $15 million, with prevention costs at $7 million and response costs at $12 million. Washington: Washington exhibits an energy cost of $9.34 per Kwh, an internet bandwidth of 35.3 Mbits/s, and a 7.2% corporation tax. Political stability stands at 14, sustainability at 20%. Energy security and water availability are both indexed at 20. A vulnerability of 20%. Consequence costs are $10 million, with prevention and response costs at $6 million and $10 million, respectively. Montana, New Mexico, and Colorado: Montana features an energy cost of $8.56 per Kwh, and New Mexico boasts a cost of $7.78 per Kwh, both with varying corporation taxes and stable operational environments. Colorado distinguishes itself with a low energy cost of $7 per Kwh. Each of these regions maintains unique attributes contributing to their operational resilience, such as moderate internet bandwidth, political stability, and sustainability. Vulnerabilities range from 5% to 15%, with associated consequence costs and prevention costs varying accordingly**.** US-East-1: US-East-1, representing the New York Zone, demonstrates a higher energy cost of $14.87 per Kwh and an impressive internet bandwidth of 46.7 Mbits/s. With a 7.1% corporation tax, political stability indexed at 20, and 100% sustainability in energy alternatives, this region stands out. With energy security and water availability both indexed at 20. Here the vulnerability is 30%. Consequence costs are $20 million, with prevention and response costs at $8 million and $15 million. Ohio Data Center: The Ohio Data Center within the US-East-1 region echoes the characteristics of the broader zone. Sharing the same energy cost, internet bandwidth, corporation tax, and stability index. Energy security and water availability, both indexed at 18, contribute to its operational robustness and vulnerability is set at 25%. Consequence costs, prevention costs, and response costs are uniform at $15 million, $7 million, and $12 million, respectively. Massachusetts, Texas, Missouri, Minnesota, and

Florida: Massachusetts maintains an energy cost of $11.45 per Kwh, an internet bandwidth of 35.1 Mbits/s, and a 6.5% corporation tax. Texas showcases an energy cost of $9.87 per Kwh, Minnesota boasts a low cost of $8.32 per Kwh, Missouri features a modest cost of $8.98 per Kwh, and Florida distinguishes itself with an energy cost of $7.65 per Kwh. Each region maintains unique attributes contributing to their operational resilience, such as varying internet bandwidth, political stability, and sustainability. There is a uniform threat percentages of 100% for all nodes. Vulnerabilities range from 5% to 30%, with associated consequence costs and prevention costs varying accordingly.

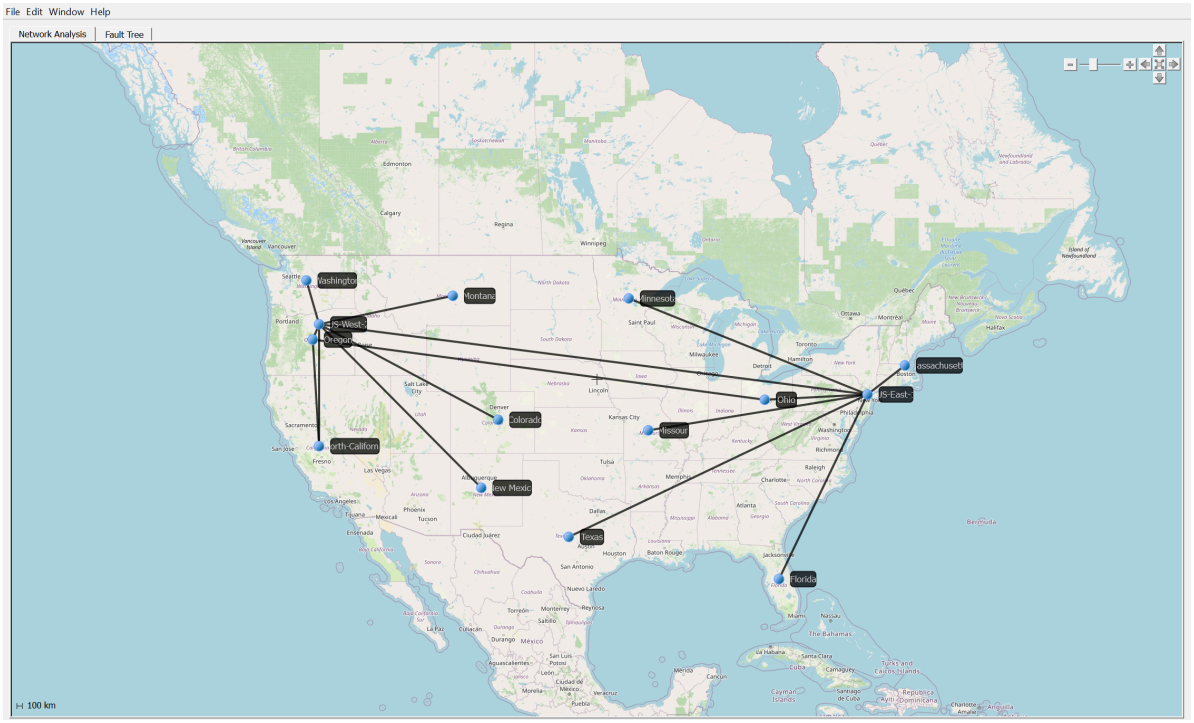


Fig 2.1 : Network Topology of AWS Data Centers using MBRA Tool

2.2 Calculating Vulnerability Percentages

The Vulnerability percentage of a node is the probability of the failure of that node which can lead to a potential exploitation of the whole critical infrastructure. The vulnerability percentages presented here are a result of combining factors of several aspects, including water supply and natural disasters, as discussed in Section 2.1 Network Topology Creation. Following are the vulnerabilities for the nodes:

> US-East-1: 30%, North California : 25%, Oregon : 20%, Ohio : 25%, US-West-2 : 20%, Massachusetts : 20%, Florida : 5%, Washington : 20%, Colorado : 5%, New Mexico : 10%, Minnesota : 5%, Texas : 15%, Montana : 15%, Missouri : 10%.

2.3 Calculating Consequence Cost

For each node, the cost of each consequence depends upon the geographical area of that node. Since the Consequence Cost is a factor of the threat percentage, the vulnerability and asset values, the US-East-1 (New York) Zone and North California have higher consequence cost based on their geographical

locations. This is because the North California zone has 3 out of the 13 DNS Root Servers in this region and the New York Zone being so susceptible to cyber-attacks. [16]

2.4 Calculating Response Cost

The response cost for a node in the critical infrastructure is the entire amount of money needed to prevent, mitigate, and handle security incidents or disruptions that affect that particular node. This includes the costs incurred, the distribution of resources, and the work required to return to regular operations and rebuild resilience following a negative incident. This provides us with an estimate of the maintenance budget, which is subsequently distributed across the nodes according to their respective percentages of the cost. That would therefore be the response cost related to a node.

The length of each link from the beginning to the end of the node is taken into account for the links.

2.5 Calculating Prevention Cost

Having a backup data center can help estimate the prevention cost, which is defined as the cost needed to reduce the probability of a node failing to 0%. Therefore, the initial cost required to build the servers in the data centers is assessed as the prevention cost for a node.

The cost of replacing both data centers might be seen as the preventative cost for the links.

3 Network Characterization

With the help of a network graph, the creation of an adjacency matrix can be done. And, based on the links and nodes of the matrix, the calculation of the spectral radius, node degree, betweenness, and centrality is performed.

The following are the key findings from the analysis:

- Degree of the network: 7
- Average node degree: 2.14
- Spectral Radius of the network: 3.22

3.1 Top Vulnerable Nodes

The analysis also gives two nodes which seem to have the highest degree, degree centrality, betweenness centrality and eigenvector centrality. They are as follows:

Node	Degree	Degree Centrality	Betweenness Centrality	Eigenvector Centrality
US-East-1	**7**	**0.53**	**0.67**	0.47
US-West-2	**7**	**0.53**	0.65	**0.54**

Table 3.1: Network Characterization – Top vulnerable nodes

The values marked in bold are the maximum values for degree, degree centrality, betweenness centrality, and eigenvector centrality in the whole network. These two nodes hold all of the top values out of the 14 nodes. US-East-1 and US-West-2 both have the maximum degree and degree centrality. The US-East-1

data center has the highest betweenness centrality in the network, and the US-West-2 has the highest eigenvector centrality.

The number of edges connecting to a node is referred to as its node degree. Nodes with higher degrees are frequently seen as significant since they are linked to many other nodes and can thus play a key role in the flow of information through the network. Network degree**:** the total of all node degrees in the network. This is a measure of the network's overall connectedness. Link robustness**:** A network's ability to tolerate the removal of links A network with high link robustness is more likely to stay connected and functional even if some of its links fail. The non-critical nodes are those that can be disconnected without severely disrupting network connectivity. Links that must be removed in order to disconnect the network are called critical nodes**.** Spectral radius**:** The biggest eigenvalue of a network's adjacency matrix. The spectral radius quantifies the network's connectedness. A high spectral radius suggests that the network is well-connected and that disconnecting it by eliminating a small number of links is difficult**.** Node robustness**:** A node's ability to tolerate the removal of its linkages A node with high node robustness is more likely to maintain connectivity with other nodes even if part of its links are destroyed. The non-blocking nodes are those that can be removed without adversely affecting network connectivity. Blocking nodes are those that must be removed in order to disconnect the network. Node centrality is a measure of a node's relevance in a network. There are other node centrality measurements, but they all basically represent the idea that a node is more central if it is connected to many other nodes or if it is placed in a crucial location in the network. Betweenness centrality**:** a measure of a node's importance in a network based on the number of shortest paths that travel through the node. A node with a high betweenness centrality is significant because it regulates the flow of information between many other nodes. Eigenvector centrality is a measure of a node's importance in a network based on how many times it is linked to other significant nodes. A node with high eigenvector centrality is significant because it is linked to numerous other nodes that are also significant.

3.2 Numerical Parameters

The resilience equation captures the trade-off between a system's ability to withstand disturbances and its adaptive response, offering a comprehensive measure of resilience in a variety of contexts such as natural systems, enterprises, and essential infrastructure.

A major vulnerability is a flaw or weakness in a system or process that, if exploited, poses a serious and potentially catastrophic danger. Malicious actors can exploit this flaw, resulting in unauthorized access, data breaches, or system failures. Because of their high likelihood of exploitation and considerable effect, critical vulnerabilities are frequently prioritized for quick remedy. Identifying and fixing these vulnerabilities is critical for preserving system security and integrity, whether in software, infrastructure, or organizational processes, in order to avoid potential injury, data loss, or operational interruptions.

With the help of excel spreadsheet and python script, the Spectral Radius = 3.22 and Mean Degree is 2.07

So, to calculate resilience:

$\log(q1) = b + k * \gamma1 * \rho$ and $\log(q2) = b + k * \gamma2 * \rho$

Here, $\rho = 3.22$

$\gamma1 = 10\%$ and $\gamma2 = 100\%$, $q1 = 1.22$ and $q2 = 0.23$

So, $\log(q1) = 0.086$

$\log(q2) = -0.638$

For finding the values of b and k, the equations are:

$$0.086 = b + k*0.1*3.22$$

$$-0.638 = b + k*1*3.22$$

Therefore, b = 0.173 and k = −0.271

Hence, the final equation becomes: $\log(q) = (0.173)+(-0.271)*3.22* \gamma$

So, the critical vulnerability, $\gamma = 0.198$, when q=1.

Furthermore, analysis of the adjacency matrix gives us the following values:

- Total number of nodes: 14
- Total number of links: 30
- Link Robustness: 6.67%
- Number of links that can be removed: 2
- Node Robustness: 68.94%
- Number of robust nodes: 9.65
- Number of blocking nodes: 4.35

The network's rather fragile because the link robustness is low. It would take the removal of just 2 links within the network to break it. On the other hand, the node robustness is higher. It would take the removal of almost 10 nodes before the system starts to break. The blocking nodes gave us the estimate of the nodes which cannot be removed further system to remain intact. As it is inversely proportional to the robust nodes, we see that the blocking nodes are relatively few when compared to the robust nodes. It would take only 4 nodes out of 14 for the system to remain intact.

4 MBRA Network Analysis

The MBRA tool supports the Model-Based Risk Analysis technique as described in Critical Infrastructure Protection in Homeland Security (Lewis, 2003). The purpose of this tool is to assist in making objective decisions about resource allocation towards the goal of reducing risk and/or vulnerability within a vast network of assets. [17]

4.1 Risk Ranking

By selecting the Weight By to Degrees and betweenness and using Risk as the objective function, we get the following results:

The two critical nodes where found to be the US-East-1 and US-West-2 data centers. The east data center is very close to New York and the west one is close to California, two of the major States in the United State. New York being the home to Wall street and California being the Silicon Valley, makes these two nodes a major threat in case of an attack be it cyber or physical. To prevent malicious activity, use of

firewalls, intrusion prevention systems, and access controls is a must. Implementation of blocking steps to prevent vulnerabilities from being further exploited in case of an attack.

4.2 Vulnerability Ranking

By selecting the Weight By to Degrees and betweenness and using Vulnerability as the objective function, we get the following results:

The US-East-1 and US-West-2 data centers are the two topmost vulnerability nodes. The reason why these nodes are considered high in the vulnerability rankings could be due to their position in the network, being located in two of the top states of the United Nations and connecting various data centers of the other zones through their links.

4.3 Threat Ranking

Weighting by degrees and betweenness and using Threat as the objective function, we get the following results:

The top three nodes ranked by threat are US-East-1, US-West-2, Oregon. Each of these three has high a degree, with US-East-1, US-West-2 having 7 as their network degree and Oregon as 3. There are significant costs for response and prevention attached to each of them. The findings of classifying the nodes according to the consequences of their failure are comparable to those obtained from the Risk rankings. This suggests that having both a high degree and a high consequence together is not what you want. Nonetheless, the network of AWS data centers as well as these nodes have this combination.

5 MBRA Chart Data

5.1 Node Degree Graph

The node degree graph tells us that the majority of nodes present in the network have just one link connecting them. It is a histogram of degree versus the count of nodes with that degree.

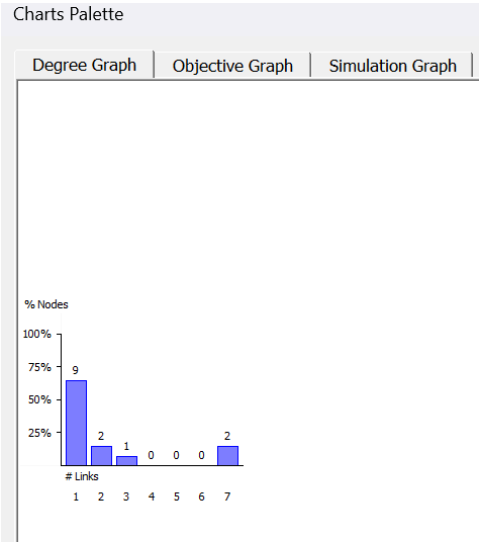


Fig. 5.1: Node Degree Graph

Here, we notice that the graph has a line curve. The highest number of nodes are found with 1 link. The nodes with 2 links are also significant. There are also three nodes with zero links each.

5.2 Exceedance Probability graph

An understanding of the "q" or fractal dimension can be gained from the simulation graph that is derived with the help of MBRA Tool.

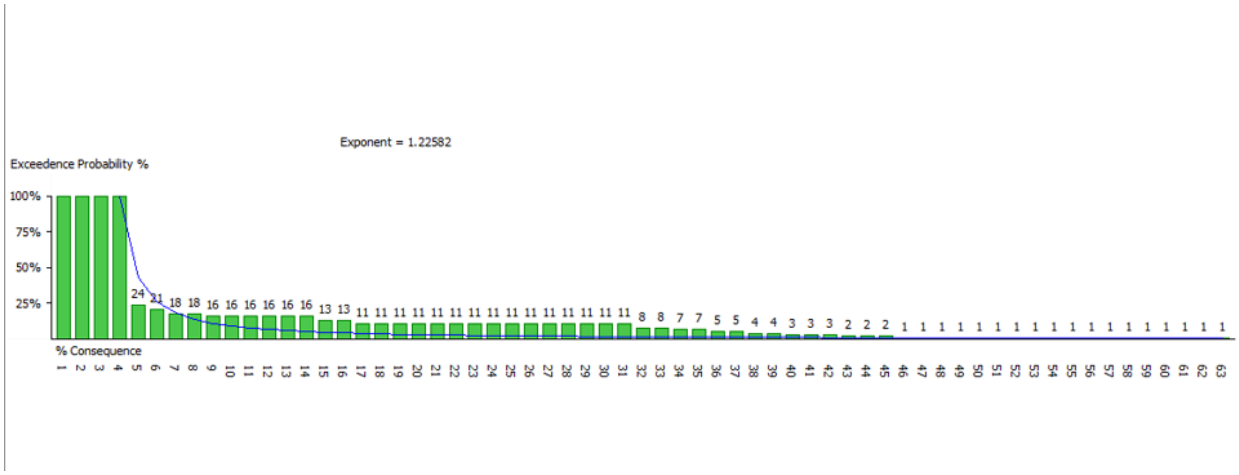


Fig. 5.2: Exceedance probability graph

We see that the PML curve for the network gives an exponent of 1.22. We know that PML risk is high if q is lesser than 1, and is low if the value of q is greater than 1. Since, q is greater than 1 so the network is not in danger of a cascading failure.

5.3 Resiliency

The fractal dimension (q) and the product of vulnerability percentage and spectral radius are the two points on a graph that represent the resiliency line. The system's critical vulnerability is indicated by the point on the curve where q=1 is passed. This is the percentage of vulnerability that a system can experience cascade failures beyond.
The following is the resilience equation:
log (fractal dimension) = vulnerability * spectral radius * b + k , with b and k serving as constants.

So, the critical vulnerability, $\gamma = 0.198$, when q=1. (Calculation in Section 3.2)

Thus, the system is likely to go into it cascading failure if the vulnerability of the nodes and links exceed 19.8%.

5.4 Risk Mitigation and Resilience Improvement

Improve security measures surrounding high-traffic nodes because the compromise of these nodes can have a major impact on network connection. For these critical nodes there should be additional layers of authentication, monitoring, and anomaly detection to mitigate risks. The creation of a comprehensive security policy that integrates multiple measures such as encryption, multi-factor authentication, and network segmentation is also important. Implementation of security awareness training to teach people how to recognize and prevent social engineering attacks which can lower the chance of an attack.

To increase system resilience by redundancy in critical nodes and diversifying infrastructure components. We can also implement failover measures to ensure that operations continue even if one node fails. For example, even if say the US-East-1 data centers shuts down for a reason, the surrounding nodes like MA or Ohio can work as a backup until the services are restored for the US-East-1 data center. The creation and following of an incident response plan that explains precise steps to take in the case of a security problem is also a important point to improve resilience. The training and education of staff members, stakeholders, various heads and employees also plays a major factor in case of attacks. If people know how to respond effectively to a situation, half the problems can be solved. So, by conducting drills and simulations should be to ensure the effectiveness of the response strategy can help a lot.

We need to ensure compliance with relevant cybersecurity regulations and standards, such as NIST Cybersecurity Framework, ISO 27001, and industry-specific standards are met.

Budget plays an important factor in order to mitigate risks, without proper cost estimation and funding sources, if even we have a plan that wouldn't work if proper allocation of budget is not done. Budget for the purchase and installation of advanced security technology like as firewalls, intrusion prevention systems, and endpoint protection solutions should be taken in account as these help improve resilience. Investing in cybersecurity training programs to educate personnel on best practices, phishing prevention, and social engineering. Implementation of a strong network monitoring and detection system capable of detecting unusual activity and potential security breaches in real time.

Budget for the creation and testing of an incident response plan, including incident response team training and the acquisition of relevant tools. Allocate resources to guaranteeing diversity in infrastructure components and building redundancy in these critical nodes. Conduct frequent security audits and penetration testing to detect vulnerabilities and evaluate the effectiveness of safeguards in place. Governance and Compliance: Investing in compliance initiatives to guarantee that industry standards and laws are followed, thereby boosting the overall security posture. Establish a budget for continual improvement to enable for the adaption of security measures in response to increasing threats and technological advancements.

To effectively mitigate risks and enhance resilience, a comprehensive budget should be allocated for various security measures, training programs, incident response preparedness, and ongoing improvement initiatives. This investment is essential for establishing a robust cybersecurity framework that addresses identified risks and safeguards the resilience of critical nodes within the system.

6 Fault Tree Analysis

We are able to investigate the different reasons for a certain weak node through fault tree analysis. Nodes with low resilience and high risk are better suited for this study. Therefore, the FTA analysis done on the two critical nodes.

For US-East-1 the major threats were: Floods, Bombing and Server fails.

And for US-West-2, the major threats taken account were Earthquakes, Bomb, and also Server failure in the data centers. As the west coast region of the United States are more prone to Earthquakes and the east coast region is more prone to floods, tsunamis. That's is why we have considered them as major threats.

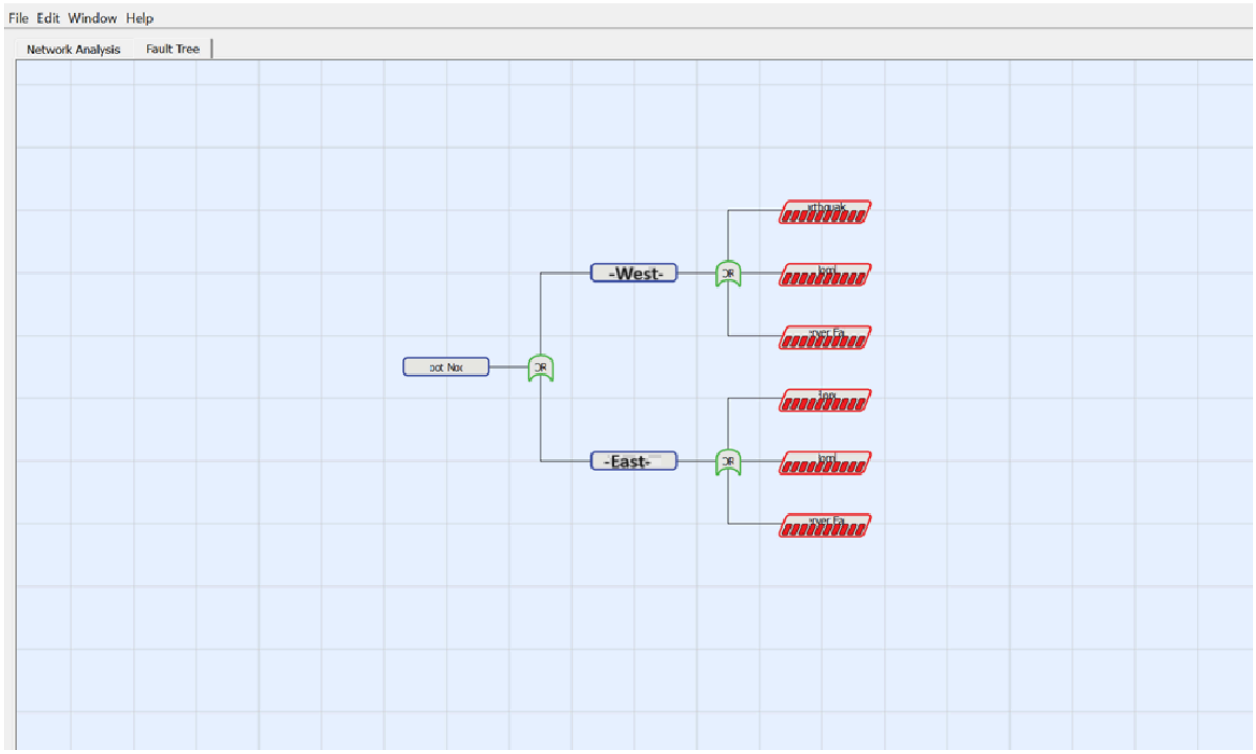


Fig. 6: Fault Tree Analysis

The maximum budget which is possible for these nodes is 17 million dollars. Applying a budget of 8 million dollars, the vulnerability to drop from 89.73% to 41.64%. The whole of this budget is spread across both the critical nodes.

7 Attacks on the network

Someone with intent may launch a targeted or random attack. It is implied by a random attack that the attacker chooses a node or link at random. In order to maximize the damage inflicted by the attack, a targeted attack suggests that the attack targets nodes and links while taking into account how critical those nodes and links are. [18]

7.1 Random Attack

Random attacks are cybersecurity occurrences in which threat actors do not expressly target a target but instead exploit vulnerabilities opportunistically. These assaults are often automated and indiscriminate, attempting to compromise systems, networks, or applications without a specific target in mind. Random attacks cast a wide net, seeking to exploit common weaknesses that may exist across a large range of entities. Examples include monitoring the internet for unsecured devices, performing brute force attacks to guess passwords, and exploiting known software flaws. The major motivation for random assaults is frequently to compromise as many systems as possible rather than to target a specific individual or organization.

7.2 Targeted Attack

Targeted attacks, also known as advanced persistent threats (APTs), include threat actors making a deliberate and focused effort to compromise a specific individual, company, or industry. Targeted attacks, as opposed to random attacks, are carefully prepared and tailored to the features of the desired target. Adversaries carrying out targeted assaults spend time performing reconnaissance to learn about the target's infrastructure, employees, and vulnerabilities. A targeted attack's purpose is usually to gain unauthorized access to sensitive information, intellectual property, or vital systems. To achieve their goals, targeted attacks frequently involve sophisticated techniques such as social engineering, spear-phishing, and bespoke malware. The motivation for targeted attacks varies and may include espionage, financial gain, or operational interruption.

7.3 Attacks on the Critical Nodes

The nodes, US-East-1 and US-West-2 here plays a vital role in supporting numerous industries and essential infrastructure sectors. It can be a prime target for a wide range of threats and attacks. These are a few typical dangers and attacks against the IT industry: Malware Attacks like viruses and worms: By infecting files, emails, or downloads, malicious software can enter IT systems and cause disruptions as well as data loss. Or Ransomware: Cybercriminals encrypt information and demand a ransom to decrypt it, thereby creating disruptions to systems and perhaps leading to data breaches. In both social engineering and phishing**,** cybercriminals deceive employees into disclosing confidential information or downloading dangerous software by using phony emails, websites, or phone calls. The attacks are called Distributed Denial of Service (DDoS), where attackers flood IT systems with traffic, preventing authorized users from accessing them and interfering with functions. Insider Dangers: Here, employees or contractors with malicious or careless intentions may purposefully or inadvertently jeopardize IT security, data, or systems. Supply Chain Deployments: In order to create weaknesses or backdoors into IT systems, attackers breach software or hardware providers. IoT and OT Vulnerabilities**:** Security flaws can result in vulnerabilities in both Internet of Things (IoT) devices and operational technology (OT) systems, including supervisory control and data acquisition (SCADA) and industrial control systems (ICS). Software Vulnerabilities**:** Attackers may use outdated or inadequately secured software to obtain access to IT systems. Cyberattacks by nation-state actors**:** These actors use cyberwarfare, cyberespionage, and cyberattacks to target vital IT infrastructure. Data interception is the practice of listening in on data transfers and stealing private information. Cryptojacking: Unauthorized mining of cryptocurrencies by hackers using IT resources reduces system performance and energy usage. Attacks Based on AI and Machine Learning**:** By utilizing AI and machine learning techniques, attackers can create more complex and devious attack plans. [19]

8 Return on Investment (ROI) considerations

Return on investment is calculated by comparing the of the risks involved before and after a certain investment is made. As a formula, it is as follows:
ROI = (Risk (before investment) – Risk (after investment)) / $Investment

8.1 Risk Prevention ROI

MBRA provides a graph which maps the risk associated with a particular prevention budget. This allows us to better estimate the ROI based on the optimum budgetary data. This graph considers the risk weighed by degrees and betweenness of the nodes in the network.

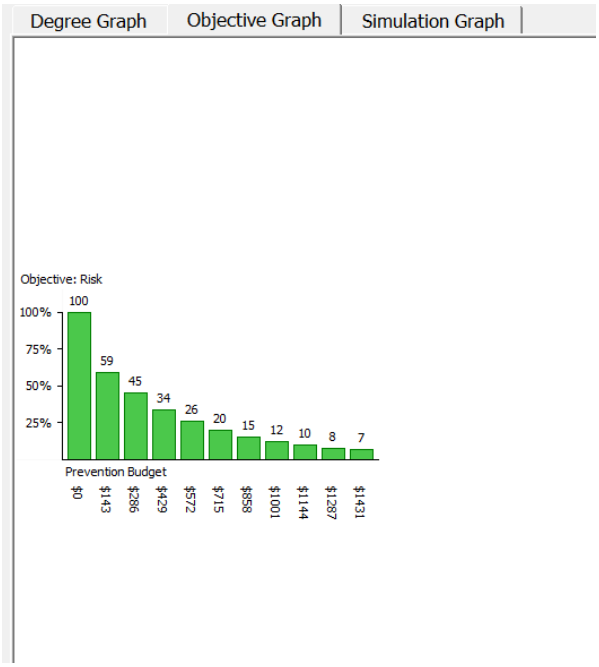


Fig. 8.1: ROI for Risk

8.2 Vulnerability ROI

Another component of investment could be to lessen the vulnerability in the hardened nodes. It is acquired by spending on vulnerability is shown in the graph below, which is based on degrees and betweenness.

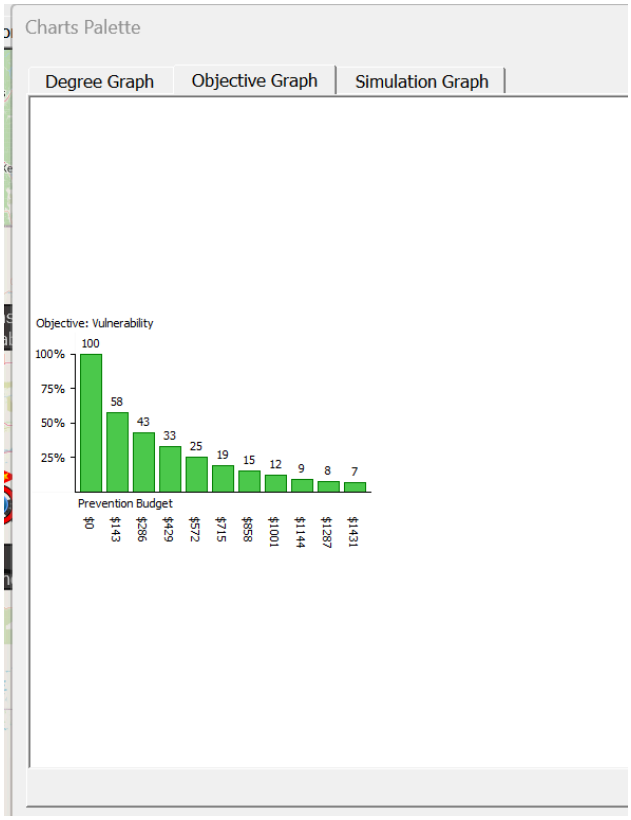


Fig. 8.2: ROI for Vulnerability

When the results of the risk and vulnerability ROI factors are combined, it may be beneficial to include both in the budgetary allocation.

9 Possible Funding Sources

The possible funding sources in this case can be by the State government. If there is a budget constraint then with the help of Federal government and private sector agencies this constraint can be resolved.

AWS offers service level agreements (SLAs) that describe the degree of service and client commitments. Depending on the terms of the SLA, AWS may be required to pay service credits, reimbursements, or compensation to customers in the event of service outages or failures.

The precise parameters of customer agreements with AWS can have an impact on recovery financing. Organizations should evaluate their contractual agreements, service agreements, and terms of use to understand both parties' obligations and responsibilities in the event of a cyber incident.

Organizations, Amazon Web Services frequently set aside funds for cybersecurity, incident response, and catastrophe recovery. These budgets may include costs associated with responding to and recovering from a cyber attacks.

Some firms have emergency reaction funds or contingency budgets on hand to deal with unforeseen catastrophes like cyber assaults. These money can be utilized to cover the costs of emergency reaction and recovery. Depending on the nature of the incident, firms may seek grants and money from government

agencies, industry groups, or charitable organizations that support cybersecurity initiatives and recovery efforts. During the recovery stage, organizations may request financial assistance from banks, lenders, or financial institutions to bridge funding shortfalls. This could include loans or credit lines.

10 Role of NICC/NCICC

The NICC and NCCIC are two important DHS agencies that work to protect the nation's critical infrastructure from cyber threats. While Amazon AWS is not directly under their jurisdiction, its role in supporting critical infrastructure organizations makes it important for the company to collaborate with these agencies on cybersecurity initiatives.

The NICC acts as a coordinating point for the United States government's reaction to incidents involving critical infrastructure. It improves information sharing, coordination, and response activities between federal, state, municipal, tribal, and territory governments, as well as commercial sector partners.

The NCCIC is an important part of the DHS's cybersecurity initiatives. It acts as a central point for the integration of cybersecurity information, the dissemination of threat intelligence, and the coordination of incident response efforts. [20]

While Amazon Web Services (AWS) is a private cloud computing service and is not one of the critical infrastructure sectors regulated by NICC, it does play an important role in supporting other critical infrastructure organizations and enterprises that rely on cloud services for their operations. AWS has its own security and compliance mechanisms in place, and it collaborates with a variety of government agencies and organizations to ensure the security and resilience of its services.

Collaboration and information exchange with bodies such as NICC and NCCIC may occur as part of broader national cybersecurity efforts if there are specific issues or activities connected to the cybersecurity of critical infrastructure that involve AWS.

The important functions performed by both the agencies includes :

- Monitors and evaluates essential infrastructure sectors' operational status.
- During emergencies or disturbances, coordinates incident response and recovery operations.
- Facilitates information sharing and collaboration across partners in the public and private sectors.
- Situational awareness and threat intelligence are provided.
- Cyber threats and vulnerabilities affecting the nation's critical infrastructure are monitored and analyzed.
- Coordination of cybersecurity information sharing among government agencies, commercial sector entities, and foreign partners.
- Assists with incident response and coordinating actions to mitigate cyber dangers.
- Provides a variety of cybersecurity services, including as vulnerability assessments and data sharing initiatives.

11 Cybersecurity Workforce Recommendations

The IT sector of the critical infrastructure is so closely connected with the other sectors that for a strong and resilient defense against evolving threats, there is a need to improve the cybersecurity workforce in Amazon AWS data centers.

The workforce joining the new team should go through continuous cybersecurity training courses for staff members who operate in AWS data centers. This guarantees that the workforce is knowledgeable on the most recent advancements in technology, security threats, and best practices. High level leadership should encourage and assist staff members in obtaining cybersecurity certifications that are relevant to their roles in the data centers. AWS Certified Security Specialty and Certified Information Systems Security Professional (CISSP) certifications, for example, can improve knowledge and abilities. Encourage cross-functional training to make that cybersecurity experts in AWS data centers are knowledgeable on a wide range of security topics. This promotes cooperation and adaptability in addressing various security issues. The assessment of a workers' skills on a regular basis to find out where they could need more growth or training. By taking a proactive stance, the cybersecurity team is certain to have the know-how to handle new threats. [21] If the attempts to hack the data centers is any indication, a incident response strategy that is unique each to Amazon AWS data centers needs to created and updated on a regular basis.

12 Conclusion

The analysis gave us the exact risk, threat, vulnerability of the two most critical nodes in the AWS US region data centers. The west coast region which consist of centers like Oregon, California are at risk of a physical attack because they are more prone to earthquakes, a possibility of bombing and other server failures. While, the east coast region of New York, Massachusetts are more prone to the natural disasters like floods, storms, etc. This region is also threatened by a possible bombing and other internal failures. We need to keep in mind that all these regions also faces a possibility of cyber - attacks, intrusions and other attacks. The utilization of these techniques like MBRA Tool and Fault Tree Analysis provided a comprehensive understanding of the attacks and vulnerabilities inside the IT industry. This knowledge will result in enhanced resilience, more effective security measures, and a lower chance of successful physical and cyberattacks.

With the help of python script and excel calculations, we were able to deduce the eigen vectors of the network graph created by us. These graph further help us in identifying the number of links, nodes that can be removed or are necessary for the proper functioning of the whole network in case there is an possible failure or other catastrophe. The spectral radius, exceedance probability, fractal dimension we were clearly able to identify the risk and resilience associated with the nodes, links and overall network.

Lastly, taking in the budget is also a major factor. The different costs associated like, response, prevention and consequence costs help us better divide the funds to the right sources. These factors can provide valuable insights, offer diverse threat intelligence, and contribute to a more robust security posture. By proper budgeting of finances, resource allocation, and efforts we can easily restore normal operations and resilience after an adverse event.

In the end, the industry with the help of government agencies ought to improve its capacity to react to and recover from occurrences, reducing any harm and interruptions to the critical infrastructure of the country. And, with the help of proper guidelines, public-private collaborations, mitigation of risks at every step, keeping ourselves aware of the emerging technologies and threats, we can came up and defend ourselves better in the future.

13 References

[1] https://www.cisa.gov/sites/default/files/2023-01/nipp-ssp-information-technology-2016-508%20%281%29.pdf

[2] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/information-technology-sector

[3] https://aws.amazon.com/

[4] https://aws.amazon.com/about-aws/global-infrastructure/

[5] https://www.datacenterdynamics.com/en/news/right-wing-terrorist-gets-10-years-for-plotting-to-blow-up-aws-data-center/#:~:text=Seth%20Aaron%20Pendley%20has%20been,He%20pled%20guilty%20in%20June.

[6]https://www.cnbc.com/2021/12/09/how-the-aws-outage-wreaked-havoc-across-the-us.html

[7]https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf

8] https://www.eia.gov/

[9] https://www.speedtest.net/global-index

[10] https://kpmg.com/us/en/articles/2023/global-withholding-taxes-guide.html

[11] https://www.eiu.com/n/solutions/country-risk-model/

[12] https://www.irena.org/

[13] https://reliefweb.int/report/world/worldriskreport-2022-focus-digitalization

[14] https://www.worldenergy.org/

[15] https://www.wri.org/data/aqueduct-water-risk-atlas

[16] https://www.outlookindia.com/magazine/story/the-13-dns-root-servers/229231

[17] MBRA Users Guide_v2.1.pd Book

[18] https://www.anomali.com/blog/targeted-attack-vs-untargeted-attack-knowing-the-difference

[19] https://www.hackerone.com/knowledge-center/principles-threats-and-solutions

[20] https://www.cisa.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf

[21] https://niccs.cisa.gov/workforce-development/nice-framework

14 Appendix

Adjacency Matrix	Colorado	Florida	Massachusetts	Montana	Minnesota	Missouri	New Mexico	North California	Ohio	Oregon	Texas	US-East-1	US-West-2	Washington
Colorado	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Florida	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Massachusetts	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Montana	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Minnesota	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Missouri	0	0	0	0	0	0	0	0	0	0	0	1	0	0
New Mexico	0	0	0	0	0	0	0	0	0	0	0	0	1	0
North California	0	0	0	0	0	0	0	0	0	1	0	0	1	0
Ohio	0	0	0	0	0	0	0	0	0	1	0	1	0	0
Oregon	0	0	0	0	0	0	0	1	1	0	0	0	1	0
Texas	0	0	0	0	0	0	0	0	0	0	0	1	0	0
US-East-1	0	1	1	0	1	1	0	0	1	0	1	0	1	0
US-West-2	1	0	0	1	0	0	1	1	0	1	0	1	0	1
Washington	0	0	0	0	0	0	0	0	0	0	0	0	1	0

Table 14.1 Adjacency Matrix for the Nodes:

	Nodes	Links /Node Degree	Network Degree	Average/ Mean Degree	Spectral Radius	Link Robustness	Node Robustness	Blocking Node
	Colorado	1						
	Florida	1						
	Massachusetts	1						
	Montana	1						
	Minnesota	1						
	Missouri	1						
	New Mexico	1						
	North California	2						
	Ohio	2						
	Oregon	3						
	Texas	1						
	US-East-1	7						
	US-West-2	7						
	Washington	1						
	Total	30	7	2.14	3.22	6.67%	68.94%	31.06%
		Or 2xLinks				2	9.65	4.35
						Number of Links that can be removed	Number of Nodes that can be removed	Blocking nodes that can't be removed

Table 14.2 Numerical Parameters for the Nodes:

Node	Degree	Degree Centrality	Betweenness Centrality	Eigenvector Centrality
Colorado	1	0.07	0.00	0.16
Florida	1	0.07	0.00	0.14
Massachusetts	1	0.07	0.00	0.14
Montana	1	0.07	0.00	0.16
Minnesota	1	0.07	0.00	0.14
Missouri	1	0.07	0.00	0.14
New Mexico	1	0.07	0.00	0.16
North California	2	0.15	0.00	0.27
Ohio	2	0.15	0.03	0.25
Oregon	3	0.23	0.04	0.33
Texas	1	0.07	0.00	0.14
US-East-1	7	0.53	0.67	0.47
US-West-2	7	0.53	0.65	0.54
Washington	1	0.07	0.00	0.16

Table 14.3 Node Network Characterization

Python Script for the Calculation of Spectral Radius, Eigen values:

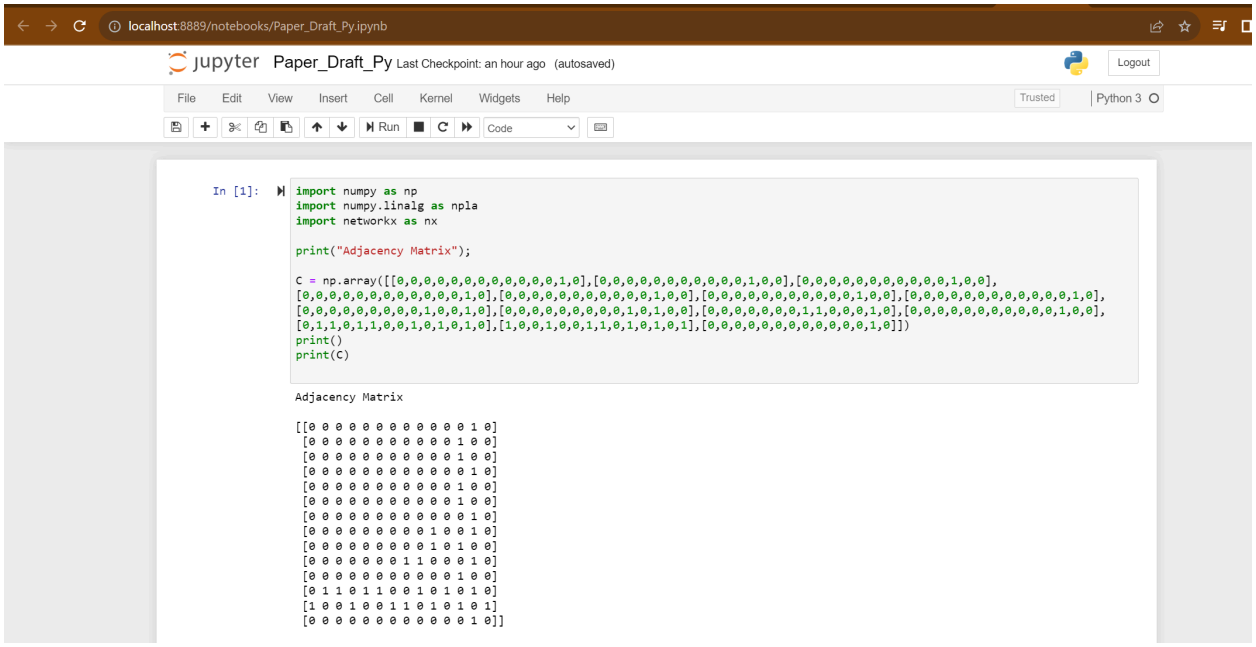
```
#!/usr/bin/env python
# coding: utf-8
# In[2]:
import numpy as np
import numpy.linalg as npla
import networkx as nx
print("Adjacency Matrix");
C = np.array([[0,0,0,0,0,0,0,0,0,0,0,0,1,0],[0,0,0,0,0,0,0,0,0,0,0,1,0,0],[0,0,0,0,0,0,0,0,0,0,0,1,0,0],
[0,0,0,0,0,0,0,0,0,0,0,0,1,0],[0,0,0,0,0,0,0,0,0,0,0,1,0,0],[0,0,0,0,0,0,0,0,0,0,1,0,0],[0,0,0,0,0,0,0,0,0,0,0,
0,1,0],
[0,0,0,0,0,0,0,0,0,1,0,0,1,0],[0,0,0,0,0,0,0,0,0,1,0,1,0,0],[0,0,0,0,0,0,0,1,1,0,0,0,1,0],[0,0,0,0,0,0,0,0,0,0,0,
1,0,0],
[0,1,1,0,1,1,0,0,1,0,1,0,1,0],[1,0,0,1,0,0,1,1,0,1,0,1,0,1],[0,0,0,0,0,0,0,0,0,0,0,0,1,0]])
print()
print(C)
# In[5]:
RowColorado = C[0,:]
RowFlorida = C[1,:]
RowMassachusetts = C[2,:]
RowMontana = C[3,:]
RowMinnesota = C[4,:]
RowMissouri = C[5,:]
RowNew_Mexico = C[6,:]
RowNorth_California = C[7,:]
RowOhio = C[8,:]
RowOregon = C[9,:]
RowTexas = C[10,:]
RowUS_East1 = C[11,:]
```

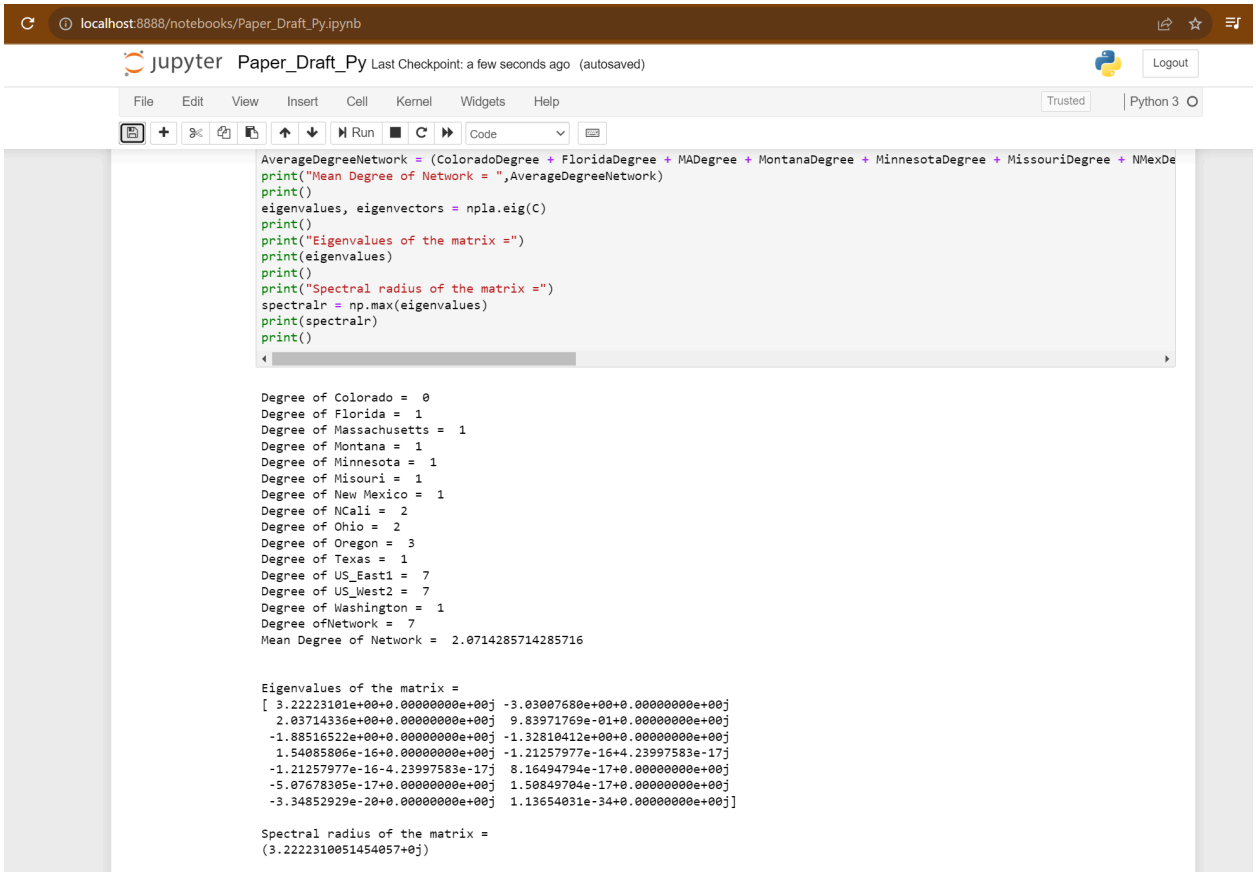
```
RowUS_West2 = C[12,:]

RowWashington = C[13,:]

print()

ColoradoDegree = RowColorado[0] + RowColorado[1] + RowColorado[2] + RowColorado[3] +
RowColorado[4] + RowColorado[5] + RowColorado[6] + RowColorado[7] + RowColorado[8] +
RowColorado[9] + RowColorado[10] + RowColorado[11] + RowColorado[13]

print("Degree of Colorado = ",ColoradoDegree)


FloridaDegree = RowFlorida[0] + RowFlorida[1] + RowFlorida[2] + RowFlorida[3] + RowFlorida[4] +
RowFlorida[5] + RowFlorida[6] + RowFlorida[7] + RowFlorida[8] + RowFlorida[9] + RowFlorida[10] +
RowFlorida[11] + RowFlorida[12] + RowFlorida[13]

print("Degree of Florida = ",FloridaDegree)


MADegree = RowMassachusetts[0] + RowMassachusetts[1] + RowMassachusetts[2] +
RowMassachusetts[3] + RowMassachusetts [4] + RowMassachusetts [5] + RowMassachusetts [6] +
RowMassachusetts [7] + RowMassachusetts [8] + RowMassachusetts [9] + RowMassachusetts [10] +
RowMassachusetts [11] + RowMassachusetts [12] + RowMassachusetts [13]

print("Degree of Massachusetts = ",MADegree)


MontanaDegree = RowMontana[0] + RowMontana[1] + RowMontana[2] + RowMontana[3] +
RowMontana[4] + RowMontana[5] + RowMontana[6] + RowMontana[7] + RowMontana[8] +
RowMontana[9] + RowMontana[10] + RowMontana[11] + RowMontana[12] + RowMontana[13]

print("Degree of Montana = ",MontanaDegree)


MinnesotaDegree = RowMinnesota[0] + RowMinnesota[1] + RowMinnesota[2] + RowMinnesota[3] +
RowMinnesota[4] + RowMinnesota[5] + RowMinnesota[6] +  RowMinnesota[7] + RowMinnesota[8] +
RowMinnesota[9] + RowMinnesota[10] + RowMinnesota[11] + RowMinnesota[12] +
RowMinnesota[13]

print("Degree of Minnesota = ",MinnesotaDegree)


MissouriDegree = RowMissouri[0] + RowMissouri[1] + RowMissouri[2] + RowMissouri[3] +
RowMissouri[4] + RowMissouri[5] + RowMissouri[6] + RowMissouri[7] + RowMissouri[8] +
RowMissouri[9] + RowMissouri[10] + RowMissouri[11] + RowMissouri[12] + RowMissouri[13]

print("Degree of Misouri = ",MissouriDegree)


NMexDegree = RowNew_Mexico[0] + RowNew_Mexico[1] + RowNew_Mexico[2] +
RowNew_Mexico[3] + RowNew_Mexico[4] + RowNew_Mexico[5] + RowNew_Mexico[6] +
```

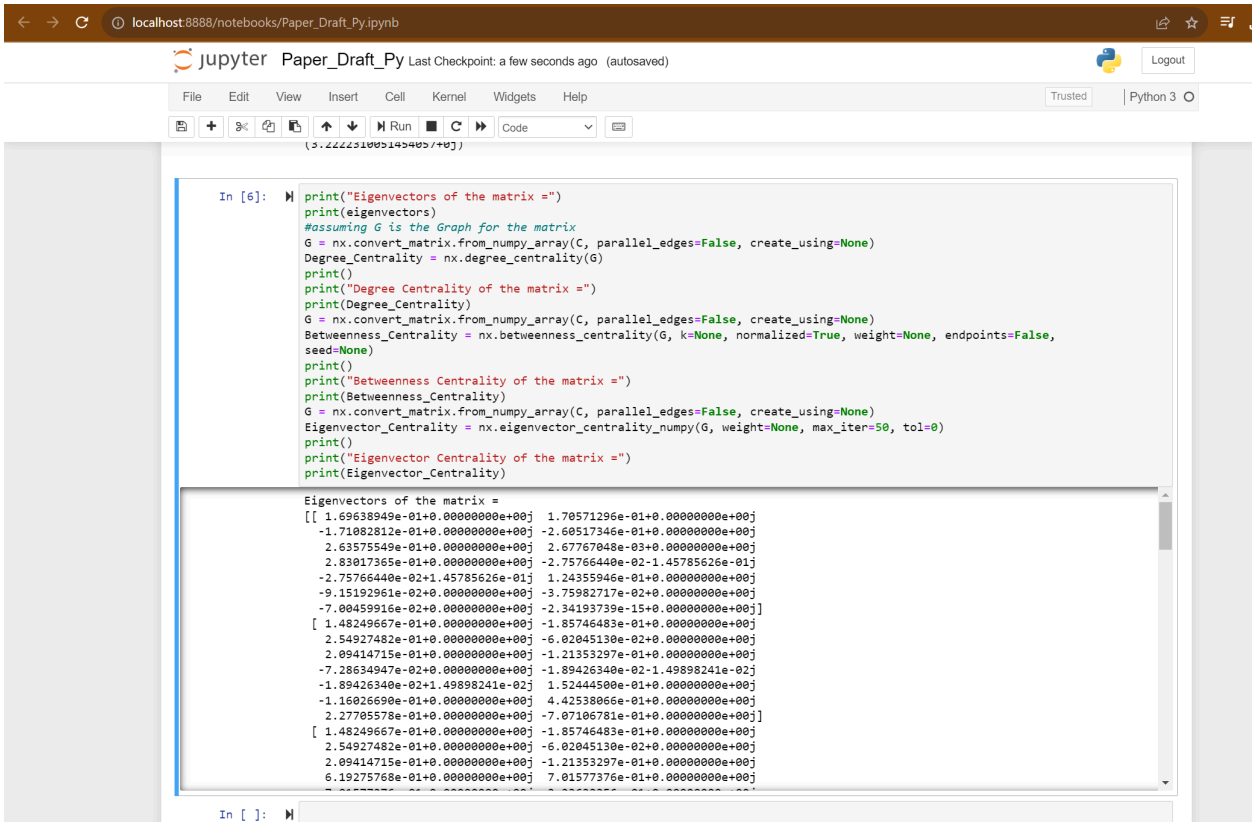
```
RowNew_Mexico[7] + RowNew_Mexico[8] + RowNew_Mexico[9] + RowNew_Mexico[10] +
RowNew_Mexico[11] + RowNew_Mexico[12] + RowNew_Mexico[13]

print("Degree of New Mexico = ",NMexDegree)


NCaliDegree = RowNorth_California[0] + RowNorth_California[1] + RowNorth_California[2] +
RowNorth_California[3] + RowNorth_California[4] + RowNorth_California[5] +
RowNorth_California[6] + RowNorth_California[7] + RowNorth_California[8] +
RowNorth_California[9] + RowNorth_California[10] + RowNorth_California[11] +
RowNorth_California[12] + RowNorth_California[13]

print("Degree of NCali = ",NCaliDegree)


OhioDegree = RowOhio[0] + RowOhio[1] + RowOhio[2] + RowOhio[3] + RowOhio[4] + RowOhio[5] +
RowOhio[6] + RowOhio[7] + RowOhio[8] + RowOhio[9] + RowOhio[10] + RowOhio[11] +
RowOhio[12] + RowOhio[13]

print("Degree of Ohio = ",OhioDegree)


OregonDegree = RowOregon[0] + RowOregon[1] + RowOregon[2] + RowOregon[3] + RowOregon[4] +
RowOregon[5] + RowOregon[6] + RowOregon[7] + RowOregon[8] + RowOregon[9] + RowOregon[10]
+ RowOregon[11] + RowOregon[12] + RowOregon[13]

print("Degree of Oregon = ",OregonDegree)


TexasDegree = RowTexas[0] + RowTexas[1] + RowTexas[2] + RowTexas[3] +  RowTexas[4] +
RowTexas[5] + RowTexas[6] + RowTexas[7] + RowTexas[8] + RowTexas[9] + RowTexas[10] +
RowTexas[11] + RowTexas[12] + RowTexas[13]

print("Degree of Texas = ",TexasDegree)


US_East1Degree = RowUS_East1[0] + RowUS_East1[1] + RowUS_East1[2] + RowUS_East1[3] +
RowUS_East1[4] + RowUS_East1[5] + RowUS_East1[6] + RowUS_East1[7] + RowUS_East1[8] +
RowUS_East1[9] + RowUS_East1[10] + RowUS_East1[11] + RowUS_East1[12] + RowUS_East1[13]

print("Degree of US_East1 = ",US_East1Degree)


US_West2Degree = RowUS_West2[0] + RowUS_West2[1] + RowUS_West2[2] + RowUS_West2[3] +
RowUS_West2[4] + RowUS_West2[5] + RowUS_West2[6] + RowUS_West2[7] + RowUS_West2[8] +
RowUS_West2[9] + RowUS_West2[10] + RowUS_West2[11] + RowUS_West2[12] +
RowUS_West2[13]

print("Degree of US_West2 = ",US_West2Degree)
```

```
WashingtonDegree = RowWashington[0] + RowWashington[1] + RowWashington[2] +
RowWashington[3] + RowWashington[4] + RowWashington[5] + RowWashington[6] +
RowWashington[7] + RowWashington[8] + RowWashington[9] + RowWashington[10] +
RowWashington[11] + RowWashington[12] + RowWashington[13]

print("Degree of Washington = ",WashingtonDegree)


NetworkDegree = max(ColoradoDegree, FloridaDegree, MADegree, MontanaDegree, MinnesotaDegree,
MissouriDegree, NMexDegree, NCaliDegree, OhioDegree, OregonDegree, TexasDegree,
US_East1Degree, US_West2Degree, WashingtonDegree)

print("Degree ofNetwork = ",NetworkDegree)


AverageDegreeNetwork = (ColoradoDegree + FloridaDegree + MADegree + MontanaDegree +
MinnesotaDegree + MissouriDegree + NMexDegree + NCaliDegree + OhioDegree + OregonDegree +
TexasDegree + US_East1Degree + US_West2Degree + WashingtonDegree) / len(C)

print("Mean Degree of Network = ",AverageDegreeNetwork)

print()

eigenvalues, eigenvectors = npla.eig(C)

print()

print("Eigenvalues of the matrix =")

print(eigenvalues)

print()

print("Spectral radius of the matrix =")

spectralr = np.max(eigenvalues)

print(spectralr)

print()

# In[6]:

print("Eigenvectors of the matrix =")

print(eigenvectors)

#assuming G is the Graph for the matrix

G = nx.convert_matrix.from_numpy_array(C, parallel_edges=False, create_using=None)

Degree_Centrality = nx.degree_centrality(G)

print()

print("Degree Centrality of the matrix =")

print(Degree_Centrality)
```

```
G = nx.convert_matrix.from_numpy_array(C, parallel_edges=False, create_using=None)

Betweenness_Centrality = nx.betweenness_centrality(G, k=None, normalized=True, weight=None, endpoints=False,

seed=None)

print()

print("Betweenness Centrality of the matrix =")

print(Betweenness_Centrality)

G = nx.convert_matrix.from_numpy_array(C, parallel_edges=False, create_using=None)

Eigenvector_Centrality = nx.eigenvector_centrality_numpy(G, weight=None, max_iter=50, tol=0)

print()

print("Eigenvector Centrality of the matrix =")

print(Eigenvector_Centrality)
```




localhost:8888/notebooks/Paper_Draft_Py.ipynb
jupyter Paper_Draft_Py Last Checkpoint: a few seconds ago (autosaved)
Logout
File Edit View Insert Cell Kernel Widgets Help
Trusted
Python 3
Run
Code
AverageDegreeNetwork = (ColoradoDegree + FloridaDegree + MADegree + MontanaDegree + MinnesotaDegree + MissouriDegree + NMexDe
print("Mean Degree of Network = ",AverageDegreeNetwork)
print()
eigenvalues, eigenvectors = npla.eig(C)
print()
print("Eigenvalues of the matrix =")
print(eigenvalues)
print()
print("Spectral radius of the matrix =")
spectralr = np.max(eigenvalues)
print(spectralr)
print()
Degree of Colorado = 0
Degree of Florida = 1
Degree of Massachusetts = 1
Degree of Montana = 1
Degree of Minnesota = 1
Degree of Misouri = 1
Degree of New Mexico = 1
Degree of NCali = 2
Degree of Ohio = 2
Degree of Oregon = 3
Degree of Texas = 1
Degree of US_East1 = 7
Degree of US_West2 = 7
Degree of Washington = 1
Degree ofNetwork = 7
Mean Degree of Network = 2.0714285714285716
Eigenvalues of the matrix =
[3.22223101e+00+0.00000000e+00j -3.03007680e+00+0.00000000e+00j
2.03714336e+00+0.00000000e+00j 9.83971769e-01+0.00000000e+00j
-1.88516522e+00+0.00000000e+00j -1.32810412e+00+0.00000000e+00j
1.54085806e-16+0.00000000e+00j -1.21257977e-16+4.23997583e-17j
-1.21257977e-16-4.23997583e-17j 8.16494794e-17+0.00000000e+00j
-5.07678305e-17+0.00000000e+00j 1.50849704e-17+0.00000000e+00j
-3.34852929e-20+0.00000000e+00j 1.13654031e-34+0.00000000e+00j]
Spectral radius of the matrix =
(3.2222310051454057+0j)


localhost:8888/notebooks/Paper_Draft_Py.ipynb
jupyter Paper_Draft_Py Last Checkpoint: a few seconds ago (autosaved)
Logout
File Edit View Insert Cell Kernel Widgets Help
Trusted
Python 3
Run
Code
In [6]:
print("Eigenvectors of the matrix =")
print(eigenvectors)
#assuming G is the Graph for the matrix
G = nx.convert_matrix.from_numpy_array(C, parallel_edges=False, create_using=None)
Degree_Centrality = nx.degree_centrality(G)
print()
print("Degree Centrality of the matrix =")
print(Degree_Centrality)
G = nx.convert_matrix.from_numpy_array(C, parallel_edges=False, create_using=None)
Betweenness_Centrality = nx.betweenness_centrality(G, k=None, normalized=True, weight=None, endpoints=False,
seed=None)
print()
print("Betweenness Centrality of the matrix =")
print(Betweenness_Centrality)
G = nx.convert_matrix.from_numpy_array(C, parallel_edges=False, create_using=None)
Eigenvector_Centrality = nx.eigenvector_centrality_numpy(G, weight=None, max_iter=50, tol=0)
print()
print("Eigenvector Centrality of the matrix =")
print(Eigenvector_Centrality)
Eigenvectors of the matrix =
[[1.69638949e-01+0.00000000e+00j 1.70571296e-01+0.00000000e+00j
-1.71082812e-01+0.00000000e+00j -2.60517346e-01+0.00000000e+00j
2.63575549e-01+0.00000000e+00j 2.67767048e-03+0.00000000e+00j
2.83017365e-01+0.00000000e+00j -2.75766440e-02-1.45785626e-01j
-2.75766440e-02+1.45785626e-01j 1.24355946e-01+0.00000000e+00j
-9.15192961e-02+0.00000000e+00j -3.75982717e-02+0.00000000e+00j
-7.00459916e-02+0.00000000e+00j -2.34193739e-15+0.00000000e+00j]
[1.48249667e-01+0.00000000e+00j -1.85746483e-01+0.00000000e+00j
2.54927482e-01+0.00000000e+00j -6.02045130e-02+0.00000000e+00j
2.09414715e-01+0.00000000e+00j -1.21353297e-01+0.00000000e+00j
-7.28634947e-02+0.00000000e+00j -1.89426340e-02-1.49898241e-02j
-1.89426340e-02+1.49898241e-02j 1.52444500e-01+0.00000000e+00j
-1.16026690e-01+0.00000000e+00j 4.42538066e-01+0.00000000e+00j
2.27705578e-01+0.00000000e+00j -7.07106781e-01+0.00000000e+00j]
[1.48249667e-01+0.00000000e+00j -1.85746483e-01+0.00000000e+00j
2.54927482e-01+0.00000000e+00j -6.02045130e-02+0.00000000e+00j
2.09414715e-01+0.00000000e+00j -1.21353297e-01+0.00000000e+00j
6.19275768e-01+0.00000000e+00j 7.01577376e-01+0.00000000e+00j
In [ ]:

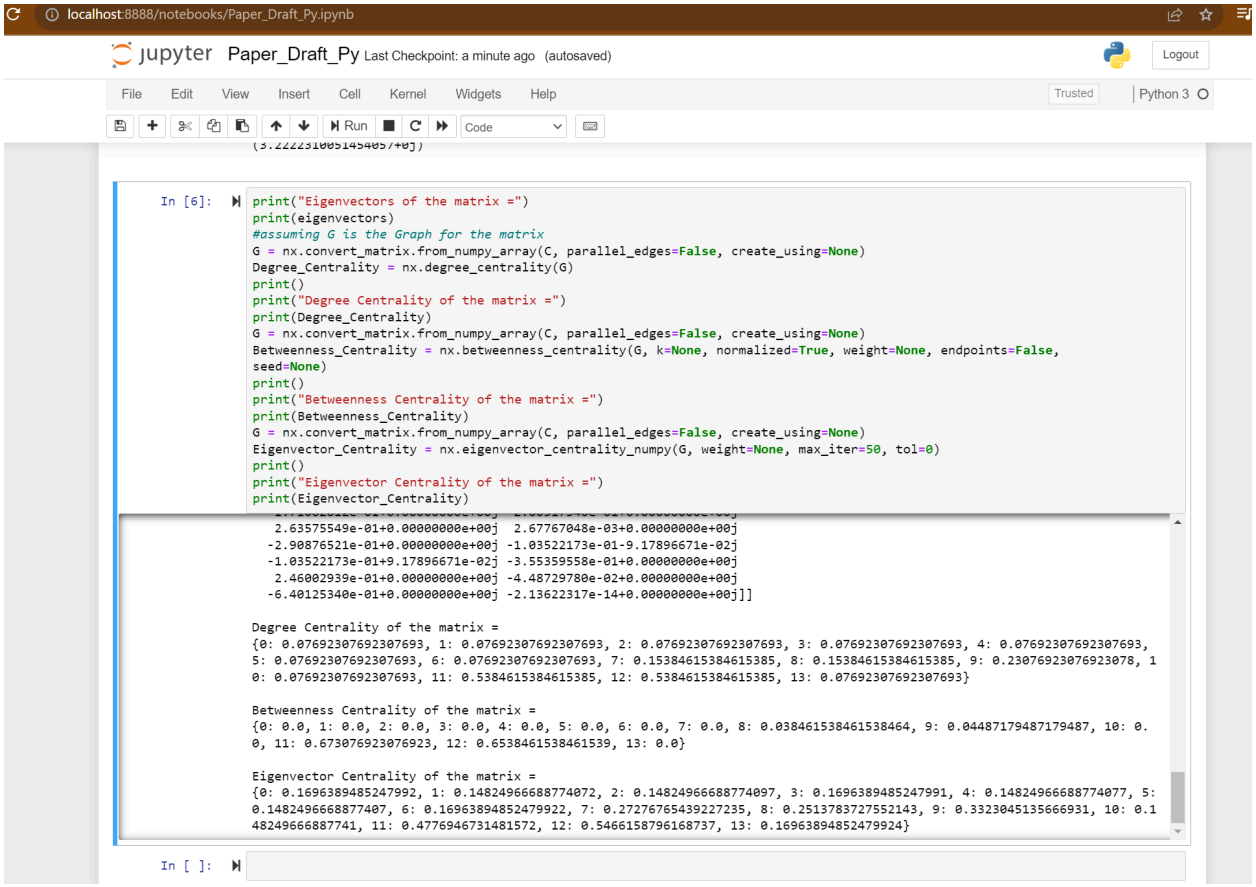


Fig 14.1 Screenshots showing the python script output

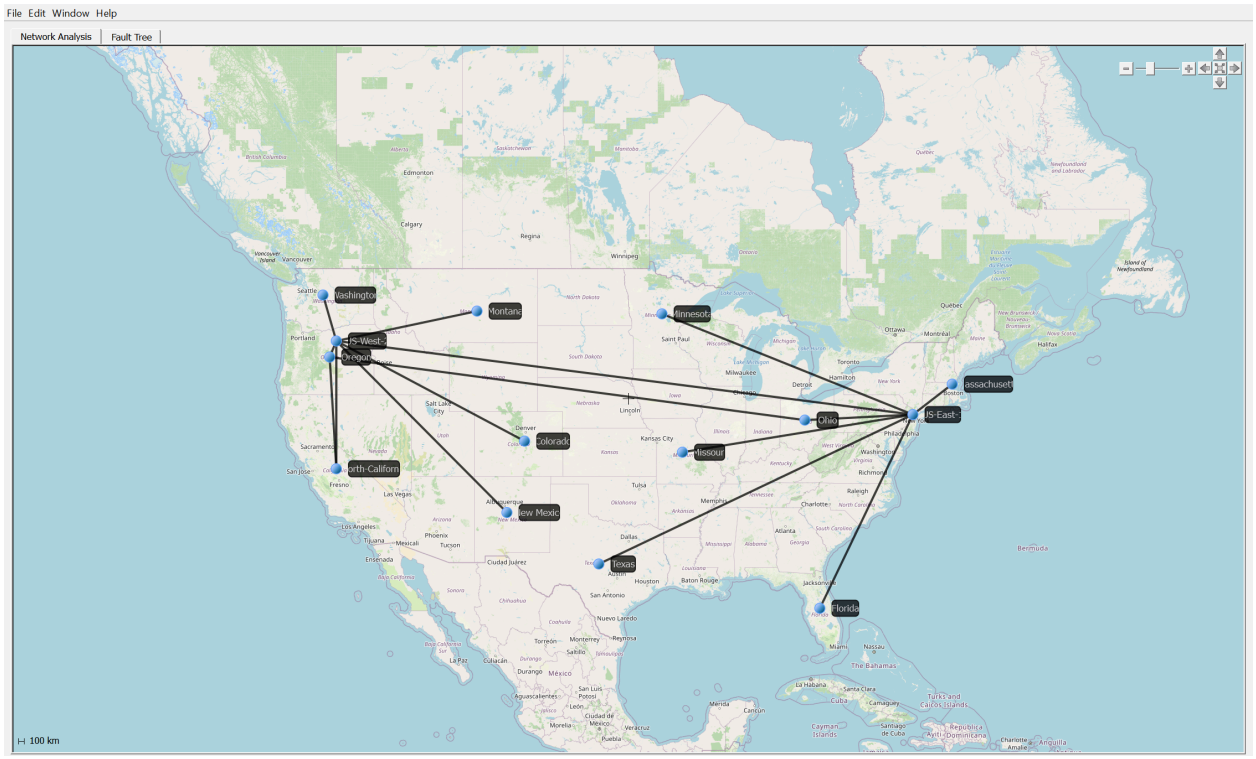


Fig 14.2 Network Graph

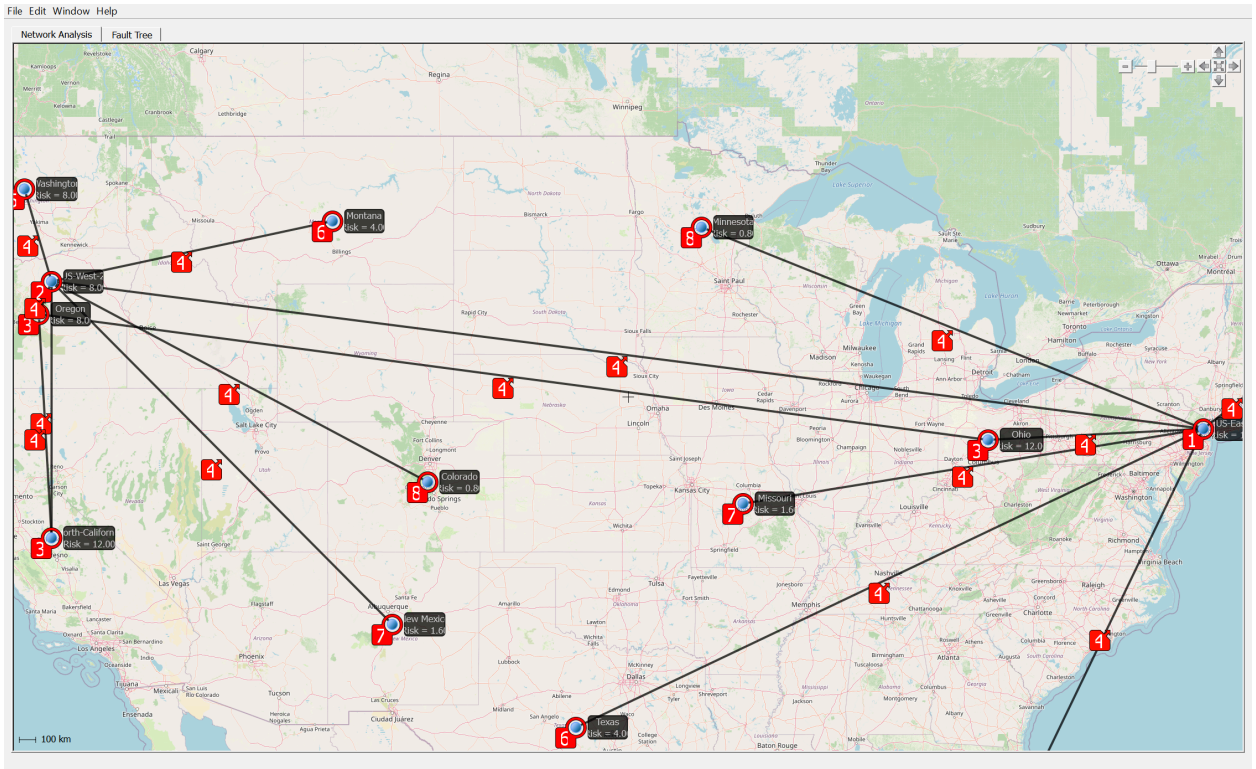


Fig 14.3 Screenshot showing Critical Nodes, namely US-East-1 and US-West-1

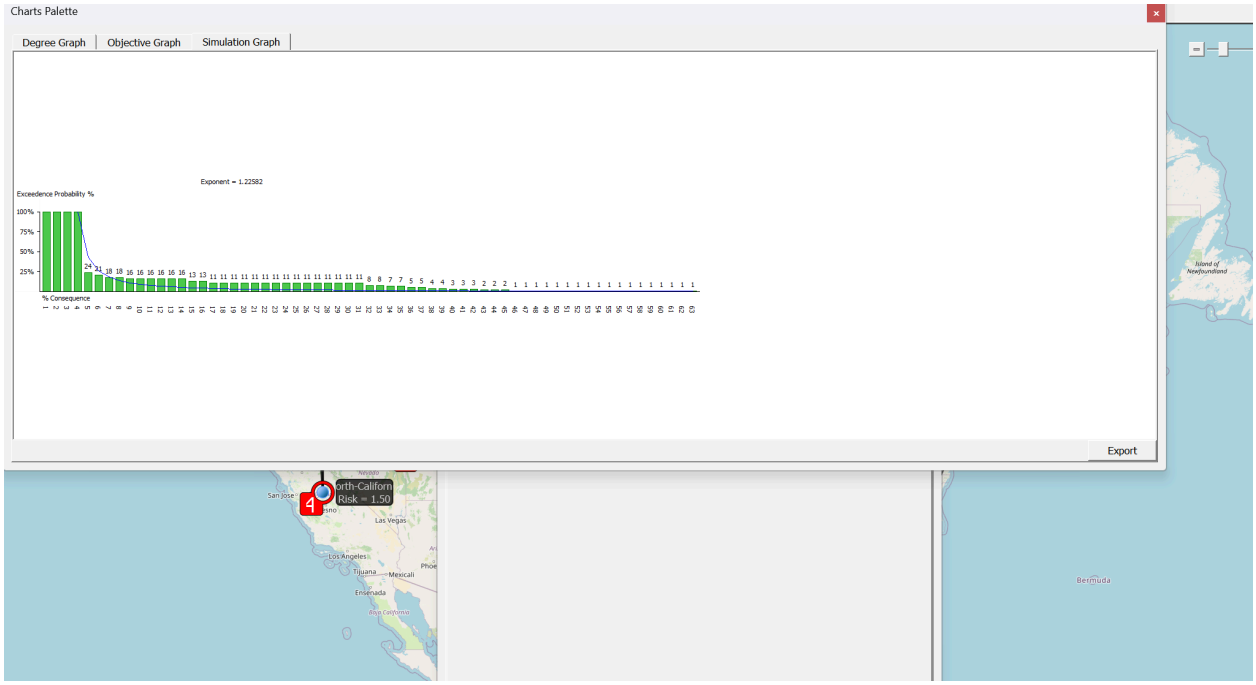


Fig 14.4 Running the graph simulation for calculating the Resilience Equation

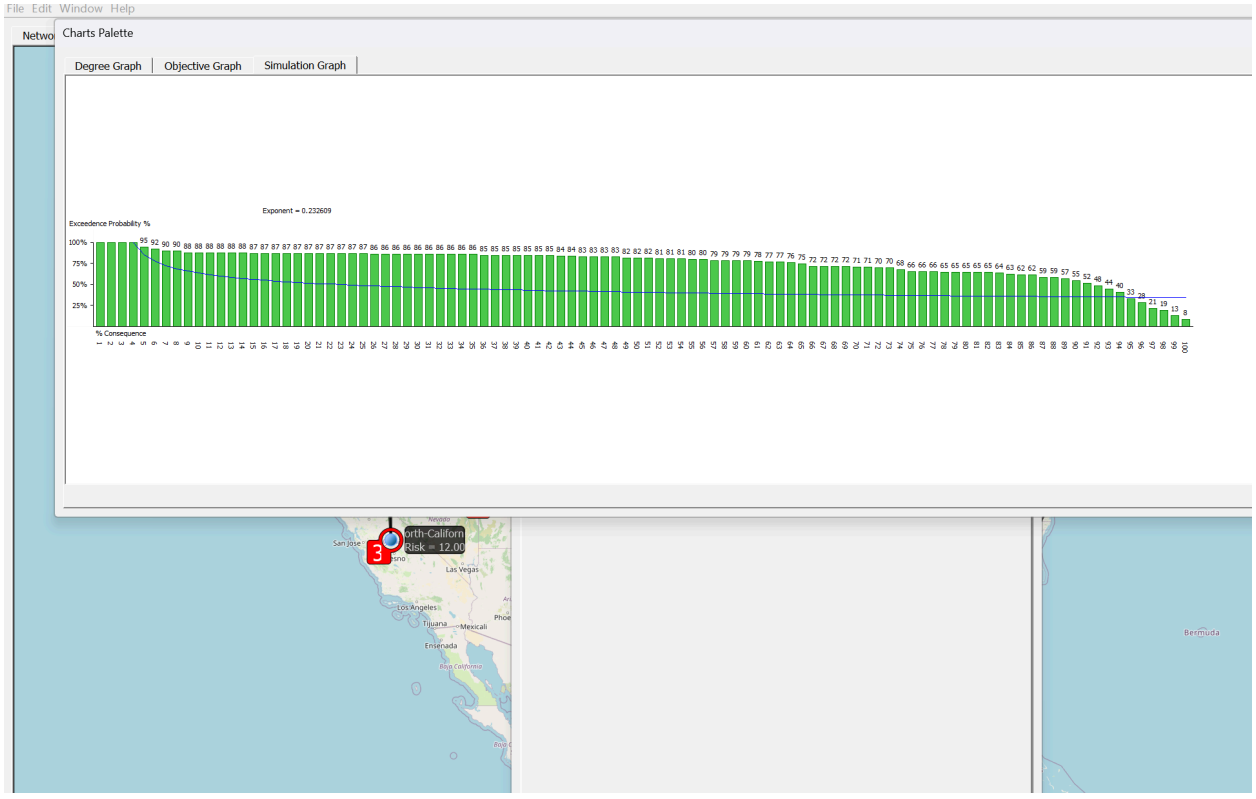


Fig 14.5 Running the graph simulation for calculating the Resilience Equation

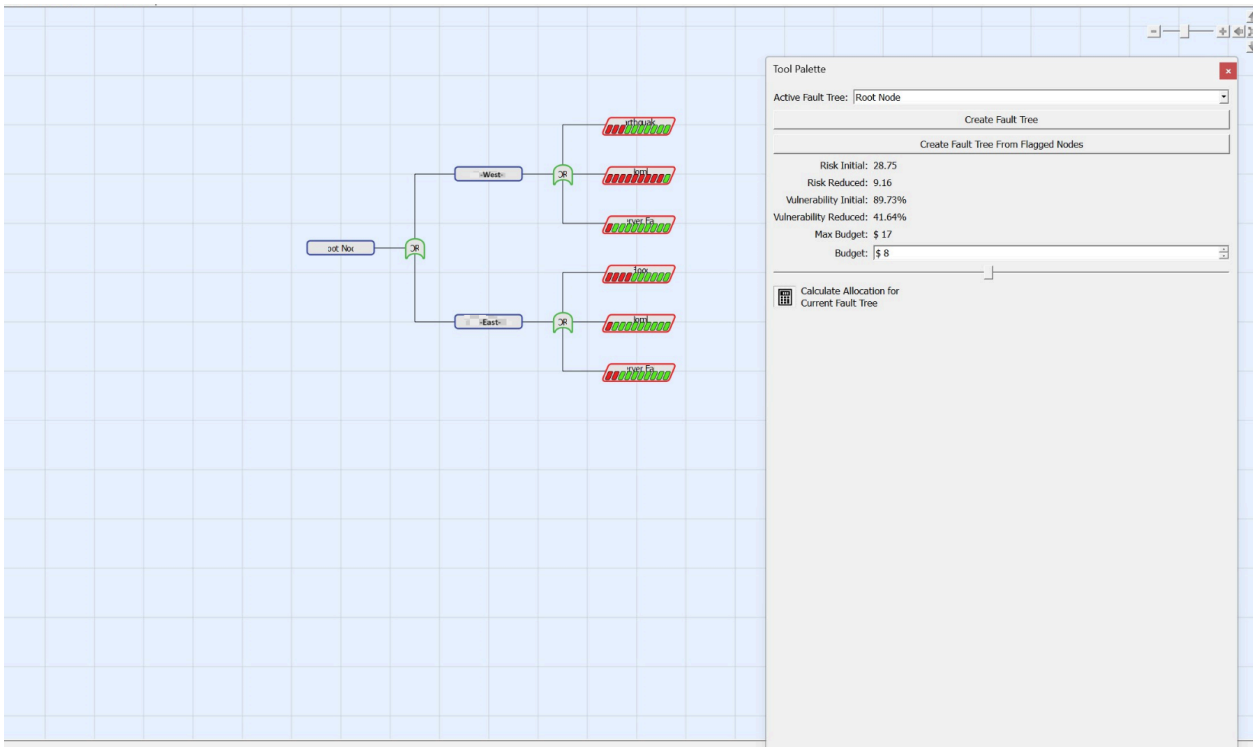


Fig 14.6 FTA Analysis after budget allocation