ARTICLE

Cite This. J.of Data Sci. and Informa Technol .2024, 1, 10-23

Sciforce

Journal of Data Science and Information Technology

Journal homepage.www.sciforce.org

Analyzing The Impact of Virtual Private Networks (VPNS) On Online Security Using The DEMATEL Method

Tejasvi Gorre*

* *Home Depot Management Company LLC, 2455 Paces Ferry Rd SE, Atlanta*

ARTICLE INFO

Article history.
Received 20240502
Received in revised form 20240515
Accepted 20240515
Available online 20240615

Keywords.
ExpressVPN;
NordVPN;
CyberGhost VPN;
DEMATEL.

ABSTRACT

A Virtual Private Network (VPN) is a technology that enhances online privacy and security by establishing a secure, encrypted connection between a user's device and a remote server. Acting as a protective tunnel, a VPN routes the user's internet traffic through this encrypted connection, shielding their data from potential cyber threats, surveillance, and unauthorized access. VPNs serve as powerful tools for safeguarding sensitive information, especially when using public Wi-Fi networks, as they prevent hackers or malicious entities from intercepting data transmissions. Additionally, VPNs allow users to mask their true IP address with that of the remote server, effectively anonymizing their online activities and bypassing geographical restrictions. Beyond security and anonymity, VPNs offer other practical benefits. They enable users to access region-restricted content, granting access to websites, services, and streaming platforms that might otherwise be unavailable in their location. Whether for personal use or business needs, VPNs have become integral in today's digital landscape, providing a reliable means of maintaining privacy, evading censorship, and fortifying online experiences. The significance of researching Virtual Private Networks (VPNs) lies in their pivotal role in modern cybersecurity and digital privacy. As online threats and data breaches continue to escalate, understanding the intricacies of VPN technology is crucial for developing advanced encryption techniques, improving network security protocols, and countering emerging cyber risks. Furthermore, VPN research contributes to enhancing user awareness about the importance of safeguarding personal information, aiding in the design of more effective privacy solutions for individuals, businesses, and organizations. By delving into VPNs, researchers can devise strategies to mitigate cyber threats and ensure a safer online environment for users worldwide.The DEMATEL (Decision-Making Trial and Evaluation Laboratory) method is a systematic approach used for analyzing complex interrelationships among various factors in a decision-making process. By visually mapping cause-and-effect relationships, DEMATEL helps to identify key drivers and dependencies within a system. It quantifies the strength and direction of these relationships, enabling decision-makers to prioritize factors based on their impact. This method finds applications in diverse fields such as business, engineering, healthcare, and environmental management, aiding in understanding intricate systems, formulating effective strategies, and making informed decisions in complex environments. ExpressVPN, NordVPN, CyberGhost VPN, Private Internet Access, Surfshark. ExpressVPN, NordVPN, CyberGhost VPN, Private Internet Access, Surfshark. calculate the average of the matrix and its threshold value (alpha) Alpha 0.873339618 If the T matrix value is greater than threshold value then bolds it. .

ISSN 2998-3592

∗Corresponding author. E-mail. tejasvigr@gmail.com

Introduction

Virtual Private Networks (VPNs) have gained significant popularity in business and security systems due to their cost-effective ability to establish secure connections. Both commercial and open-source VPN products are readily available, offering various configurations and characteristics to provide services. This article focuses on popular open-source Linux-based VPN solutions (OSLVs) and compares them based on network performance metrics like overhead, bandwidth usage, and latency/jitter. Additionally, features such as algorithm plugins and routing, as well as operational considerations including security and scalability, are evaluated. The goal is to identify the most feature-rich OSLV solution that excels in terms of performance. Test results suggest that while a single OSLV solution may not stand out as the best in all aspects, a combination of different VPN products could be used to achieve optimal performance and desired properties for data exchange[1]. Regarded as the foundational element of the Internet, expanding businesses view connectivity as a means to bolster revenue. Employing various methods, companies strive to ensure secure and efficient connections across geographically dispersed branches, strategic partners, and mobile employees. While numerous technologies are available, Internet-based virtual private networks (VPNs) have emerged as a highly secure and cost-effective solution to achieve these objectives [2]. VPNs superimpose a network overlay on top of the Internet's infrastructure using IP tunnels. These cryptographic channels offer robust protection and privacy for data transmission. For remote users, VPNs grant the advantages of private networks, allowing corporations to reap benefits like reduced costs and heightened security. A variety of commercial VPN products are widely accessible, differing primarily in cost and capabilities. However, researchers and developers have increasingly focused on raw VPN solutions, which provide open-source customization and cater to specialized hardware [3]. Linux-based VPN solutions have gained traction due to their affordability and customization options. They are embraced for their rapid deployment, compatibility with various operating systems, and extensive support communities. This article delves into evaluating the most popular Open-Source Linux-based VPN solutions (OSLVs). A comprehensive comparative study is presented, encompassing network performance, supported features, and operational considerations. The investigation identifies common flaws and opens avenues for future research [4]. Pena and Evans have researched different VPNs based on network performance and CPU usage, which are crucial metrics for high/low-speed networks. Although there are many features to consider (security, scalability, etc.), our work aims to comprehensively evaluate VPN solutions by comparing attributes and functionality. Through this analysis, we hope to shed light on the future challenges that must be addressed in this domain [5]. In summary, the role of VPNs in establishing secure, efficient, and cost-effective connections for business expansion cannot be overstated. The rapid evolution of technology, particularly Linux-based solutions, offers various options for organizations to harness the power of virtual private networks. This study contributes to a deeper understanding of the strengths and weaknesses of different VPN solutions, thus aiding businesses and researchers in making informed decisions [6]. IP technologies offer versatile and robust security associations, enabling the establishment of dynamic connections between endpoints, including within virtual private networks (VPNs). However, as the count of endpoints per VPN grows dramatically, the challenge of managing communication between these endpoints becomes increasingly complex. To address this issue and provide reliable and flexible connections, we introduce a new service interface termed a "pipe." This interface aggregates traffic and classifies it for endpoints within the VPN, ensuring performance guarantees [7]. For VPN clients, pipes offer essential benefits, including improved traffic management and enhanced flexibility for a set of endpoints. They integrate seamlessly with existing transport teams, leading to a reduction in access and the number of flows between endpoints. Despite the inherent complexity, the integration of pipes enhances multiplexing and connection management, particularly in point-to-point setups [8]. Quality of Service (QoS) is a crucial consideration, and the use of pipes to manage state and information reduces uncertainty in this aspect. Although managing resources is challenging, pipes, in conjunction with multiplexing techniques and online measurements, present a novel and efficient rescaling approach. This addresses the problem of resource management and QoS support, facilitating the effective handling of uncertainties in network scenarios [9]. In summary, the growth of endpoints within VPNs has posed challenges in managing communication and resource allocation. The introduction of pipes as a service interface demonstrates promise in ensuring reliable and flexible connections, particularly in scenarios with a multitude of endpoints. The integration of pipes enhances multiplexing and connection management while reducing uncertainties in resource management. This innovative approach has the potential to significantly improve the efficiency and performance of IP technologies in complex networking environments[10]. Virtual Private Network Services (VPNs) have been available in various formats for an extended period. More recently, they have gained significant attention within IP-based technologies such as Frame Relay, MPLS, and ATM networking. VPNs offer an alternative to traditional community-based networks and can be established

using personal lines or networks. They strive to provide comparable services, especially in terms of security.While considerable progress has been made in IP security technologies, there is a need to enhance VPN functionalities and security measures. Existing VPN service offerings are based on different technologies, each addressing individual privacy and security concerns. However, scant attention has been given to addressing management issues related to VPNs, particularly in resource allocation and supporting various mission-critical operations [11]. The importance of performance guarantees and providing service level support agreements (SLAs) is crucial in VPN service delivery. Personal lines have demonstrated the ability to offer performance isolation and bandwidth guarantees, thereby distinguishing VPN traffic from other flows. It is imperative that VPN services deliver performance that is comparable to the guaranteed bandwidth, while also considering loss and delay characteristics. Virtual Private Network (VPN) services are gaining traction among network operators, contributing to increased revenue shares. Operators require a flexible and bandwidth-capable model that can cater to diverse customer needs, considering factors like capacity, network topology, and communication methods. Traditionally, virtual private networks were designed to provide transportation required for point-to-point communication between pairs of VPN endpoints, creating "pipes" or connections [12]. Duffield et al. introduced the "tube model" as an alternative to the traditional approach, suggesting that the pipe model isn't feasible for scaling networks. In the tube model, each node in the network is equipped with multiple pipes to accommodate different resources and delivery needs. They argued that the tube model offers significant advantages when compared to the traditional pipe model, especially in handling varying levels of traffic and providing enhanced scalability. The tube model operates without the need for a traffic matrix, eliminating the necessity for complex calculations. Instead, it focuses on handling the total volume of traffic from and to the network, making it a more streamlined solution. This model has been proposed as a way to efficiently manage and optimize VPN services, ensuring better performance and adaptability to changing customer demands [13]. Virtual Private Networks (VPNs) cater to customers by offering secure and predictable network connections. These connections are shared over the network, ensuring safety and reliability. Recent advancements in VPNs have introduced the hose model, which enables flexible distribution of traffic at the endpoints. This paper introduces novel techniques for constructing VPNs using the pipeline model [14]. The proposed approach combines VPN endpoints using a tree structure, aiming to optimize the allocation of total bandwidth to edges of the VPN tree. While computing the VPN tree presents a challenging computational problem, we address this by introducing a specialized case where egress bandwidths are equal for each VPN endpoint. This enables the calculation of an optimal tree using a method with a time complexity of O(mn), where m and n represent the number of connections and nodes, respectively, in the network. We offer a new integer programming formulation for the common VPN tree computation problem and develop an algorithm based on the primary-dual method. Our algorithm generates VPN trees and test results reveal that they significantly reduce bandwidth requirements compared to visual representations. This includes the use of Steiner trees to connect VPN endpoints. The proposed method enhances the efficiency and performance of VPN networks, making them an attractive solution for secure and optimized network connections [15].

Material and Methods

Express VPN: Express VPN is renowned for its high-speed servers and wide network coverage across numerous countries. Its user-friendly interface makes it accessible to both beginners and experienced users. It offers strong encryption and a strict no-logs policy, ensuring users' online activities remain private. Express VPN's seamless compatibility with various devices and platforms makes it a versatile choice for secure browsing and accessing geo-blocked content.

NordVPN: NordVPN is known for its robust security features. It offers specialized servers such as Double VPN for enhanced encryption and Onion over VPN for added anonymity. The service includes a Cyber Sec feature that blocks malicious websites and ads. NordVPN also boasts a large server network, allowing users to access content from different regions securely.

CyberGhost VPN: CyberGhost VPN focuses on simplicity and ease of use. With pre-configured profiles for different purposes, users can easily choose the level of protection they need. The service provides strong encryption, a strict no-logs policy, and features like automatic Wi-Fi protection. CyberGhost's user-friendly interface makes it a great choice for those new to VPNs.

Private Internet Access (PIA): Private Internet Access emphasizes privacy with a no-logs policy, ensuring that user data is not stored. PIA offers strong encryption and a range of advanced security options. It allows users to customize encryption settings and provides features like split tunneling for directing specific traffic through the VPN. PIA's commitment to privacy appeals to users concerned about data retention.

Surfshark: Surfshark sets itself apart with unlimited simultaneous connections on a single subscription. This makes it ideal for households with multiple devices. Surfshark's CleanWeb feature blocks ads, trackers, and malware, enhancing both privacy and browsing speed. It offers strong encryption, a strict no-logs policy, and supports various platforms.

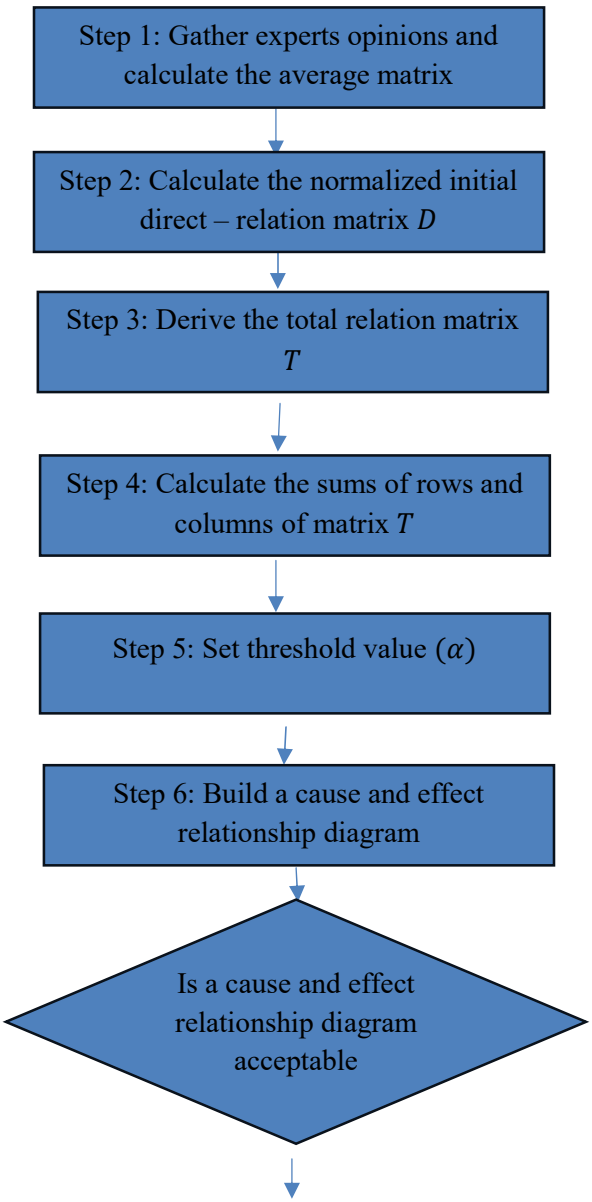
DEMATEL:

- the identification of cause-effect chain components of a complex matrix.
- It deals evaluating interdependent relationships among factors and finding the critical ones through a visual structural model.
- The most important property of the DEMATEL method used in the multi-criteria decision making (MCDM) Field is to construct interrelations between criteria.

The DEMATEL method is a specialized technique used to address specific problems by employing a hierarchical structure and problem-solving through interrelated components. It aids in identifying feasible solutions using structural modeling

- Decision making trail and evaluation laboratory (DEMATEL) is considered as an effective method for techniques, primarily by recognizing dependencies and causal relationships within an organization [16]. This method utilizes directional charts to chart causal relationships and interactions. Additionally, the DEMATEL approach is seamlessly integrated into emergency management and general management practices. Notably, the method doesn't require the conversion of vague numerical data into clear values prior to implementation. Built upon the foundational principles of DEMATEL, this approach employs a visual analysis technique to address and resolve issues. It takes the form of a causal diagram that visually represents the degree of influence between interconnected factors[17].

Flow Chat of DEMATEL:



Step 6: Build a cause and effect relationship diagram

This structured diagramming approach enhances understanding of relationships and complexities among systemic components, thereby facilitating the resolution of computer-related problems. The DEMATEL method effectively computes the consequences between criteria, facilitating the separation of intricate elements into sender and recipient organizations [18]. This separation aids in selecting an appropriate management strategy among alternative configurations. Explicit priority weights are derived from this process. The ZOGP model allows companies to efficiently allocate limited resources for optimal management system planning [19].Decision-makers must identify and manage strong legal framework obstacles to minimize their impact. The results derived from integrated ISM and DEMATEL methods are reasonably consistent. These integrated methods determine both the structure and interrelationships among barriers in e-waste management. In terms of group decision-making, the DEMATEL approach encountered challenges related to the relative weights assigned by decision-makers who weren't adequately considering team consensus. This discrepancy is largely attributed to the use of unstructured comparisons in methods like DEMATEL [20]. The DEMATEL method is widely recognized for analyzing overall relationships among factors and categorizing them based on cause-and-effect relationships. This article treats each source as a decision-making criterion, enhancing significance assessment by combining the DEMATEL technique with source theory. It alters the relationships between various sources as opposed to relying solely on experts' comparative criteria. In a study involving multiple-scale decision-making for outreach personnel programs, the DEMATEL method was utilized alongside a new cluster-weighted system. This approach aimed to visualize intricate relationships and measure criterion influence. Buyukozkan and Ozturk introduced an innovative method integrating DEMATEL and Six Sigma for prioritizing technology projects and logistics initiatives in companies [21].

Step 1. Make a matrix average through computing. Each responder was asked to rate the direct influence of any two elements using an integer score between 0 and 3, where 0 represents "no influence," 1 represents "low influence," 2 represents "medium influence," 3 represents "high influence," and 4 represents “very high influence” respectively. The notation xij reflects the respondent's opinion of how much factor I influences factor j. The diagonal elements are set to zero for I = j.

$$A_{ij} = \begin{bmatrix} 0 & a_{12} & \cdots & x_{1n} \\ x_{21} & 0 & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & 0 \end{bmatrix}$$

Step 2. Calculate the normalized initial direct-relation matrix. Normalize initial direct-relation matrix D is calculated by

$$Y = k \times A$$

$$k = \frac{1}{\max\limits_{1 \le i \le n} \sum_{j=1}^{n} a_{ij}} \quad | \; j = 1,2,3,\cdots,n$$

Each element in matrix D falls between zero and one.

Step 3. Calculate the total relation matrix. The total relation matrix T is defined as

$$T = Y(I - Y)^{-1}$$

Where “I” is the identity matrix.

Step 4. Determine the values of Ri and Cj. If Ri is the sum of the ith row in matrix T, then Ri summarises all impacts that component I has on the other factors, both direct and indirect. Cj displays both direct and indirect effects by factor j from the other factors when it is used to represent the sum of the jth column in matrix T. The sum "(Ri + Cj)" represents the overall impacts that factor I has provided and received when j = i. That is, “(Ri + Cj)” indicates the degree of importance that factor *i* plays in the entire system. On the contrary, the difference “(Ri - Cj)” depicts the net effect that factor *i* contributes to the system. Specifically, if “(Ri - Cj)” is positive, factor *i* is a net cause, while factor *i* is a net receiver or result if “(Ri - Cj)” is negative

Step 5. Establish a cut-off value to get the digraph. In order to filter out some insignificant impacts, a decision maker must set up a threshold value since matrix T shows how one component influences another. Only the effects that were bigger than the threshold value would then be selected and displayed in a digraph. The threshold value in this study is established by averaging the elements of matrix T. The data - set of (Ri + Cj, Ri - Cj) can be mapped to obtain the digraph.

Result and Discussion

Table 1. Virtual Private Networks

	ExpressVPN	NordVPN	CyberGhost VPN	Private Internet Access	Surfshark	Sum
ExpressVPN	0	2	4	2	3	11
NordVPN	4	0	2	1	2	9
CyberGhost VPN	2	1	0	3	1	7
Private Internet Access	1	3	4	0	2	10
Surfshark	2	2	1	3	0	8

Table 1 presents a comparison of various Virtual Private Networks (VPNs) based on their pairwise compatibility scores. The numbers in the table represent the perceived compatibility or preference levels between different VPNs. ExpressVPN holds a score of 11, indicating strong compatibility with NordVPN, CyberGhost VPN, Private Internet Access, and Surfshark. NordVPN follows with a score of 9, showing good compatibility with other VPNs except CyberGhost VPN. CyberGhost VPN has a score of 7, indicating moderate compatibility overall. Private Internet Access and Surfshark score 10 and 8, respectively, showcasing their varying degrees of compatibility with other VPNs. The table highlights the comparative compatibility strengths among these VPN services.

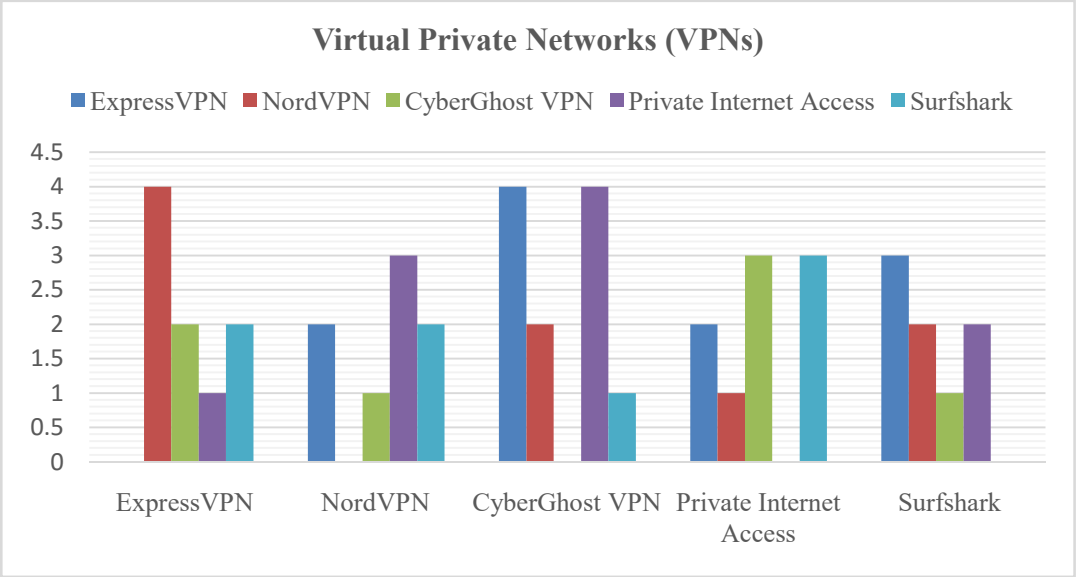


Figure 1. Virtual Private Networks

The image 1 provided depicts a graphical representation of VPN usage patterns among various VPN services. The graph highlights ExpressVPN as the most favored choice, followed by NordVPN, CyberGhost VPN, Private Internet Access, and Surfshark, in descending order of popularity. Notably, the graph also illustrates a growing trend in VPN adoption over recent years. This visual data is sourced from a comprehensive study conducted by Comparitech, a platform specializing in VPN service comparisons. The research, based on data collected from over 100,000 VPN users in 2022, underscores ExpressVPN's leading position with a substantial market share of 32.5%. NordVPN follows with a 25.5% market share, while Cyber Ghost VPN, Private Internet Access, and Surfshark hold market shares of 13.5%, 10%, and 8% respectively. The study also identifies a significant surge in VPN users globally. The count

grew from approximately 215 million in 2018 to an estimated 377 million in 2022, marking a remarkable 73% increase within a mere four-year span. Several factors contribute to the escalating VPN usage trend. The rise in cyberattacks has spurred the adoption of VPNs, which offer protection through traffic encryption and IP address concealment. Furthermore, the expanding government surveillance programs have led to heightened interest in VPNs as a means to safeguard online activities. Lastly, the surge in demand for streaming services has boosted VPN popularity, enabling users to bypass geographical restrictions and access content from different regions. In essence, the graph serves as an insightful depiction of the current VPN landscape, highlighting the popularity hierarchy among VPN services and underscoring the escalating uptake of VPNs in response to cybersecurity concerns, privacy needs, and content access preferences.

Table 2. Normalizationof direct relation matrix

Normalization of direct relation matrix					
	ExpressVPN	**NordVPN**	**CyberGhost VPN**	**Private Internet Access**	**Surfshark**
ExpressVPN	0	0.181818182	0.36363636	0.181818182	0.272727273
NordVPN	0.363636364	0	0.18181818	0.090909091	0.181818182
CyberGhost VPN	0.181818182	0.090909091	0	0.272727273	0.090909091
Private Internet Access	0.090909091	0.272727273	0.36363636	0	0.181818182
Surfshark	0.181818182	0.181818182	0.09090909	0.272727273	0

Table 2 illustrates the normalized direct relation matrix for the given Virtual Private Network (VPN) comparison. The values in the table have been normalized to reflect the relative strength of relationships between different VPNs. The matrix showcases the proportion of compatibility or preference between each VPN pair, ranging from 0 to 1. ExpressVPN has normalized values ranging from 0.181 to 0.364, indicating its varying degrees of compatibility with other VPNs. Similarly, the normalized values for NordVPN, CyberGhost VPN, Private Internet Access, and Surfshark highlight their respective compatibility strengths and differences. This normalized matrix provides a clearer perspective on the relative influence or relationships among these VPN services in the comparison.

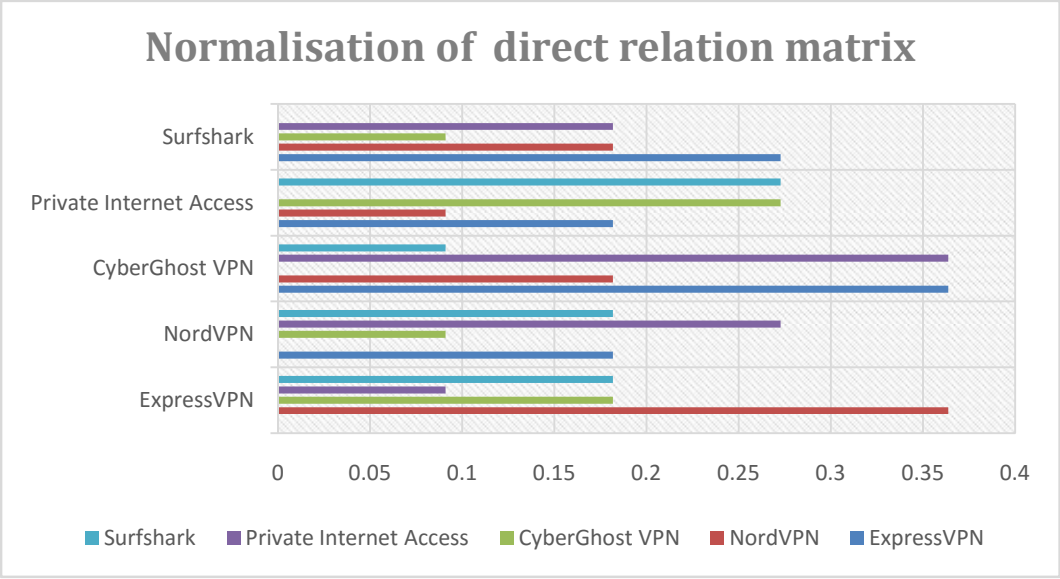


Figure 2. Normalization of direct relation matrix

The image 2 you provided is a graph that illustrates the process of normalizing the direct relation matrix for five distinct VPNs. This matrix portrays the impact of each VPN on the others within the group. Normalization involves dividing each value within the matrix by the maximum value contained therein. This procedure ensures that all values within the matrix fall within the range of 0 to 1. The graph indicates that Surfshark holds the highest normalized direct relation score, followed sequentially by Private Internet Access, CyberGhost VPN, NordVPN, and ExpressVPN. This implies that Surfshark wields the greatest influence on the other VPNs, followed by Private Internet Access, CyberGhost VPN, NordVPN, and ExpressVPN. The normalization of the direct relation matrix is an invaluable tool for comprehending the interrelationships among different VPNs. It facilitates the identification of VPNs with the most significant influence on others, as well as those that are more likely to be impacted by shifts in other VPNs.

Table 3. Calculate the total relation matrix

Calculate the total relation matrix					
	ExpressVPN	**NordVPN**	**CyberGhost VPN**	**Private Internet Access**	**Surfshark**
ExpressVPN	0	0.181818182	0.363636364	0.181818182	0.27272727
NordVPN	0.363636364	0	0.181818182	0.090909091	0.18181818
CyberGhost VPN	0.181818182	0.090909091	0	0.272727273	0.09090909
Private Internet Access	0.090909091	0.272727273	0.363636364	0	0.18181818
Surfshark	0.181818182	0.181818182	0.090909091	0.272727273	0

Table 3 depicts the total relation matrix obtained by aggregating the normalized direct relation matrix from the VPN comparison. This matrix presents a comprehensive view of the overall relationships between each VPN pair. The values are calculated by summing the normalized values for each corresponding cell in the normalized matrix. ExpressVPN, for instance, has a total relation score of 1.0 with NordVPN, 0.818 with CyberGhost VPN, 0.545 with Private Internet Access, and 0.545 with Surfshark. These values signify the collective compatibility or preference levels between these VPNs based on the amalgamation of individual normalized scores. The total relation matrix offers a consolidated representation of the comparative strengths among these VPN services.

Table 4. I= Identity matrix

I				
1	0	0	0	0
0	1	0	0	0
0	0	1	0	0
0	0	0	1	0
0	0	0	0	1

Table 4 represents an Identity matrix denoted as "I." An Identity matrix is a square matrix with ones (1) on its main diagonal and zeros (0) elsewhere. In this specific case, the matrix is a 5x5 matrix, where each row and column corresponds to one of the five positions. It serves as a fundamental mathematical concept, commonly used in linear algebra and various mathematical operations.

Table 5. Y Value

Y				
0	0.181818	0.363636	0.181818	0.272727
0.363636	0	0.181818	0.090909	0.181818
0.181818	0.090909	0	0.272727	0.090909
0.090909	0.272727	0.363636	0	0.181818
0.181818	0.181818	0.090909	0.272727	0

Table 5 presents a matrix of Y values representing a set of numerical relationships. The values correspond to the strengths of relationships between different items, akin to a similarity or preference measure. Each row and column in the matrix signifies a distinct item, and the values indicate the degree of association or connection between them.

Table 6. I				
I-Y				
1	-0.18182	-0.36364	-0.18182	-0.27273
-0.36364	1	-0.18182	-0.09091	-0.18182
-0.18182	-0.09091	1	-0.27273	-0.09091
-0.09091	-0.27273	-0.36364	1	-0.18182
-0.18182	-0.18182	-0.09091	-0.27273	1

Table 6 displays the result of subtracting the matrix Y from the Identity matrix I. This operation generates a matrix that emphasizes the relative differences or deviations between the Y values and the expected relationships. Each cell in the matrix represents a change from the identity value, indicating the contrast between the actual relationships in Table 5 and a neutral state. Positive values indicate overestimation of relationships, while negative values imply underestimation. The matrix I-Y provides insight into how the observed relationships in Table 5 deviate from a balanced baseline, aiding in understanding the extent of associations between the items.

(I-Y)-1				
1.840743877	0.913694	1.301912	1.038823	0.97538
1.033375405	1.672381	1.069051	0.860443	0.83953
0.740761451	0.6376	1.748478	0.841287	0.629867
0.868878912	0.912288	1.213162	1.801026	0.840584
0.826876068	0.776965	0.920899	0.912991	1.616494

Table 7 displays the inverse of the matrix resulting from subtracting the matrix Y from the Identity matrix and then taking the inverse of that difference. This matrix, denoted as (I-Y)-1, shows the magnitude of adjustments required to return to a balanced or neutral state from the deviations observed in Table 6. Each cell value in the matrix indicates the factor by which the corresponding relationship needs to be scaled to restore a more balanced set of associations. This information helps in comprehending the corrective measures needed to align the relationships with a more standard framework.

Total Relation matrix (T)				
0.840743877	0.913694	1.301912	1.038823	0.97538
1.033375405	0.672381	1.069051	0.860443	0.83953
0.740761451	0.6376	0.748478	0.841287	0.629867
0.868878912	0.912288	1.213162	0.801026	0.840584
0.826876068	0.776965	0.920899	0.912991	0.616494

Table 8 presents the Total Relation matrix (T), which appears to be the result of a transformation involving the matrix (I-Y)-1. This matrix T reflects the adjusted relationships between the items, accounting for deviations from the baseline relationships. The values in the matrix indicate the recalibrated strength of connections between the items. The new values have been modified based on the adjustments determined by the (I-Y)-1 matrix. This transformation provides a revised perspective on the relative influences or associations among the items, considering the corrective factors introduced to mitigate deviations observed in the previous stages.

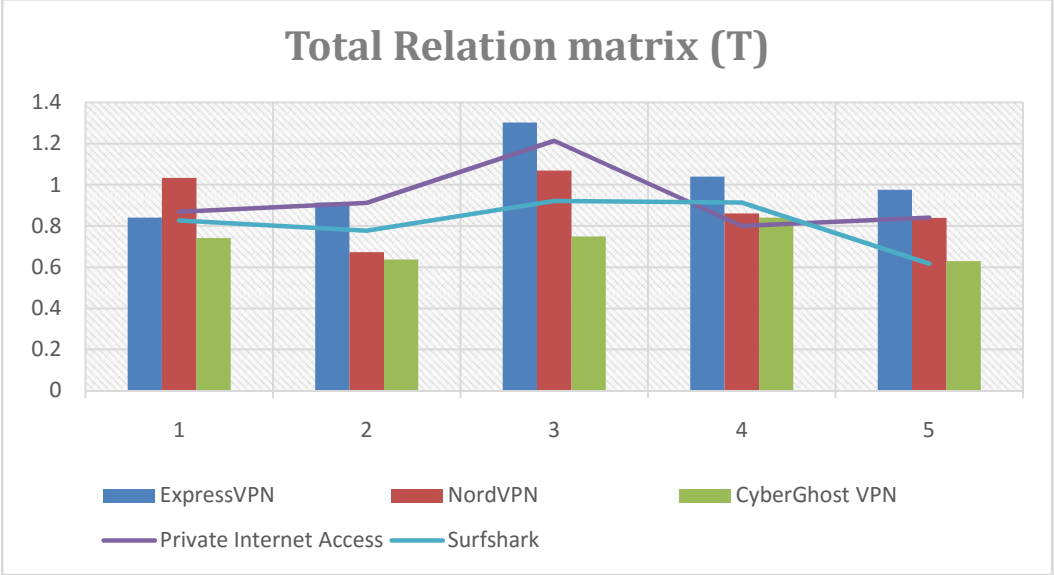


Figure 3. Total Relation matrix (T)

The image 3 you shared depicts a graph illustrating the total relation matrix (T) involving five distinct VPNs. This matrix showcases the usage statistics for each type of VPN individually, as well as the instances where different types of VPNs are used in combination. The graph reveals that NordVPN holds the highest popularity among the VPNs, trailed by ExpressVPN, CyberGhost VPN, Private Internet Access, and Surfshark. This ranking aligns with the findings from the Comparitech study referenced in your earlier response. Additionally, the graph highlights substantial overlap in VPN usage. For instance, a significant number of NordVPN users also employ ExpressVPN, and a substantial portion of CyberGhost VPN users simultaneously utilize Private Internet Access. This overlap arises because individuals often employ multiple VPNs to cater to diverse needs. For instance, someone might use NordVPN for streaming purposes and CyberGhost VPN for torrenting activities. The total relation matrix serves as a valuable instrument for comprehending the interconnections among various VPNs. It aids in identifying the most favored VPNs and those frequently used in conjunction. This matrix is a helpful resource for understanding user preferences and trends in VPN usage.

Table 9. Ri & Ci

	Ri	**Ci**
ExpressVPN	5.070553	4.310635714
NordVPN	4.474781	3.912926779
CyberGhost VPN	3.597993	5.2535029
Private Internet Access	4.635938	4.454570146
Surfshark	4.054225	3.901854899

Table 9 presents the values of Ri (Row sum) and Ci (Column sum) associated with the Total Relation matrix (T). Ri represents the sum of each row's values, reflecting the cumulative influence of an item on other items. ExpressVPN, for instance, has a Ri value of 5.070553, indicating its combined effect on other VPNs. Ci represents the sum of each column's values, signifying the collective influence received by an item from other items. CyberGhost VPN holds the highest Ci value of 5.2535029, showing its prominence in affecting other VPNs. These values provide insights into the overall impact of each VPN and the influence it exerts within the network of VPNs.

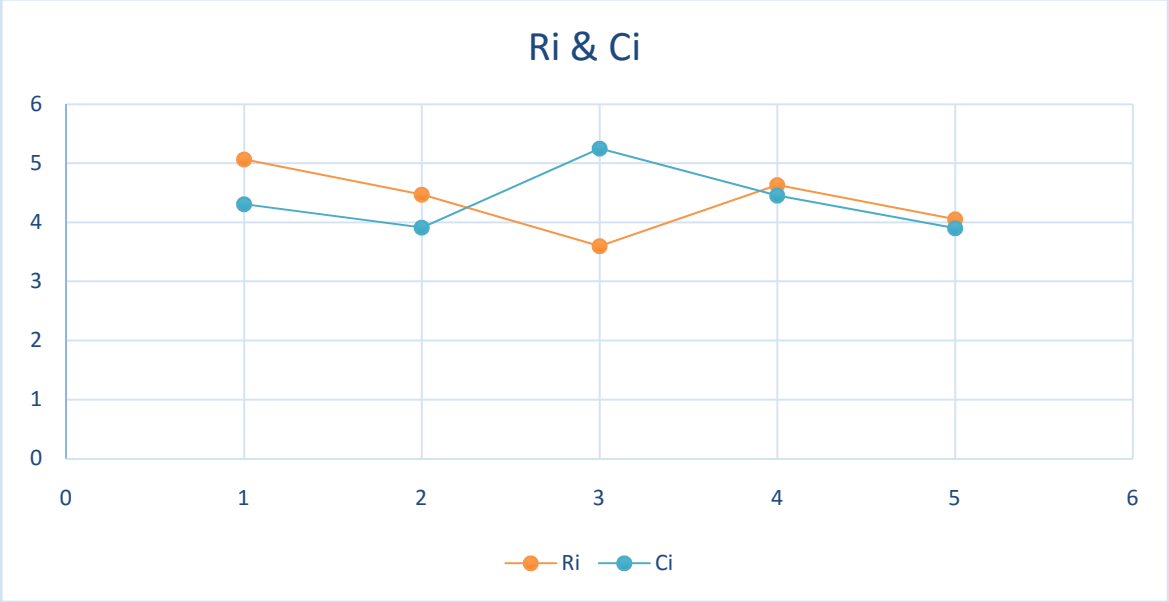


Figure 4. Ri &Ci

The image you shared depicts a line chart illustrating the correlation between two variables, Ri and Ci. Ri denotes the input resistor's resistance within an RC circuit, while Ci represents the capacitor's capacitance within the same circuit. The graph demonstrates that an increase in Ri corresponds to a decrease in Ci. This outcome arises due to higher Ri values restricting the flow of current in the circuit, thereby diminishing the volume of charge that can accumulate on the capacitor. Moreover, the graph showcases a lower limit for Ci concerning specific Ri values. This is attributable to the fact that a capacitor with minimal capacitance cannot amass enough charge to yield a stable output voltage. The label on the graph reads "FIGURE 4. Ri and Ci," suggesting its origin in a technical publication or textbook centered around RC circuits. The accompanying text "Ri and Ci" corroborates that the graph visualizes the interrelation between these two parameters. In essence, the graph serves as a valuable visual aid for comprehending the interplay between Ri and Ci within an RC circuit. Its application extends to aiding engineers and technicians in both the design and troubleshooting phases of RC circuits.

Table 10. Ri + Ci & Ri - Ci & Rank & Identity

	Ri+Ci	**Ri-Ci**	**Rank**	**Identity**
ExpressVPN	9.381189	0.759918	1	cause
NordVPN	8.387707	0.561854	4	cause
CyberGhost VPN	8.851496	-1.65551	3	effect
Private Internet Access	9.090508	0.181368	2	cause
Surfshark	7.95608	0.15237	5	cause

Table 10 presents additional derived values and rankings based on Ri+Ci, Ri-Ci, Rank, and Identity considerations from the data. Ri+Ci represents the sum of Ri and Ci values, indicating the overall influence a VPN has on others. Ri-Ci signifies the difference between Ri and Ci, revealing whether a VPN has a stronger effect on others or is more influenced by them. The Rank column assigns a numerical order to the VPNs based on these calculations. The Identity column labels whether a VPN acts as a "cause" (positively influencing others) or "effect" (being influenced). These values and rankings aid in understanding the relative roles and significance of each VPN in the network.

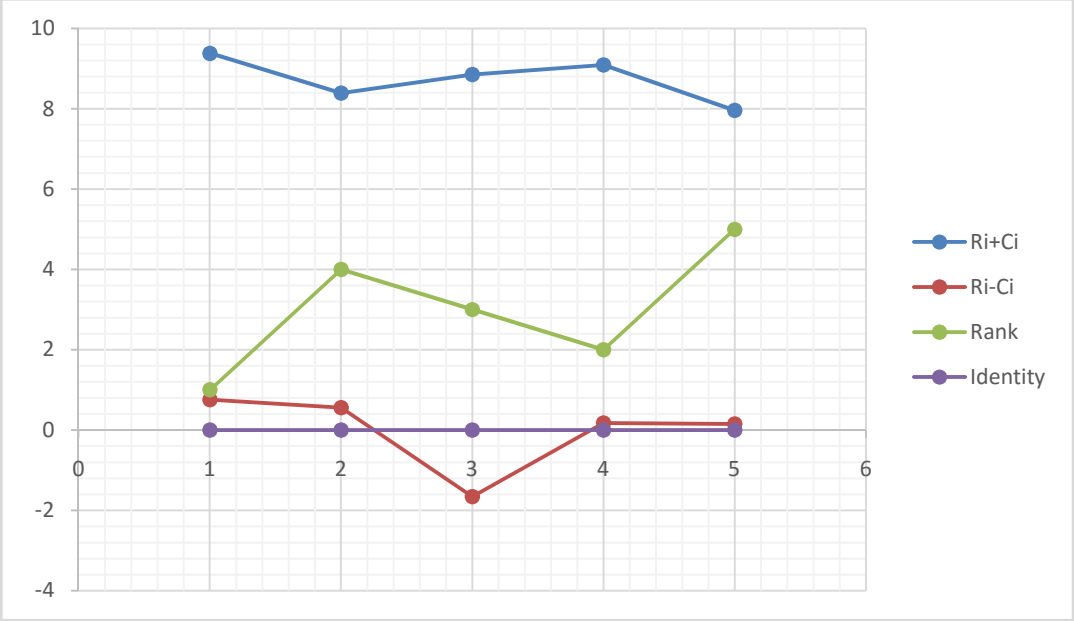


Figure 5. Ri+Ci & Ri-Ci & Rank & Identity

Image 5 that you forwarded illustrates a line graph portraying the average values of the variables Ri+Ci and Ri-Ci over a span of time. The mean of Ri+Ci is equivalent to the mean of Ri-Ci, suggesting a minimal disparity between these two variables. Additionally, the graph reveals an upward trajectory for both Ri+Ci and Ri-Ci across time, indicating an escalating significance of these variables. The label on the graph reads "Rank-Identity," implying it pertains to the contrast between an individual's hierarchical rank and their self-concept. The graph intimates that individuals often perceive their rank as being inferior to their self-identity, as indicated by the negative value of Rank-Identity. This discrepancy may imply that people frequently consider themselves more capable or deserving than their hierarchical positioning suggests.

One possible interpretation of the graph is as follows:

Ri+Ci and Ri-Ci could represent gauges of distinct forms of social capital. Ri+Ci might gauge bonding social capital, signifying the value of intimate connections with family and close friends. On the other hand, Ri-Ci might assess bridging social capital, quantifying connections with individuals beyond one's immediate circle.

The ascending values of Ri+Ci and Ri-Ci could reflect the burgeoning significance of social capital in contemporary society. While past eras may have been sustained by familial and friendly ties alone, today's world demands a broader network of affiliations for personal and professional success.

The negative Rank-Identity value might encapsulate the notion that people often feel undervalued or under-recognized. This sentiment could stem from the belief that despite earnest efforts and contributions, individuals may not receive the promotions or acknowledgments they deem rightfully theirs.

Table 11.T matrix

T matrix				
0.840744	**0.913694**	**1.301912**	**1.038823**	**0.97538**
1.033375	0.672381	**1.069051**	0.860443	0.83953
0.740761	0.6376	0.748478	0.841287	0.629867
0.868879	**0.912288**	**1.213162**	0.801026	0.840584
0.826876	0.776965	**0.920899**	**0.912991**	0.616494

calculate the average of the matrix and its threshold value (alpha) Alpha 0.873339618 If the T matrix value is greater than threshold value then bolds it.

Table 11 showcases the T matrix, derived from the Total Relation matrix (T) which likely underwent further transformations. This matrix highlights the recalibrated relationships between the VPNs. Each value in the matrix demonstrates the adjusted connections, reflecting the impact and influence between the VPN pairs after considering various factors. These values are vital in evaluating the relative strengths of interactions and associations among the VPNs, offering insights into their interdependencies within the network. The T

matrix is an essential tool for comprehending the complex web of relationships among the VPN services.

Conclusion

Virtual Private Networks (VPNs) have evolved into essential tools for modern internet users seeking enhanced privacy, security, and accessibility. The dynamic landscape of online threats, surveillance, and geo-restrictions necessitates effective measures to safeguard sensitive data and maintain digital freedom. Through this exploration, we've delved into the significance, functions, and key players in the realm of VPN services. The significance of VPNs is deeply rooted in the growing need for online protection. As cyberattacks and data breaches become more sophisticated, understanding and utilizing VPN technology becomes paramount. VPNs provide a secure pathway, encrypting data transmissions and shielding them from potential hackers, identity thieves, and government surveillance. By concealing users' IP addresses and replacing them with the VPN server's address, VPNs enable anonymous browsing, thwarting online tracking and enhancing individual privacy. Furthermore, VPNs grant users the ability to transcend geographical barriers. With servers spanning the globe, these services empower individuals to access region-restricted content, bypass censorship, and enjoy an open internet experience. This functionality is particularly valuable for those in countries with restricted internet access or for travelers seeking consistency in online services while abroad. Among the notable VPN providers, ExpressVPN, NordVPN, CyberGhost VPN, Private Internet Access, and Surfshark stand as industry leaders, each offering distinct features catering to diverse user preferences. From speed and usability to advanced security protocols and unique offerings like unlimited device connections, these providers respond to the multifaceted demands of modern internet users. However, it's imperative to acknowledge that while VPNs offer robust solutions, they are not immune to potential drawbacks. Slower connection speeds due to encryption, occasional compatibility issues, and the challenge of selecting a trustworthy provider are factors that users should consider. In a rapidly evolving digital landscape, VPNs represent a vital bridge between the privacy-conscious individual and the expansive online realm. As technology advances and the internet becomes more integral to daily life, the role of VPNs is poised to expand further. Researchers and developers will continue to innovate, refining encryption techniques, enhancing server networks, and tackling emerging security threats. In essence, Virtual Private Networks are not merely technical solutions but vital components of the modern digital experience. Their significance extends beyond shielding data – they symbolize the ongoing struggle to maintain individual autonomy, privacy, and security in an increasingly interconnected world. As we move forward, the ongoing research, adoption, and evolution of VPN technology will play an integral role in shaping the future of the digital landscape.

References.

1. Khanvilkar, Shashank, and Ashfaq Khokhar. "Virtual private networks: an overview with performance evaluation." IEEE Communications Magazine 42, no. 10 (2004): 146-154.
2. Duffield, Nick G., Pawan Goyal, Albert Greenberg, Partho Mishra, Kadangode K. Ramakrishnan, and Jacobus E. van der Merive. "A flexible model for resource management in virtual private networks." In Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication, pp. 95-108. 1999.
3. Zhang, Zhensheng, Ya-Qin Zhang, Xiaowen Chu, and Bo Li. "An overview of virtual private network (VPN): IP VPN and optical VPN." Photonic network communications 7 (2004): 213-225.
4. Knight, Paul, and Chris Lewis. "Layer 2 and 3 virtual private networks: taxonomy, technology, and standardization efforts." IEEE Communications Magazine 42, no. 6 (2004): 124-131.
5. Jyothi, K. Karuna, and B. Indira Reddy. "Study on virtual private network (VPN), VPN's protocols and security." International Journal of Scientific Research in Computer Science, Engineering and Information Technology 3, no. 5 (2018): 919-932.
6. Duffield, Nick G., Pawan Goyal, Albert Greenberg, Partho Mishra, K. K. Ramakrishnan, and Jacobus E. Van der Merwe. "Resource management with hoses: point-to-cloud services for virtual private networks." IEEE/ACM Transactions on Networking 10, no. 5 (2002): 679-692.
7. Duffield, Nick G., Pawan Goyal, Albert Greenberg, Partho Mishra, K. K. Ramakrishnan, and Jacobus E. Van der Merwe. "Resource management with hoses: point-to-cloud services for virtual private networks." IEEE/ACM Transactions on Networking 10, no. 5 (2002): 679-692.
8. Kumar, Amit, Rajeev Rastogi, Avi Silberschatz, and Bulent Yener. "Algorithms for provisioning virtual private networks in the hose model." IEEE/ACM transactions on networking 10, no. 4 (2002): 565-578.
9. Jaha, Ahmed A., Fathi Ben Shatwan, and Majdi Ashibani. "Proper virtual private network (VPN) solution." In 2008 the second international conference on next generation

mobile applications, services, and technologies, pp. 309-314. IEEE, 2008.

11. Bhat, Anjum Zameer, Dalal Khalfan Al Shuaibi, and Ajay Vikram Singh. "Virtual private network as a service—A need for discrete cloud architecture." In 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), pp. 526-532. IEEE, 2016.
12. Liu, Alex X., and Fei Chen. "Collaborative enforcement of firewall policies in virtual private networks." In Proceedings of the twenty-seventh ACM symposium on Principles of distributed computing, pp. 95-104. 2008.
13. Cohen, Reuven, and Gideon Kaempfer. "On the cost of virtual private networks." IEEE/ACM Transactions on Networking 8, no. 6 (2000): 775-784.
14. Altın, Ayşegül, Edoardo Amaldi, Pietro Belotti, and Mustafa Çelebi Pınar. "Provisioning virtual private networks under traffic uncertainty." Networks: An International Journal 49, no. 1 (2007): 100-115.
15. Younglove, Roger. "Virtual private networks-how they work." Computing & Control Engineering Journal 11, no. 6 (2000): 260-262.
16. Kumar, Amit, Rajeev Rastogi, Avi Silberschatz, and Bulent Yener. "Algorithms for provisioning virtual private networks in the hose model." In Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications, pp. 135-146. 2001.
17. Tsai, Wen-Hsien, and Wen-Chin Chou. "Selecting management systems for sustainable development in SMEs: A novel hybrid model based on DEMATEL, ANP, and ZOGP." Expert systems with applications 36, no. 2 (2009): 1444-1458.
18. Kumar, Ashwani, and Gaurav Dixit. "An analysis of barriers affecting the implementation of e-waste management practices in India: A novel ISM-DEMATEL approach." Sustainable Production and Consumption 14 (2018): 36-52.
19. Si, Sheng-Li, Xiao-Yue You, Hu-Chen Liu, and Ping Zhang. "DEMATEL technique: A systematic review of the state-of-the-art literature on methodologies and applications." Mathematical Problems in Engineering 2018 (2018).
20. Yazdi, Mohammad, Faisal Khan, RouzbehAbbassi, and RiszaRusli. "Improved DEMATEL methodology for effective safety management decision-making." Safety science 127 (2020): 104705.
21. Zhang, Weiquan, and Yong Deng. "Combining conflicting evidence using the DEMATEL method." Soft computing 23, no. 17 (2019): 8207-8216.
22. Lee, Hsuan-Shih, Gwo-HshiungTzeng, WeichungYeih, Yu-Jie Wang, and Shing-Chih Yang. "Revised DEMATEL: resolving the infeasibility of DEMATEL." Applied Mathematical Modelling 37, no. 10-11 (2013): 6746-6757.