Symbiosis

www.symbiosisonlinepublishing.com
ISSN Online: 2374-8141

Research Article | Nanoscience & Technology: Open Access | Open Access

Applying The Promethee Method In The Field Of Computer Cybersecurity Is "Ranking Cybersecurity Solutions For Risk Mitigation

Mr. Vedaswaroop Meduri*

*Full Stack Lead, Laboratory Corporation of America, Illinois, USA

Received: November 05, 2023; Accepted: November 21, 2023; Published: December 12, 2023

***Corresponding author:** Vedaswaroop Meduri, Full Stack Lead, Laboratory Corporation of America, Illinois, USA; E-mail: ved.workemail@gmail.com*

Abstract

Introduction: Cybersecurity, also known as computer security or information technology security, is a field dedicated to safeguarding computer systems, networks, and data from unauthorized access, damage, or disruption. With the rapid advancements in technology and the increasing reliance on digital infrastructure, cyber threats have become a significant concern for individuals, organizations, and governments worldwide. cybersecurity involves understanding and countering various cyber threats, such as malware, phishing attacks, data breaches, and ransomware. It encompasses a wide range of practices and measures, including encryption, firewalls, authentication protocols, intrusion detection systems, and security awareness training. The primary goal of cybersecurity is to protect sensitive information, maintain the integrity of computer systems, and ensure the availability of critical services in the face of potential cyber-attacks. As the digital landscape continues to evolve, the importance of cybersecurity becomes more prominent, making it a critical aspect of modern-day computing and information management.

Research significance: Computer cybersecurity research is of utmost significance as it safeguards critical infrastructure, protects personal data, defends against evolving cyber threats, preserves national security, fosters economic growth, upholds privacy and individual rights, promotes global cooperation, and prepares for future challenges. In an increasingly interconnected world, this research plays a pivotal role in ensuring a secure digital landscape for individuals, organizations, and nations.

Methodology: The PROMETHEE (Preference Ranking Organization Method for Enrichment Evaluations) method is a multi-criteria decision-making technique used to rank and select alternatives based on various criteria. Developed by J.P. Brans and P. Vincke in the 1980s, PROMETHEE enables decision-makers to evaluate complex problems with conflicting objectives. The method assesses the relative importance of each criterion, compares alternatives pairwise, and calculates preference indices to generate a global ranking. By providing a systematic approach to decision-making, PROMETHEE helps in choosing the most suitable option from a set of alternatives in a wide range of applications, such as business, engineering, and environmental management.

Alternative: Next-Generation Firewall with Advanced Threat Protection, Endpoint Detection and Response (EDR) System, Cloud-Based Security Information and Event Management (SIEM), Network Behavior Analytics Platform, Multi-Factor Authentication (MFA) Solution, Web Application Firewall (WAF)

Evaluation preference: Threat Detection, Incident Response, User-Friendliness, Scalability

Results: From the result it is seen that Incident Response is got the first rank where as is the Scalability is having the lowest rank.

Keywords: Cloud-Based Security, Web Application Firewall, PROMETHEE, Computer Cyber Security

Introduction

Cybersecurity is often used interchangeably with information security, both focusing on the role of humans in the security process. Considering cybersecurity as an additional dimension, it highlights the potential targeting of individuals. However, ethical considerations play a crucial role when discussing cybersecurity, as it holds significant meaning for society as a whole. Various structures and models have been developed to address cybersecurity issues, including safety-related personnel and information on personal computers.[1] This article examines different cybersecurity models and their limitations, as well as past reviews of threats and mitigation techniques. While cybersecurity information and security are used interchangeably, the role of individuals in the security process is carefully considered. Adding an extra dimension, it emphasizes the potential targeting of attentive individuals as potential victims. However, discussing cybersecurity also involves important ethical implications for society as a whole. Despite various definitions and features related to internet security, such as secure sharing, privacy, and access to information, there is still a lack of clarity and a lack of consensus among experts.[2] Cyber security information can be used interchangeably with the term "security." In this context, it takes into account the role it plays in the security process. To fully grasp its significance, one should consider an additional dimension and be attentive to the ability of cyber threats to target individuals.

However, when discussing cyber security's ethical aspects, it becomes crucial to focus on the implications it has on society as a whole. Despite various definitions and features attributed to cyber security, such as internet security, secure sharing, privacy, and access to information, there remains a lack of clarity and a consensus on its precise definition.[3] The Department of Defense (DoD) of the country has established a strategy for responding to cyber threats, which includes the activation of efforts to protect computer networks and servers in cyberspace. This strategy introduces definitions of cyberspace, outlines how to safeguard DoD networks and systems, and emphasizes the importance of partnering with other government agencies and cybersecurity partners to strengthen cyber defenses.

The DoD also focuses on developing relationships and utilizing technological innovations to expedite cybersecurity initiatives for the department's benefit.[4] At the United States Naval Academy (USNA), cybersecurity is an integral part of the curriculum. All midshipmen (USNA undergraduates) are required to take two main courses on cybersecurity, regardless of their major. Consequently, significant resources have been allocated to these courses, as well as other computer science-related majors and the required courses outlined in the developed syllabus presented at the Academy. [5] The education sector is increasingly prioritizing cyber security education and its implementation, seeking accreditation and understanding the interactions between hardware, software, human factors, policy, and politics in cyberspace. Various sample syllabuses and recommendations have been discussed internationally, impacting education, policy, and practice. This paper addresses three main questions: i) what should be taught to general computer science students regarding cyber security; ii) whether internet security should be taught separately or integrated into general computer science education; and iii) the accreditation of cyber security programs by national professional and regulatory bodies, with a focus on England as a case study.[6] The global internet security crises have compelled the education sector to emphasize the need for cyber security education to produce qualified professionals. However, there is a lack of a structured academic discipline for cyber security, and most efforts have been training-driven rather than knowledge-driven.

This has led to difficulties in creating a comprehensive cyber security curriculum with universally accepted reference models. [7] As the international perspective introduces local requirements and different criteria, designing effective cyber security programs becomes more challenging. There is a need for universally accepted reference models to help employers and students understand the size and scope of cyber security education. Despite the challenges, the paper suggests making efforts to enter this space by designing programs that are free from constraints, with initiatives focused on designing, compiling, and marketing cyber security education. It emphasizes the importance of a comprehensive approach to internet safety planning.[8] the importance of excellence in teaching and explaining cyber security, presenting it as an opportunity that goes hand in hand with the need for cyber security education. The rest of the paper is organized as follows: it begins with a brief overview of NetsBlox and its technical details, followed by a description of Roboscape's syllabus, which outlines the opportunities for teaching cyber security to K-12 students. The authors discuss their experience of using a week-long summer camp as a platform to deliver cyber security education and conclude with lessons learned during its implementation.[9] The creators and developers of Building Management Systems often prioritize service-related aspects over cyber security concerns, resulting in neglect and overlooking potential security problems.

Manufacturers of such systems often fail to provide adequate support and notifications to users about security breaches or vulnerabilities, leaving these systems unsafe and poorly protected.[10] In the context of the Internet of Things (IoT) and Smart Cities, cyber security becomes a critical issue due to the multiple security concerns arising from the integration of various technologies and the extensive communication involved. The complexity and openness of these systems create an unlimited attack surface, leading to cryptography-related challenges. Addressing cyber security in Smart Cities is a global issue that requires the collaboration of experts and international cooperation to tackle this important problem effectively.[11] This cyber security threat is of significant physical magnitude and will result in adverse consequences for infrastructure, economy, and society. Within technical contexts, there have already been numerous instances of unauthorized users launching attacks to gain access to critical data, demonstrating their ability to penetrate protected network domains. Additionally, the heavy reliance of information technology (IT) in managing real-time control, monitoring, and maintenance of electric power grids makes them susceptible to targeted cyber-attacks. [12] A prominent example of such an attack occurred in 2015 when the Ukrainian power grid experienced widespread power outages due to a sophisticated cyber-attack.

This incident highlights the crucial importance of investing in internet security measures to protect against intruders. Consequently, researchers have focused on exploring cyber security solutions to safeguard power grids and have made progress in this area. The paper under discussion presents cutting-edge research studies in power systems and addresses various cyber security risks, providing evidence and justification for creating effective solutions.[13] These camps provide hands-on learning experiences in Computer Science, specifically focusing on Cybersecurity and dealing with policies. Participants, ranging from 10 to 18 years old, use inexpensive hardware and free software during the camp. The 2018 camp received positive feedback, leading to the creation of a new iteration in 2019. The Cybersecurity content covered various real-world scenarios, identity protection, and the identification of potential threats. Surveys showed significant improvements in participants' knowledge and interest levels after the camp. The results

indicate that the camp had a positive impact on students' interest in Cybersecurity, with a considerable increase in their capacity to identify threats and understand Cybersecurity concepts. The camps attracted highly motivated students, with attendance increasing from 31% to 65% in the latter camp. These findings suggest that such activities can play a crucial role in providing quality education in Cybersecurity and related STEM fields.[14] Educators can take note of the implications of these camps and their potential to supplement traditional schooling with unique and engaging experiences. The rapidly evolving technology landscape introduces new security vulnerabilities, making the need for Cybersecurity experts even more essential. Integrating such camps into formal education or offering them as after-school or summer programs can be beneficial for students of all ages. This research highlights the effectiveness of outreach programs like these week-long summer camps in stimulating interest in Cybersecurity among students aged 10-18. The growing importance of Cybersecurity in various fields and career paths further emphasizes the significance of introducing problem-solving skills early on. Overall, the camps have proven to be a valuable tool in encouraging students to pursue Cybersecurity as they progress through their academic journey.[15]

Material and Methods

Alternative:

Next-Generation Firewall with Advanced Threat Protection:

This cybersecurity solution combines traditional firewall features with advanced threat detection and prevention capabilities. It can identify and block sophisticated threats, providing an enhanced level of security for network traffic.

Endpoint Detection and Response (EDR) System:

EDR systems focus on detecting and responding to threats at the endpoint level, such as individual devices and servers. They provide real-time monitoring, threat hunting, and incident response capabilities to protect endpoints from cyber-attacks.

Cloud-Based Security Information and Event Management (SIEM):

Cloud-based SIEM solutions collect and analyze security event data from various sources, enabling the detection of abnormal behavior and potential security incidents in cloud environments.

Network Behavior Analytics Platform:

This solution analyzes network traffic patterns and behaviors to identify anomalies that could indicate cyber threats. It helps in detecting advanced and stealthy attacks that may evade traditional security measures.

Multi-Factor Authentication (MFA) Solution:

MFA adds an extra layer of security to user authentication by requiring multiple forms of verification, such as passwords, biometrics, or security tokens. This mitigates the risk of unauthorized access even if passwords are compromised.

Web Application Firewall (WAF):

A WAF protects web applications from various cyber threats, including SQL injection, cross-site scripting (XSS), and other web-based attacks. It filters and monitors HTTP requests and responses, safeguarding web applications from potential vulnerabilities.

Evaluation preference:

Threat Detection:

Threat detection refers to the process of identifying and recognizing potential cyber threats and security breaches within a system or network. It involves continuous monitoring and analysis of security logs, events, and network traffic to identify malicious activities, abnormal behavior, and indicators of compromise. Effective threat detection allows organizations to take proactive measures to mitigate potential risks and prevent cyber attacks before they cause significant harm.

Incident Response:

Incident response involves the coordinated actions taken by an organization to manage and contain cybersecurity incidents once they are detected. It includes processes for investigating, analyzing, and responding to security breaches and cyber attacks. A well-defined incident response plan helps minimize the impact of incidents, facilitates recovery, and ensures business continuity.

User-Friendliness:

User-friendliness in the context of cybersecurity solutions refers to the ease of use and accessibility of security tools and interfaces for end-users and administrators. Intuitive and user-friendly interfaces make it easier for users to understand and utilize security features effectively. A user-friendly cybersecurity solution enhances the overall security posture by encouraging proper implementation and reducing the likelihood of human errors or misconfigurations.

Scalability:

Scalability refers to the ability of a cybersecurity solution to handle increasing workloads and adapt to the changing needs of an organization. A scalable solution can accommodate growing volumes of data, users, and devices without compromising performance or security. In the context of cybersecurity, scalability is crucial as it ensures that the organization's security infrastructure can keep up with the evolving threat landscape and organizational growth.

Promethee Method

The PROMETHEE (Preference Ranking Organization Method for Enrichment Evaluations) is a multi-criteria decision-making (MCDM) approach used to compare and rank alternative options based on multiple criteria. Developed by J.P. Brans and P. Vincke in the 1980s, PROMETHEE has found applications in various fields, including business, engineering, environmental management, and public policy. [16] At its core, PROMETHEE

focuses on pairwise comparisons between alternatives for each criterion, allowing decision-makers to capture the relative importance and preferences associated with different criteria. The method is based on the assumption that decision-makers can express their preferences through a set of predefined criteria and the relative importance of each criterion. [17] The PROMETHEE method considers each criterion individually, enabling the evaluation of alternatives based on various aspects. This approach allows for a comprehensive and well-rounded assessment, leading to more informed conclusions. PROMETHEE employs Area Ranking to identify incomparable and neglected alternatives, providing a complete ranking of the alternatives.[18] The overall MCDA process using PROMETHEE involves selecting decision-makers, weighing criteria, evaluating alternatives against the criteria, applying PROMETHEE where necessary, and conducting sensitivity analysis to make the final decision.[19] One significant distinction of PROMETHEE from other MCDA techniques is its use of common criterion functions.[21]

Steps Involved

Step 1: Determine the criteria (j=1,....,k) and the set of possible alternatives in a decision problem

Step 2: Determine the weight wj of the criteria

$$\sum_{j=1}^{k} Wj = 1$$

Step 3 Normalize the decision matrix

$$R_{ij} = \frac{[x_{ij} - Min\ (x_{ij})]}{[Max\ (x_{ij}) - Min\ (x_{ij})]}$$ BENEFIT CRITERIA

$$R_{ij} = \frac{[Max\ (x_{ij} - x_{ij}]}{[Max\ (x_{ij}) - Min\ (x_{ij})}$$ COST CRITERIA

Where xij is evaluation values provided by decision makes i=1,.....,n, and numbers of criteria j=1,....,m.

Step 4: Determination of deviation by pairwise comparison

$$d_j(a, b) = g_j(a) - g_j(b)$$

$d_j(a,b)$ denotes the difference between the evaluations of a and b on each criterion.

Step 5: Define the preference function

$$P_j(a,b) = F_j[d_j(a, b)]$$

$P_j(a,b)$ represent the function of the difference between the evaluations of alternative a regarding alternative b on each criterion into a degree ranging from 0 to 1

Step 6: Determine the multi- criteria preference criteria

$$\pi(a, b) = \sum_{j-1}^{k} P(a, b) w_j$$

Step: Determine the positive and negative outranking flows

- The positive outranking flows:

$$\Phi^{+}(a) = \frac{1}{n-1} \sum_{x \in A} \pi(a, x),$$

- The Negative outranking flows:

$$\Phi^{-}(a) = \frac{1}{n-1} \sum_{x \in A} \pi(x, a).$$

Step 8: Calculate the net values and rank accordingly

$$\Phi(a) = \Phi^{+}(a) - \Phi^{-}(a) = \frac{1}{n-1} \sum_{j-1}^{k} \sum_{x \in A} [P_j(a, x) - P_j(x, a)] w_j$$

This outreach-based approach supports decision-makers by establishing a valuable relationship between alternatives and the PROMETHEE model. PROMETHEE is especially useful in handling complex real-world Multi-Attribute Decision-Making (MADM) problems, relying on expert judgment and subjective consciousness. [22] PROMETHEE helps decision-makers find relevant and preferred alternatives by sorting them based on the balance between positive and negative outranking flows. It aids in identifying clusters, integrating actions, and highlighting key

alternatives and their rationales, providing a structured decision-making process.[23] The PROMETHEE family, introduced in 1982 in Quebec, includes various methods such as PROMETHEE I, PROMETHEE II, PROMETHEE V, and PROMETHEE VI, each addressing different types of problems. PROMETHEE methods are widely used, with many practitioners and researchers utilizing them for multi-criteria decision problems. While PROMETHEE offers flexibility in handling different criteria, selecting appropriate criterion functions and associated limits can be challenging and may introduce uncertainty. [24]To overcome this, reliability-based approaches have been proposed to explore the robustness of solutions. PROMETHEE is commonly used in portfolio complexity applications, and its extended fuzzy data handling capabilities cater to situations with numerical data of varying accuracy. However, when encountering a large number of criteria, the decision-making process may become complex. In such cases, PROMETHEE can be combined with other approaches to tackle the problem effectively.[25]

Material and Methods

Table 1. Computer Cyber Security

	Next-Generation Firewall with Advanced Threat Protection	Endpoint Detection and Response (EDR) System	Cloud-Based Security Information and Event Management (SIEM)	Network Behavior Analytics Platform	Multi-Factor Authentication (MFA) Solution	Web Application Firewall (WAF)
Threat Detection	10	15	25	33	41	36
Incident Response	45	27	31	46	17	40
User-Friendliness	33	35	29	19	12	23
Scalability	40	28	11	31	32	41
Max	45	35	31	46	41	41
Min	10	15	11	19	12	23
max-Min	35	20	20	27	29	18

Table 1 presents a comparison of various computer cybersecurity solutions using a the "Next-Generation Firewall with Advanced Threat Protection" scores highest in "Threat Detection" with a rating of 41, indicating its effectiveness in identifying and responding to potential threats. However, it has a lower score in "Incident Response" (45), suggesting room for improvement in handling security incidents. The "Endpoint Detection and Response (EDR) System" performs well in "User-Friendliness" with a score of 35, indicating ease of use for end-users. It also scores high in "Incident Response" (27), showcasing its capability to address cybersecurity incidents. The "Cloud-Based Security Information and Event Management (SIEM)" excels in "Scalability" with a score of 32, making it suitable for handling large-scale security data. It also scores well in "Threat Detection" (25), showcasing its ability to identify potential threats. The "Network Behavior Analytics Platform" ranks highest in "Incident Response" with a score of 46, indicating its strong capabilities in responding to cybersecurity incidents. However, it receives a relatively low score in "User-Friendliness" (19), suggesting potential challenges in user adoption. The "Multi-Factor Authentication (MFA) Solution" performs well in "Threat Detection" with a score of 41, indicating its effectiveness in detecting potential threats. It also ranks high in "Scalability" (32), making it suitable for expanding security needs. The "Web Application Firewall (WAF)" scores well in "Threat Detection" (36), showcasing its ability to detect potential threats targeting web applications. However, it receives a relatively lower score in "User-Friendliness" (23), suggesting possible complexities in user interaction. this table provides valuable insights into the strengths and weaknesses of different computer cybersecurity solutions based on their performance in various criteria. It can help decision-makers in choosing the most appropriate solutions that align with their specific security requirements and organizational needs.

Table 2. Normalized Matrix

	Normalized Matrix					
	Next-Generation Firewall with Advanced Threat Protection	Endpoint Detection and Response (EDR) System	Cloud-Based Security Information and Event Management (SIEM)	Network Behavior Analytics Platform	Multi-Factor Authentication (MFA) Solution	Web Application Firewall (WAF)
Threat Detection	-3.5	-1.33333	-0.54545	-0.68421	0	-0.21739
Incident Response	0	-0.53333	0	0	-2	-0.04348

User-Friendliness	-1.2	0	-0.18182	-1.42105	-2.41667	-0.78261
Scalability	-0.5	-0.46667	-1.81818	-0.78947	-0.75	0

Table 2 presents the normalized matrix of the cybersecurity solutions, providing a relative comparison of their performance across the criteria: "Threat Detection," "Incident Response," "User-Friendliness," and "Scalability." The values in the matrix are scaled between -3 and 3, where negative values indicate weaker performance, zero represents an average performance, and positive values indicate stronger performance in each criterion. For instance, the "Next-Generation Firewall with Advanced Threat Protection" has a significantly low score of -3.5 in "Threat Detection," indicating strong detection capabilities. Conversely, it scores -1.33333 in "Incident Response," suggesting room for improvement in handling security incidents effectively. Similarly, the "Cloud-Based Security Information and Event Management (SIEM)" performs relatively well in "Threat Detection" with a score of -0.54545, but shows weaknesses in "Scalability" with a score of -1.81818, indicating that it might face challenges in handling large-scale security data. The normalized matrix allows decision-makers to evaluate and compare the cybersecurity solutions more objectively, aiding in the selection process based on their specific security requirements and priorities.

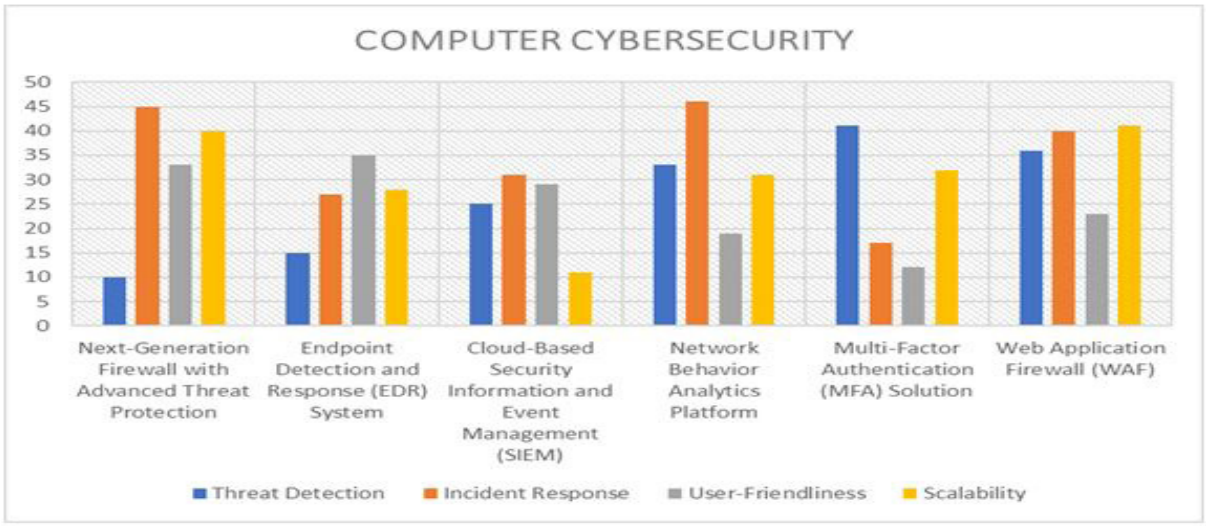

Figure 1 : Computer Cyber Security

In Figure 1, the performance of various Computer Cyber Security the Next-Generation Firewall with Advanced Threat Protection the highest Incident Response, while Threat Detection the lowest value. Endpoint Detection and Response (EDR) System the highest User-Friendliness, while Threat Detection the lowest value. Cloud-Based Security Information and Event Management (SIEM) the highest Incident Response, while Network Behavior Analytics Platform the highest Incident Response, while User-Friendliness the lowest value. Multi-Factor Authentication (MFA) Solution the highest Threat Detection, while ESET User-Friendliness the lowest value. Web Application Firewall (WAF) the highest Scalability, while Scalability the lowest value.

Table 3. Pair wise Comparison

	Pair wise Comparison					
	Next-Generation Firewall with Advanced Threat Protection	Endpoint Detection and Response (EDR) System	Cloud-Based Security Information and Event Management (SIEM)	Network Behavior Analytics Platform	Multi-Factor Authentication (MFA) Solution	Web Application Firewall (WAF)
D12	-3.5	-0.8	-0.54545	-0.68421	2	-0.17391
D13	-2.3	-1.33333	-0.36364	0.736842	2.416667	0.565217
D14	-3	-0.86667	1.272727	0.105263	0.75	-0.21739
D21	3.5	0.8	0.545455	0.684211	-2	0.173913

D23	1.2	-0.53333	0.181818	1.421053	0.416667	0.73913
D24	0.5	-0.06667	1.818182	0.789474	-1.25	-0.04348
D31	2.3	1.333333	0.363636	-0.73684	-2.41667	-0.56522
D32	-1.2	0.533333	-0.18182	-1.42105	-0.41667	-0.73913
D34	-0.7	0.466667	1.636364	-0.63158	-1.66667	-0.78261
D41	3	0.866667	-1.27273	-0.10526	-0.75	0.217391
D42	-0.5	0.066667	-1.81818	-0.78947	1.25	0.043478
D43	0.7	-0.46667	-1.63636	0.631579	1.666667	0.782609

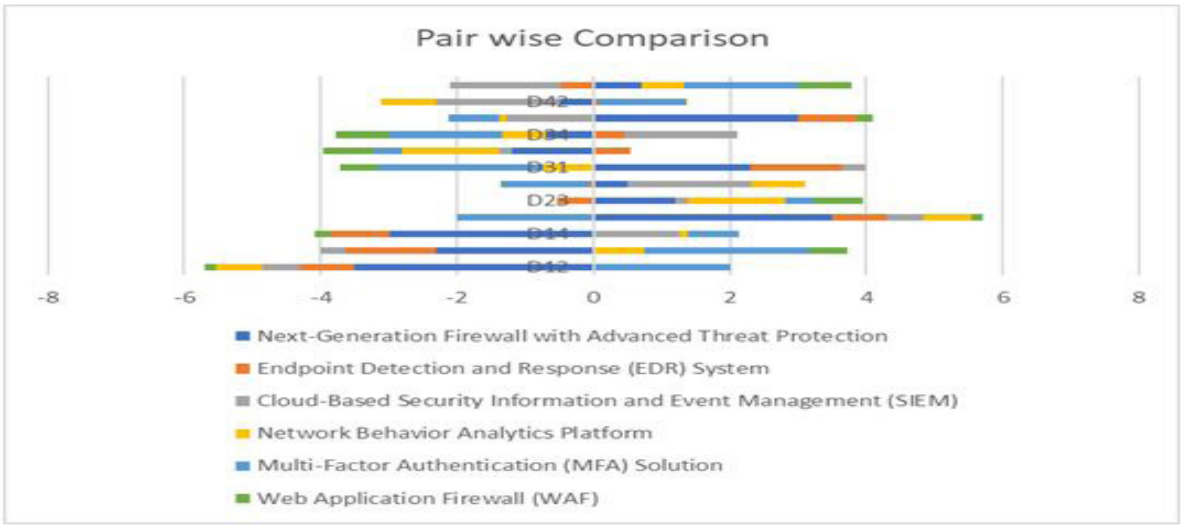

Figure 2 : Pair wise Comparison

Figure 2 represents a pair-wise comparison chart for the cybersecurity solutions. Each cell in the chart shows the relative scores assigned to one solution over another concerning specific criteria. Positive values indicate preference, negative values indicate inferiority, and zero indicates equal performance. The chart allows decision-makers to visually understand the comparative strengths and weaknesses of the cybersecurity solutions across different criteria, aiding in the decision-making process for selecting the most suitable solution based on specific priorities and requirements.

Table 4. Preference Value

	Preference Value						
	0.2336	0.1652	0.3355	0.1021	0.0424	0.1212	
D12	0	0	0	0	0.0848	0	0.0848
D13	0	0	0	0.075232	0.102467	0.068504	0.246203
D14	0	0	0.427	0.010747	0.0318	0	2
D21	0.8176	0.13216	0.183	0.069858	0	0.021078	1.223696
D23	0.28032	0	0.061	0.145089	0.017667	0.089583	0.593659
D24	0.1168	0	0.61	0.080605	0	0	0.807405
D31	0.53728	0.220267	0.122	0	0	0	0.879547
D32	0	0.088107	0	0	0	0	0.088107
D34	0	0.077093	0.549	0	0	0	0.626093
D41	0.7008	0.143173	0	0	0	0.026348	0.870321
D42	0	0.011013	0	0	0.053	0.00527	0.069283
D43	0.16352	0	0	0.064484	0.070667	0.094852	0.393523

Table 4 shows the preference values resulting from applying the PROMETHEE method to the pair-wise comparison matrix (Table 3) of the cybersecurity solutions. The preference values represent the relative strength of preference for one solution over another, calculated based on the pair-wise comparison scores. For instance, in comparison D12, the "Next-Generation Firewall with Advanced Threat Protection" has a preference value of 0.0848 over the "Endpoint Detection and Response (EDR) System," indicating a slight preference for the former in terms of "Threat Detection." In comparison D14, the "Cloud-Based Security Information and Event Management (SIEM)" has a high preference value of 2 over the "Network Behavior Analytics Platform," demonstrating a substantial preference for the former concerning "Scalability." The preference values provide decision-makers with a quantitative ranking of the cybersecurity solutions, allowing them to prioritize the most preferred options based on their specific criteria and preferences.

Table 5. Sum of Performance Value

	M1	M2	M3	M4	SUM	positive flow
M1	0	0.0848	0.246203	2	2.331003	0.777001
M2	1.223696	0	0.593659	0.807405	2.62476	0.87492
M3	0.879547	0.088107	0	0.626093	1.593747	0.531249
M4	0.870321	0.069283	0.393523	0	1.333127	0.444376
SUM	2.973564	0.24219	1.233384	3.433499		
Negative Flow	0.991188	0.08073	0.411128	1.1445		

Table 5 presents the results of the PROMETHEE method in the form of the sum of performance value and positive and negative flows for the cybersecurity solutions. The sum of performance value represents the net preference for each solution over all other alternatives, where higher values indicate more preferred solutions. For instance, "M4" has the highest sum of performance value at 3.433499, making it the most preferred cybersecurity solution overall. The positive flow measures the extent of dominance a solution has over other alternatives. "M1" has the highest positive flow at 0.777001, indicating its strong dominance in the decision-making process. On the other hand, the negative flow represents the extent to which a solution is dominated by other alternatives. "M4" has the lowest negative flow at 1.1445, suggesting that it is least dominated by other solutions. Overall, Table 5 provides decision-makers with valuable insights into the relative preferences and strengths of the cybersecurity solutions, allowing them to make well-informed choices based on the collective performance values and flows.

Table 6. positive flow & Negative Flow & Net flow & Rank

	positive flow	Negative Flow	Net flow	Rank
Threat Detection	0.777001	0.991188	-0.21419	3
Incident Response	0.87492	0.08073	0.79419	1
User-Friendliness	0.531249	0.411128	0.120121	2
Scalability	0.444376	1.1445	-0.70012	4

Table 6 presents the positive flow, negative flow, net flow, and ranking for each criterion in the context of the cybersecurity solutions. The positive flow indicates the extent to which a solution outperforms other alternatives within a specific criterion. "Incident Response" shows the highest positive flow of 0.87492, indicating its dominance in handling cybersecurity incidents. On the other hand, the negative flow measures the degree to which a solution is outperformed by other alternatives. "Scalability" has the highest negative flow at 1.1445, signifying its relatively weaker performance compared to other solutions in scalability. The net flow is calculated by subtracting the negative flow from the positive flow, representing the overall performance of each criterion. "Incident Response" attains the highest net flow of 0.79419, making it the most preferred criterion overall. the ranking column indicates the relative preference of each criterion, with "Incident Response" ranking first, followed by "User-Friendliness" in the second position, "Threat Detection" in the third position, and "Scalability" in the fourth position. These rankings enable decision-makers to prioritize cybersecurity criteria based on their importance and contribution to the overall decision-making process.

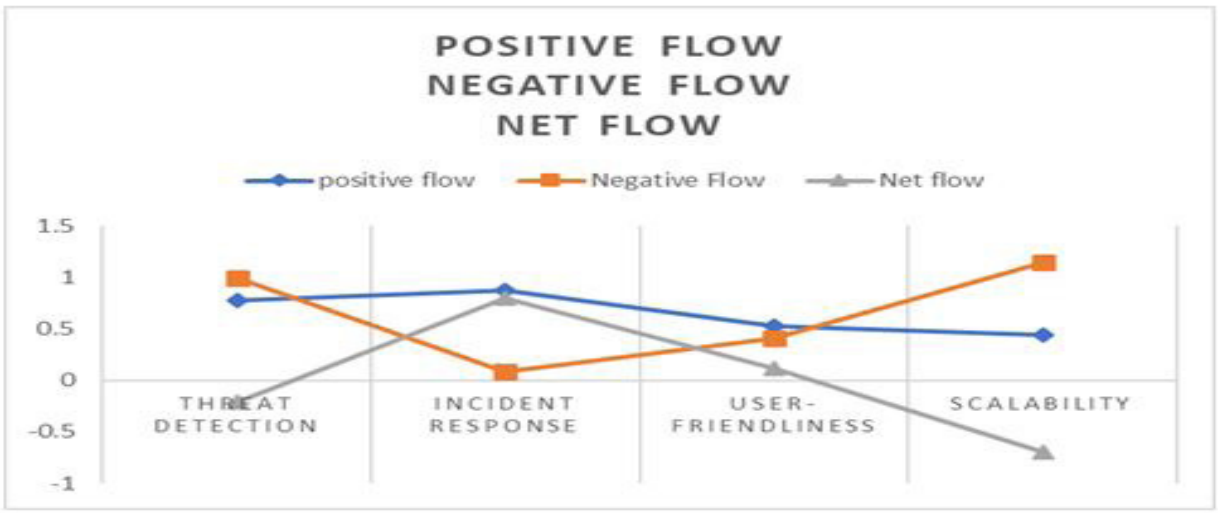

Figure 3 : Positive flow & Negative Flow & Net flow & Rank

In Figure 3, the positive flow, negative flow, and net flow values for each criterion ("Threat Detection," "Incident Response," "User-Friendliness," and "Scalability") are graphically represented using a line graph. The x-axis represents the criteria, and the y-axis represents the values of the flows. The line graph visually illustrates the performance and dominance of each criterion in comparison to others. The positive flow values are depicted as points above the zero line, indicating the degree of preference or dominance for a particular criterion. The negative flow values are shown as points below the zero line, signifying the extent to which a criterion is dominated by others. The net flow values are presented as the distance between the positive and negative flow points. This line graph helps decision-makers understand the relative strengths and weaknesses of each criterion, making it easier to prioritize and select the most suitable cybersecurity solutions based on their overall performance and contribution to the decision-making process.

Figure 3 : Positive flow & Negative Flow & Net flow & Rank

In Figure 6, the ranks for each criterion ("Threat Detection," "Incident Response," "User-Friendliness," and "Scalability") are represented using a line graph. The x-axis shows the criteria, and the y-axis represents the corresponding ranks. The line graph visually displays the relative rankings of the cybersecurity solutions, with "Incident Response" ranked first, "User-Friendliness" second, "Threat Detection" third, and "Scalability" fourth. This graph enables decision-makers to easily identify the most preferred criteria based on their rank in the decision-making process.

Conclusion

Computer cybersecurity stands as a critical and indispensable discipline in our modern digital landscape. As technology continues to advance and permeate all aspects of our lives, the security of computer systems, networks, and data becomes increasingly vital. Cyber threats, ranging from simple malware to sophisticated state-sponsored attacks, are pervasive and constantly evolving, making the protection of digital assets an ongoing challenge. The significance of computer cybersecurity lies in its multifaceted impact on various domains. From individual users to large corporations, from government agencies to critical infrastructure providers, everyone is vulnerable to cyber threats. Breaches and attacks can lead to devastating consequences, such as financial losses, data breaches, reputational damage, and even endangering public safety. Robust cybersecurity measures play a crucial role in safeguarding critical infrastructure, including power grids, transportation systems, and communication networks. The disruption of such vital systems could have severe consequences for society, making their protection a matter of national security. Moreover, cybersecurity research and implementation are essential in protecting personal and sensitive data. With the vast amount of information stored and exchanged online, from financial transactions to private communications, the risk of identity theft and privacy breaches is ever-present. Effective cybersecurity measures are essential to preserve individual privacy and protect against cybercrime. As technology evolves, cyber threats continue to become more sophisticated and adaptable. Cybersecurity research is crucial for staying ahead of attackers by identifying emerging threats and developing advanced defense mechanisms. The ability to anticipate and respond to evolving threats is vital to maintain the integrity of computer systems and networks. cybersecurity plays a critical role in fostering economic growth and innovation. Businesses must ensure the security of their digital assets and intellectual property to maintain a competitive edge and build trust with their customers. A secure digital environment encourages investment and enables the growth of digital economies. International cooperation and information sharing are vital components of effective cybersecurity. Cyber threats are not constrained by borders, and cybercriminals often operate from different countries. Collaborative efforts among nations are crucial in sharing threat intelligence, coordinating responses, and deterring cyber attackers.

References

1. Crick, Tom, James H. Davenport, Paul Hanna, Alastair Irons, and Tom Prickett. "Overcoming the challenges of teaching cybersecurity in uk computer science degree programmes." In 2020 IEEE Frontiers in Education Conference (FIE), pp. 1-9. IEEE, 2020
2. Wolf, Shaya, Andrea Carneal Burrows, Mike Borowczak, Mason Johnson, Rafer Cooley, and Kyle Mogenson. "Integrated outreach: Increasing engagement in computer science and cybersecurity." Education Sciences 10, no. 12 (2020): 353.
3. Thakur, Kutub, Meikang Qiu, Keke Gai, and Md Liakat Ali. "An investigation on cyber security threats and security models." In 2015 IEEE 2nd international conference on cyber security and cloud computing, pp. 307-311. IEEE, 2015.
4. Fees, Rachel E., Jennifer A. Da Rosa, Sarah S. Durkin, Mark M. Murray, and Angela L. Moran. "Unplugged cybersecurity: An approach for bringing computer science into the classroom." International Journal of Computer Science Education in Schools 2, no. 1 (2018): 3-13.
5. Gupta, Brij B., Gregorio Martinez Perez, Dharma P. Agrawal, and Deepak Gupta. "Handbook of computer networks and cyber security." Springer 10 (2020): 978-3.
6. Crick, Tom, James H. Davenport, Alastair Irons, and Tom Prickett. "A UK case study on cybersecurity education and accreditation." In 2019 IEEE Frontiers in Education Conference (FIE), pp. 1-9. IEEE, 2019.
7. Lédeczi, Ákos, MiklÓs MarÓti, Hamid Zare, Bernard Yett, Nicole Hutchins, Brian Broll, Péter Völgyesi et al. "Teaching cybersecurity with networked robots." In Proceedings of the 50th ACM Technical Symposium on Computer Science Education, pp. 885-891. 2019.
8. Arabo, Abdullahi. "Cyber security challenges within the connected home ecosystem futures." Procedia Computer Science 61 (2015): 227-232.
9. AlDairi, Anwaar. "Cyber security attacks on smart cities and associated mobile technologies." Procedia computer science 109 (2017): 1086-1091.
10. Abubakar, Adamu I., Haruna Chiroma, Sanah Abdullahi Muaz, and Lababatu Baballe Ila. "A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems." Procedia Computer Science 62 (2015): 221-227.
11. Tobey, David H., Portia Pusey, and Diana L. Burley. "Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league." ACM Inroads 5, no. 1 (2014): 53-56.
12. Katsikeas, Sotirios, Pontus Johnson, Mathias Ekstedt, and Robert Lagerström. "Research communities in cyber security: A comprehensive literature review." Computer Science Review 42 (2021): 100431.
13. Frank, Charles E., James W. McGuffee, and Cynthia Thomas. "Early undergraduate cybersecurity research." Journal of Computing Sciences in Colleges 32, no. 1 (2016): 46-51.
14. Burrell, Darrell Norman. "An exploration of the cybersecurity workforce shortage." In Cyber warfare and terrorism: Concepts, methodologies, tools, and applications, pp. 1072-1081. IGI Global, 2020.
15. Samtani, Sagar, Maggie Abate, Victor Benjamin, and Weifeng Li. "Cybersecurity as an industry: A cyber threat intelligence perspective." The Palgrave Handbook of International Cybercrime and Cyberdeviance (2020): 135-154.
16. Babaei, Sahar, Reza Ghazavi, and Mahdi Erfanian. "Urban flood simulation and prioritization of critical urban sub-catchments using SWMM model and PROMETHEE II approach." Physics and Chemistry of the Earth, Parts A/B/C 105 (2018): 3-11.
17. Venkata Rao, R., and Bhisma K. Patel. "Decision making in the manufacturing environment using an improved PROMETHEE method." International Journal of Production Research 48, no. 16 (2010): 4665-4682.

18. Anand, Gapesh, and Rambabu Kodali. "Selection of lean manufacturing systems using the PROMETHEE." Journal of modelling in management (2008).
19. Corrente, Salvatore, Salvatore Greco, and Roman Słowiński. "Multiple criteria hierarchy process with ELECTRE and PROMETHEE." Omega 41, no. 5 (2013): 820-846.
20. Goumas, MetVLYGEROU, and V. Lygerou. "An extension of the PROMETHEE method for decision making in fuzzy environment: Ranking of alternative energy exploitation projects." European Journal of Operational Research 123, no. 3 (2000): 606-613.
21. Mareschal, Bertrand, and Yves De Smet. "Visual PROMETHEE: Developments of the PROMETHEE & GAIA multicriteria decision aid methods." In 2009 IEEE International conference on industrial engineering and engineering management, pp. 1646-1649. IEEE, 2009.
22. Brans, Jean Pierre, and Bertrand Mareschal. "The PROMETHEE methods for MCDM; the PROMCALC, GAIA and BANKADVISER software." In Readings in multiple criteria decision aid, pp. 216-252. Springer, Berlin, Heidelberg, 1990.
23. Feng, Feng, Zeshui Xu, Hamido Fujita, and Meiqi Liang. "Enhancing PROMETHEE method with intuitionistic fuzzy soft sets." International Journal of Intelligent Systems 35, no. 7 (2020): 1071-1104.
24. Marinoni, Oswald. "A stochastic spatial decision support system based on PROMETHEE." International Journal of Geographical Information Science 19, no. 1 (2005): 51-68.
25. Tuzkaya, Gülfem, Bahar Sennaroglu, Zeynep Tuğçe Kalender, and Meltem Mutlu. "Hospital service quality evaluation with IVIF-PROMETHEE and a case study." Socio-Economic Planning Sciences 68 (2019): 100705.