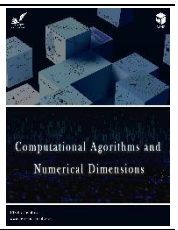
Computational Algorithms and Numerical Dimensions

www.journal-cand.com

Com. Alg. Num. Dim Vol. 2, No. 1 (2023) 23–34.



Paper Type: Original Article

Integrating PCA and DEA Techniques for Strategic Assessment of Network Security

Reza Rasinojehdehi[1,*], Seyyed Esmaeil Najafi[1]

[1] Department of Industrial Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran; reza.rasi1515@gmail.com; najafi1515@yahoo.com.

Citation:

Rasinojehdehi, R., & Najafi, S. E. (2023). Integrating PCA and DEA techniques for strategic assessment of network security. *Computational algorithms and numerical dimensions, 2*(1), 23-34.

Received: 12/10/2022 Reviewed: 14/11/2022 Revised: 09/12/2022 Accepted: 16/01/2023

Abstract

Network security is paramount in safeguarding the integrity of computer networks and the data they host. The primary objective of network security is to protect data from cyber-attacks and ensure the overall reliability of the network. A robust network security strategy deploys various solutions to shield data within networks, safeguarding both users and organizations from potential threats. This paper introduces a novel approach to evaluating computer network security using Data Envelopment Analysis (DEA), a mathematical method designed to measure the performance of Decision-Making Units (DMUs) employing identical inputs to yield identical outputs. We present a practical application of DEA to assess the security of 10 distinct networks, treating them as DMUs. The resulting performance measurements allow us to classify computer network security into four levels: "terribly insecure," "insecure," "safe," and "very safe. To optimize the discriminating power of DEA, we employ Principal Component Analysis (PCA) to reduce the number of inputs and outputs. It not only enhances the precision of our evaluation but also ensures that the number of DMUs remains well-suited to the analysis. As a rule of thumb, the number of DMUs should be at least three times larger than the sum of the numbers of inputs and outputs to maintain DEA's discriminating power. Through the combined application of DEA and PCA, this research contributes a comprehensive and efficient method for evaluating and classifying computer network security, providing valuable insights for enhancing overall network resilience against cyber threats.

Keywords: Data envelopment analysis, Principal component analysis, Computer network security, Decision-making unit.

1 | Introduction

The advancements in network technology undoubtedly enhance convenience in people's lives; however, they also introduce vulnerabilities, providing opportunities for cyber-attacks, Trojans, and other malicious programs that can compromise computer systems. This escalating threat poses a growing danger to the security of computer networks.

The primary goal of network security is to mitigate the potential damage caused by the misuse of data. Incorrect implementation of network security can lead to various issues. Every organization must safeguard sensitive information from unauthorized access, as the loss of data can diminish the added value of marketing efforts. In essence, the absence or inadequacy of security measures in a network may result in breaches of confidentiality in business and marketing. Thus, it becomes crucial

Corresponding Author: reza.rasi1515@gmail.com

https://doi.org/10.22105/cand.2023.424893.1076

for network administrators to enforce stringent policies to prevent potential data losses, irrespective of the network's size or type.

To bolster network security, identifying potential attacks is imperative. Attacks are defined as attempts to alter or exploit accessible resources on the network contrary to their intended use. These attacks can be broadly categorized into three groups:

I. Unauthorized access to data.
II. Unauthorized manipulation of information on a network.
III. Attacks leading to the disruption of service delivery, known as Denial of Service (DoS) [1].

Further classifications in the network security literature include:

I. Passive attacks: aimed at network identification, these attacks challenge the network's security [2].
II. Active attacks: direct assaults on servers [2], [3].
III. Internal attacks (Close-in): occur when the attacker has physical access to systems, potentially causing irreparable damage [3].
IV. Insider attacks: executed by internal users with access to systems and information [3], [4].

Effectively addressing these attacks involves selecting an appropriate security policy, which should minimize risks and potential damage. Security policies should be sufficiently general, focusing on broader aspects rather than intricate details. Key factors to be considered in a security policy include 1) the reason and type of data requiring protection, 2) assigning responsibility for data protection, and 3) designing a framework capable of resolving potential conflicts.

Traditional evaluation techniques like AHP and gray models struggle to capture the non-linear relationships between variables accurately. The Data Envelopment Analysis (DEA) method, introduced in this paper, is a novel mathematical approach based on operational research. Known for its objectivity and flexibility, DEA has demonstrated success across various fields. Due to its parameter-free nature, DEA simplifies mathematical operations and yields highly accurate results. In this study, DEA is employed to evaluate the security of computer networks, providing a robust and efficient method for assessing and enhancing network security.

2 | Literature Review

In this section, we review some key studies conducted by researchers in the fields of DEA, Principal Component Analysis (PCA), and computer network security.

DEA is a mathematical method designed to assess the relative efficiency of a set of homogeneous units referred to as Decision-Making Units (DMUs). These DMUs utilize multiple inputs to generate multiple outputs, and they are considered homogeneous as they all employ identical inputs to produce equivalent outputs. DEA gauges the relative efficiency of DMUs by constructing an efficiency frontier based on the best-observed data. Charnes et al. [5] developed a DEA model (CCR) grounded in Farrell's seminal work [6], assuming Constant Returns to Scale (CRS). Banker et al. [7] extended this model, known as BCC, to measure relative efficiency under the assumption of Variable Returns to Scale (VRS).

Here are some notable advantages of DEA [8]:

I. It accommodates multiple outputs and input variables for different units.
II. It handles both qualitative and quantitative data effectively.
III. It serves as a valuable decision-making tool, directing managerial attention to efficiency-related indices.

After the pioneering work of Charles, Cooper, and Rodes, a significant number of scholars proposed their models on DEA. [7, 8, 17–19, 9–16].

Karami et al. [20] introduced a three-step integrated procedure, DEA-PCA-VIKOR, to assess the garment industry. PCA reduced the criteria, and the additive DEA model evaluated the efficiency of suppliers or efficient suppliers.

Adler and Golany [8] determined the efficiency of deregulated railway networks by combining DEA and PCA, focusing on the West European air transportation industry.

Łozowicka and Lach [21] proposed an aggregated index variable for DEA models, utilizing original variables. The weights in their technique are obtained through an optimization problem, and variables are iteratively combined, akin to PCA-DEA. Their model is termed CI-DEA.

In their study, Gabriela et al. [22] measured the performance of Brazilian HUFs participating in the REHUF, employing PCA and DEA. They presented a descriptive and quantitative analysis, illustrating the applicability of their model, and applied their approach to assess the efficiency score of digitalization in the lives of Generation 50+ individuals across 32 European countries.

Horng et al. [23] introduced an innovative flow for an intrusion detection system using the Support Vector Machine (SVM) method. Their approach was implemented on the renowned KDD Cup 1999 dataset to evaluate its effectiveness. The findings reveal that, in comparison with other intrusion detection systems based on the same dataset, their method demonstrates superior performance in detecting DoS and Probe attacks.

Ahmad et al. [24] proposed a hybrid anomaly detection method employing k-means clustering. Wireless Sensor Networks (WSN) were simulated using the Optimized Network Engineering Tool (OPNET) simulator, generating a dataset consisting of traffic data with end-to-end delay data. The clustering of this dataset using WEKA 3.6 unveiled the activation of two types of anomalies: misdirection and black hole attacks in the network.

Tran et al. [25] presented a study introducing fuzzy gaussian mixture modeling for anomaly detection in networks. By employing fuzzy C-means approximation, they approximated Gaussian parameters, utilizing the KDD cup dataset. Their proposed approach demonstrated greater effectiveness than the vector quantization method.

Golmah [26] introduced a hybrid method incorporating the C5.0 decision tree and SVM algorithm to assess performance using the DARPA dataset. Their study indicates that the combination of SVM and C5.0 results in less execution time compared to applying only C5.0 or only SVM.

Mulak and Talhar [27] proposed a combined boundary-cutting algorithm and clustering algorithm to enhance the accuracy of the intrusion detection system, providing superior results compared to other segmentation methods.

Takkellapati and Prasad [28] presented a novel system based on the K-Nearest Neighbors (KNN) algorithm for feature selection to identify more discriminative features. They combined Greedy K-means clustering and SVM algorithms to detect network attacks, achieving a higher accuracy detection rate and lower error rate. The system was implemented on the KDD CUP 1999 training dataset.

Ioannis et al. [29] introduced a lightweight intrusion detection scheme to assess the impact of attacks in WSN by applying collaborative communication methodology. Their study also provided a general formulation for WSN.

Amini and Jalili [30] proposed an intrusion detection method using Adaptive Resonance Theory (ART) and PCA. PCA was utilized for feature selection to reduce the computational complexity and training time of ART. The study results indicate that their approach enhances the speed and accuracy of intrusion detection.

3 | Methods

This section delineates the procedural steps involved in implementing the PCA-DEA model for assessing computer network security. The key steps are outlined as follows:

I. Identify the assessment purpose: the initial step is to define the purpose of the evaluation clearly. The assessment purpose plays a fundamental role in shaping the criteria for inputs and outputs within the DEA models.
II. Determine DMUs: it is essential to identify the DMUs for evaluation. As a general guideline, the number of DMUs should be three times greater than the number of indicators to maintain the discriminating power of DEA effectively.
III. Select the appropriate model: choose the most suitable DEA model based on the identified assessment purpose and the nature of the network security evaluation.
IV. Evaluate computer network security: employ the DEA method to evaluate computer network security. Determine the scale models by integrating the chosen DEA model, taking into consideration the specified evaluation criteria.
V. Analyze performance and provide improvement suggestions: conduct a comprehensive analysis using performance metrics derived from the DEA evaluation. Based on the results, formulate improvement suggestions to enhance the overall network security.

To enhance the discriminating power of the DEA model, PCA is applied in this paper to reduce the number of indicators. Additionally, the Slacks-Based Measure (SBM) model, a renowned DEA model proposed by Rasoulzadeh et al. [11], is employed to evaluate the performance of DMUs.

In the subsequent sections, essential details about the SBM model and the PCA method are presented.

3.1 | SBM Model

The SBM, introduced by Rasoulzadeh et al. [11], is expressed as follows:

Assume there are n DMUs that need to be evaluated (DMU_j, j =1,...,n) and each DMU_juses m inputs indicated by x_{ij} , (i =1,...,m) to produce s outputs indicated by y_{rj} (r = 1, ..., s). the efficiency score for DMU_p (p = 1, ..., n) under evaluation using a non-orientated SBM model [26] with the VRS is formulated as follows:

$$\rho = \min \frac{1 - \frac{1}{m}\sum_{i=1}^{m}\frac{s_i^-}{x_{ip}}}{1 + \frac{1}{s}\sum_{r=1}^{s}\frac{s_r^+}{y_{rp}}}, \quad (1)$$

$$\text{s.t.} \quad \sum_{j=1}^{n}\lambda_j x_{ij} + s_i^- = x_{ip}, \quad i = 1, \ldots, m), \quad (2)$$

$$\sum_{j=1}^{n}\lambda_j y_{rj} - s_r^+ = y_{rp}, \quad r = 1, \ldots, s). \quad (3)$$

$$\sum_{j=1}^{n}\lambda_j = 1, \quad (4)$$

$$s_i^-, s_r^+, , \lambda_j \geq 0. \quad (5)$$

The model returns efficiency scores greater than 0 and is equal to 1 if and only if the DMU is on the efficient frontier without any slacks. *Models (1)* to *(5)* with fractional objective functions can be transformed into a standard linear programming problem.

3.2 | Principal Component Analysis

PCA stands out as a pivotal tool in the realm of dimensionality reduction, offering a nuanced approach to simplifying complex data in multivariate analyses. In this context, envision a scenario involving n DMUs, each strategically employing m inputs (\ (i = 1, ..., m\)) to yield s outputs (\ (r = 1, ..., s\)). The PCA-DEA approach integrates PCA to transform the original m inputs and s outputs into a set of Principal Components (PCs) of lower dimensionality. These PCs, arising from linear combinations of the original variables, succinctly capture the maximum variance inherent in the data.

PCA is fundamentally about substituting original variables with chosen components, especially when these initial components capture a considerable portion of the overall variance. It's worth noting that the resultant components derived through PCA are not only uncorrelated but also represent linear combinations of input and output variables arranged in descending order based on their variances. In our implementation, we opt for correlation over covariance, given the varying units of measurement often associated with DEA inputs and outputs. *Formulas (6)* and *(7)* delineate the mathematical expressions governing the PCs.

$$PC_i = l_{1i}.X_1 + l_{2i}.X_1 + \cdots + l_{mi}.X_m. \tag{6}$$

Subject to

$$\text{var } PC_i) = \max, \text{and } \sum_{j=1}^{m} l_{2i}^{\ 2} = 1. \tag{7}$$

Extending these concepts, analogous formulas guide the computation of principal component scores for the output variables. The overarching objectives of PCA encompass the derivation of a new set of variables known as PCs, characterized by:

I. Linearity as they represent combinations of the original variables.
II. A hierarchy where the first principal component captures the maximum variance in the sample data, followed by subsequent components.
III. Uncorrelated nature, contributing to their independence.

In the context of DEA, a methodological consideration arises—inputs and outputs typically must be strictly positive, while PCs can span negative values. Addressing this incongruity, we adjust all PC input data by the most negative value in the vector plus one when necessary, ensuring the positivity of the data.

PCs seamlessly substitute groups of variables with shared themes in DEA, a feature effortlessly accommodated by a generalized *Linear Program (2)*. Importantly, this integration of PCs preserves the fundamental properties of DEA models. The estimation of PCA model parameters, a crucial aspect of this methodology, is skillfully executed through the utilization of the Python programming language. This multifaceted exploration of PCA not only illuminates its operational intricacies but also underscores its indispensable role in augmenting the analytical capabilities of DEA within the dynamic landscape of computer network security assessment.

4 | Discussion

In the assessment of computer network security using the DEA model, a systematic approach is pivotal. The steps involved in this evaluation encompass determining the evaluation purpose, selecting decision units, acquiring and processing evaluation data, conducting the network security evaluation, and finally, performing an insightful analysis.

I. Determine the evaluation purpose: the bedrock of a successful DEA application lies in defining the evaluation purpose. This step is critical as it establishes the foundation for input and output indicators, shaping the entire assessment process.

II. Select decision units: a crucial consideration is the selection of DMUs. Generally, the number of DMUs should not fall below the number of indicators, encompassing both input and output variables.
III. Select and process evaluation data: The meticulous selection and processing of evaluation data are paramount. If the calculated results deviate from model assumptions, adjustments to input and output indicators become necessary. A recalibration ensures that the evaluation maintains its integrity, preventing extremes in the assessment of computer network security.
IV. Evaluate computer network security: by leveraging the DEA method, computer network security is comprehensively evaluated. This step involves determining the scale models by amalgamating the chosen model, resulting in a comprehensive assessment of the network's security posture.
V. Analyze and improve: informed by the findings of the computer network security evaluation, a meticulous analysis ensues. This analysis serves as the bedrock for deriving improvement suggestions, offering actionable insights to enhance the overall security framework.

In essence, this structured discussion outlines the essential steps within the DEA model application for evaluating computer network security. Each phase, from defining the purpose to deriving improvement recommendations, contributes to a comprehensive and effective assessment process.

Input and Output Indicators

In this study, we employ a comprehensive set of 5 input indicators focusing on both management security and logical security perspectives:

I. Safety management systems: encompasses systematic procedures, actions, and policies designed for managing safety risks and ensuring the effectiveness of safety risk controls.
II. Emergency response mechanisms: Activated in response to a network security incident, defined as inappropriate behaviors impacting network security. Given the severity and rapid occurrence of damages in such incidents, the speed and efficiency of emergency response mechanisms are paramount [31].
III. Data backup: involves the essential process of duplicating data from a primary to a secondary location, protecting in case of an incident.
IV. Data recovery: encompasses the crucial process of restoring data that has been lost in the event of an incident.
V. Access control: represents a security technique regulating who or what can access or utilize resources within a network.

In addition to the input indicators, we incorporate 3 comprehensive output indicators:

I. Network room security: pertains to the security of the room hosting network infrastructure, security equipment, servers, storage, and databases.
II. Fault-tolerant redundancy: signifies the property, enabling the network to continue functioning seamlessly even in the presence of incidents.
III. Security equipment: quantifies the number of essential security tools, including but not limited to anti-malware tools, intrusion detection and prevention systems, firewalls, network access control products, security information and event management products, mobile device management software, application security products, authentication and authorization technologies, data loss prevention technologies, email security appliances, web security solutions, virtual private networks, behavioral analytics tools, and all-in-one network security hardware appliances.

This comprehensive set of input and output indicators provides a holistic framework for the evaluation of computer network security, considering both preventative and responsive aspects. The inclusion of logical security measures alongside management security parameters ensures a nuanced assessment of the overall security posture.

Decision-Making Units

Given the scarcity and limited accessibility of shared datasets in the realm of computer network security, this study relies on an empirical investigation utilizing 13 distinct datasets for evaluation. These datasets are denoted as DMU1, DMU2, DMU3, DMU4, DMU5, DMU6, DMU7, DMU8, DMU9, DMU10, DMU11, DMU12, and DMU13.

Setting the Computer Security Level

This paper introduces a classification system for computer network security levels, categorizing them into four distinct tiers: 1) Safety (A), 2) Basic Safety (B), 3) Insecurity (C), and 4) Terribly Insecure (D). To operationalize this classification, efficiency score intervals have been established for each security level, as detailed in *Table 2*. This categorization framework enables a nuanced and practical assessment of the varying degrees of security across the evaluated computer networks.

Table 2. Network security levels.

Level	A	B	C	D
score	[0.85,1]	[0.7,0.85)	[0.5,0.7)	[0,0.5)

Evaluation

As the number of DMUs is not 3 times more than the number of input and output indicators, in this section, we apply PCA to input and output indicators.

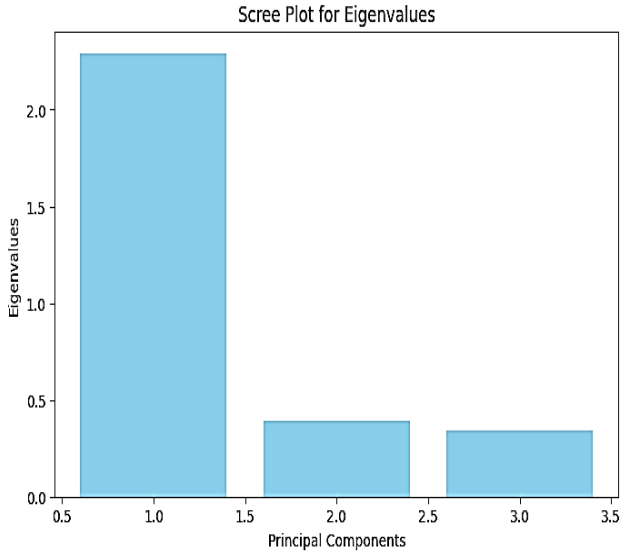
Table 3. The result of applying PCA on output indicators.

	Eigen Analysis			Coefficients of Correlations		
	Eigen Value	Proportion	Cumulative	y1	y2	y3
pc1	2.29	76	76.5	0.87	0.87	-0.89
pc2	0.39	12.6	88.9	0.48	-0.39	0.08
pc3	0.34	11.3	100.0	0.17	0.3	0.47

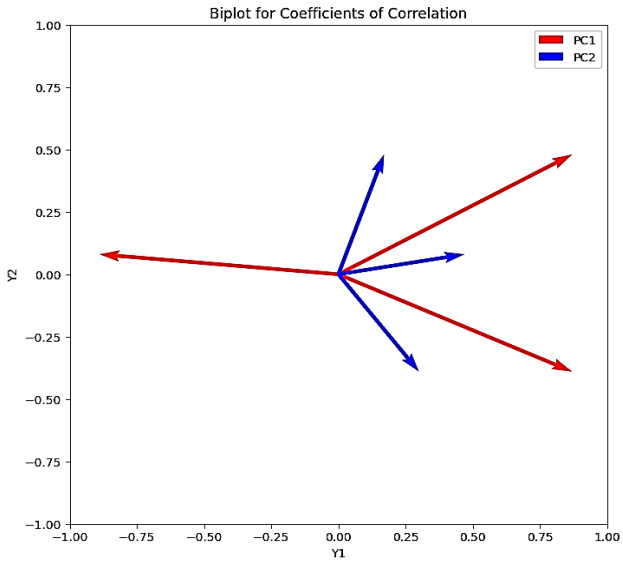
The results of the PCA applied to the output indicators are summarized in *Table 3*. PC1 emerges as the dominant principal component, capturing a substantial 76% of the total variance with a strong positive correlation between Y1 and Y2 and a notable negative correlation with Y3. PC2 contributes an additional 12.6% to the cumulative variance, demonstrating a distinct dimension of variability characterized by a positive correlation with Y1, a negative correlation with Y2, and a marginal impact on Y3. PC3, while having the smallest eigenvalue and proportion (11.3%), reveals a unique pattern of variation, particularly influenced by a positive correlation with Y1 and Y2 and a more pronounced positive correlation with Y3. The cumulative proportions of eigenvalues highlight the collective explanatory power of the PCs, with PC1 being the most influential. Coefficients of correlation provide insights into the strength and direction of relationships between the original variables (Y1, Y2, Y3) and the respective PCs, contributing to a nuanced interpretation of the dimensionality reduction achieved through PCA. The scree plot of eigenvalues (*Fig. 1(a)*) provides a concise visual representation, revealing the significance and contribution of each principal component in shaping the variability within the data.

In our quest to unravel the intricate relationships within the output indicators following PCA, the Biplot for coefficient of correlation emerges as a powerful visual tool. This dynamic representation encapsulates the interplay between the original variables (Y1, Y2, Y3) and the PCs (PC1, PC2, PC3), providing a comprehensive snapshot of their associations. Considering the biplot presented in *Fig. 1(b)*, vectors originating from the origin extend toward the variables and PCs, depicting the strength and direction of correlations. Each vector's length signifies the magnitude of the correlation, and the angle between vectors denotes the degree of association. The red vector, representing PC1, exhibits a strong positive correlation with both Y1 and Y2 while concurrently showcasing a notable negative correlation with Y3. On the other hand, the blue vector, representing PC2, illustrates its unique pattern with a positive correlation to Y1, a negative correlation with Y2, and a subtle influence on Y3. This biplot not only demystifies the complex

relationships but also aids in understanding the contribution of each original variable to the formation of PCs. As we traverse this visual landscape, the Biplot for the Coefficient of Correlation becomes a guiding compass, steering us through the multidimensional space of data relationships with clarity and precision. In conclusion, selecting PC1 as the sole output for the DEA model, capturing 80% of the output variance, streamlines variables from 3 to 1, ensuring efficiency without significant information loss.



a.



b.

Fig. 1. Visualization of principle components for inputs.

Table 4 showcases the results of PCA on input indicators, revealing that the first three PCs contribute significantly to data variance, cumulatively accounting for approximately 80%. PC1, with an eigenvalue of 1.84, stands out as the most influential component, displaying strong positive correlations with X3 and X4. PC2 and PC3 follow, contributing 22.5% and 20.3% to the cumulative variance, respectively. Their coefficients of correlation highlight distinct patterns of correlation with the original input variables. The subsequent components, PC4 and PC5, contribute progressively less to the overall variance. Considering the outcomes depicted in *Table 4*, it is evident that the first three components collectively account for approximately 80% of the entire variance within the input data. This substantial proportion signifies a comprehensive representation of the original inputs, emphasizing the efficiency gained by utilizing a reduced set of PCs. Opting for these first three components instead of the initial five inputs not only streamlines the data but also augments the discriminatory power of the DEA model,

offering a more concise and effective approach to evaluating the input indicators. *Fig. 2* visualizes the results indicated in *Table 4*.

Table 4. The result of applying PCA on input indicators.

	Eigen Analysis			Coefficients of Correlations				
	Eigen Value	Proportion	Cumulative	x1	x2	x3	x4	x5
pc1	1.84	37.0	37.0	0.27	0.55	0.82	0.59	0.68
pc2	1.1	22.5	59.5	-0.7	-0.3	-0.27	0.37	0.55
pc3	1.0	20.3	79.8	-0.59	0.65	0.12	-0.48	0.01
pc4	0.6	12.2	92.0	-0.08	0.35	0.27	0.52	-0.38
pc5	0.4	8.0	100	0.25	0.22	-0.42	0.1	0.35

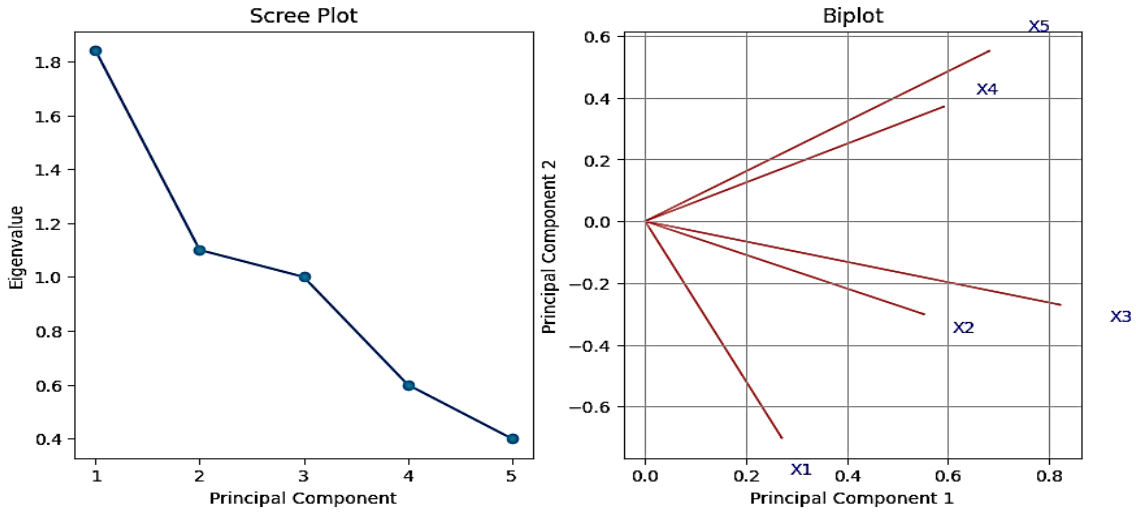


Fig. 2. Visualization of principle components for outputs.

4.1 | Performance Evaluation and Analysis of DMUs

In this subsection, we evaluate the computer network security of the presented models by applying a non-oriented SBM model under the assumption of a VRS. *Table 5* indicates the evaluation results, which show the efficiency score of each DMU. The efficiency value also ranks these ten samples.

Table 5. Efficiency score and Security level.

DMU	Efficiency Score	Level
DMU1	0.94	A
DMU2	0.55	C
DMU3	0.79	B
DMU4	1.00	A
DMU5	0.84	B
DMU6	0.53	C
DMU7	0.56	C
DMU8	0.81	B
DMU9	0.89	B
DMU10	1.00	A
DMU11	1.00	A
DMU12	0.72	B
DMU13	1.00	A

The efficiency scores in *Table 5* provide a comprehensive assessment of the computer network security for each Decision-Making Unit (DMU), categorized into efficiency levels. DMU1, DMU4, DMU10, DMU11, and DMU13 exhibit perfect efficiency scores of 1.00, placing them in level A, indicating a high degree of effectiveness in network security. DMU3, DMU5, DMU8, and DMU9 fall into level B, with efficiency scores ranging from 0.79 to 0.89, signifying a commendable performance. On the other hand, DMU2, DMU6, and DMU7, with efficiency scores ranging from 0.53 to 0.56, are classified in level C, suggesting areas for improvement in their network security measures. This analysis enables a nuanced understanding of the relative performance of each DMU, facilitating targeted enhancements for those in level C and acknowledging the robust security measures implemented by those in level A and level B.

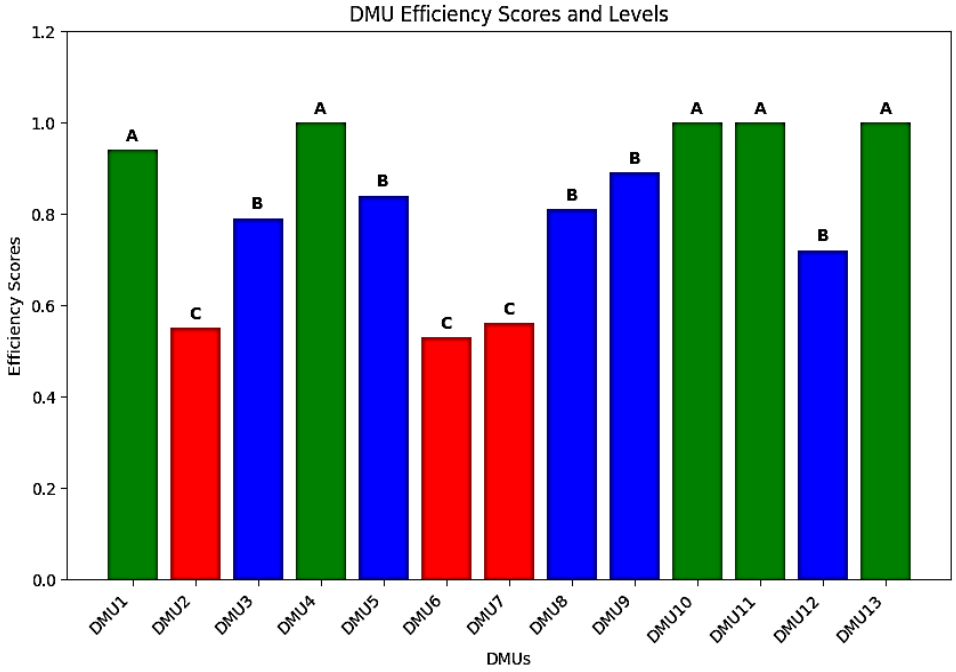


Fig. 3. Levels of network security for DMUs.

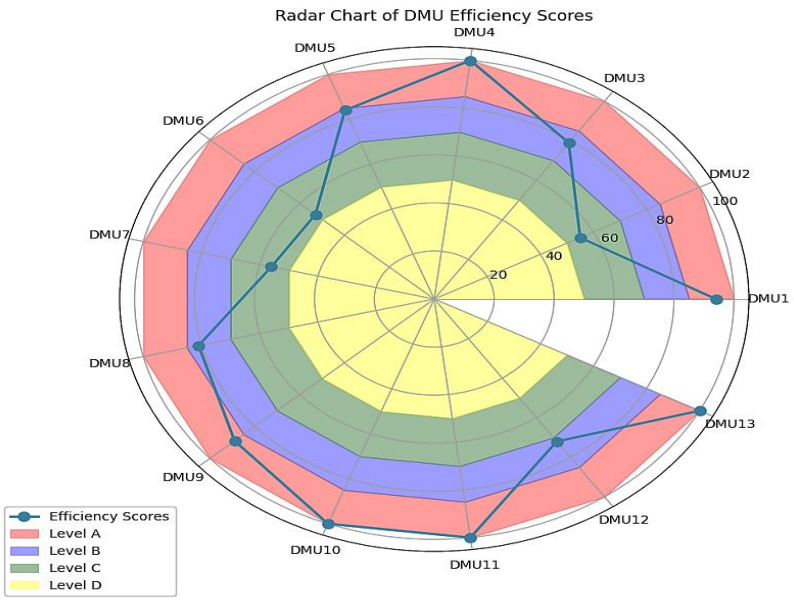


Fig. 4. A comparison of scores related to network security for DMUs.

5 | Conclusion

In conclusion, network security plays a crucial role in safeguarding connected computers and the data traversing the network from potential cyber threats. Our study delves into the evaluation of network security effectiveness using DEA, considering key input indicators such as safety management systems,

emergency response mechanisms, data backup, data recovery, and access control, along with output indicators like network room security, fault-tolerant redundancy, and line safety. Given the limited datasets, we employed PCA to reduce the number of indicators and enhance the discrimination power of DEA. The application of PCA revealed that the first output component and the first three input components sufficiently explained 80% of the variance, allowing us to streamline the original indicators. Subsequently, we employed the non-oriented SBM model to assess DMU performance, leading to the classification of security levels (A, B, C, D). Our findings indicate that 40% of the network settings are at the safety level, 37% are at basic safety, and the remaining 23% are classified as insecure. This study emphasizes the importance of strategic security measures in maintaining the integrity and reliability of network environments.

5.1 | Suggestions for Future Research

For future research, an exploration into the dynamic nature of network security, considering evolving cyber threats and technological advancements, could provide valuable insights. Investigating the effectiveness of emerging security technologies, such as artificial intelligence and blockchain, in enhancing network security would be a promising avenue. Additionally, an in-depth analysis of the impact of organizational size and industry type on network security performance could contribute to tailored security strategies.

References

[1] Xie, Q., Zhu, Y., Shang, H., & Li, Y. (2021). Variations on the theme of slacks-based measure of efficiency: convex hull-based algorithms. *Computers & industrial engineering, 159*. https://www.sciencedirect.com/science/article/pii/S0360835221003788

[2] Simmonds, A., Sandilands, P., & Van Ekert, L. (2004). An ontology for network security attacks. *Applied computing* (pp. 317–323). Berlin, Heidelberg: Springer Berlin Heidelberg.

[3] Pawar, M. V, & Anuradha, J. (2015). Network security and types of attacks in network. *Procedia computer science*, *48*, 503–506. https://www.sciencedirect.com/science/article/pii/S1877050915006353

[4] Greitzer, F. L., & Hohimer, R. E. (2011). Modeling human behavior to anticipate insider attacks. *Journal of strategic security, 4*(2), 25–48. http://www.jstor.org/stable/26463925

[5] Charnes, A., Cooper, W. W., & Rhodes, E. (1978). Measuring the efficiency of decision making units. *European journal of operational research, 2*(6), 429–444.

[6] Farrell, M. J. (2018). The measurement of productive efficiency. Royal statistical society. *Journal series a: general, 120*(3), 253–281. https://doi.org/10.2307/2343100

[7] Banker, R. D., Charnes, A., & Cooper, W. W. (1984). Some models for estimating technical and scale inefficiencies in data envelopment analysis. *Management science, 30*(9), 1078–1092.

[8] Adler, N., & Golany, B. (2001). Evaluation of deregulated airline networks using data envelopment analysis combined with principal component analysis with an application to Western Europe. *European journal of operational research, 132*(2), 260–273.

[9] Tone, K. (2001). A slacks-based measure of efficiency in data envelopment analysis. *European journal of operational research, 130*(3), 498–509.

[10] Shermeh, H. E., Najafi, S. E., & Alavidoost, M. H. (2016). A novel fuzzy network SBM model for data envelopment analysis: a case study in Iran regional power companies. *Energy, 112*, 686–697.

[11] Rasoulzadeh, M., Edalatpanah, S. A., Fallah, M., & Najafi, S. E. (2022). A multi-objective approach based on Markowitz and DEA cross-efficiency models for the intuitionistic fuzzy portfolio selection problem. *Decision making: applications in management and engineering, 5*(2), 241–259.

[12] Nojehdehi, R. R., Abianeh, P. M. M., & Valami, H. B. (2012). A geometrical approach for fuzzy production possibility set in data envelopment analysis (DEA) with fuzzy input-output levels. *African journal of business management, 6*(7), 2738. https://www.researchgate.net/profile/Hadi-Bagherzadeh-Valami/publication/266228810_A_geometrical_approach_for_fuzzy_production_

[13] Ghasemi, N., Najafi, E., Hoseinzadeh Lotfi, F., & Movahedi Sobhani, F. (2020). Assessing the performance of organizations with the hierarchical structure using data envelopment analysis: an efficiency analysis of Farhangian University. *Measurement, 156*, 107609. https://www.sciencedirect.com/science/article/pii/S0263224120301469

[14] Najafi, E., Aryanezhad, M., & others. (2011). A BSC-DEA approach to measure the relative efficiency of service industry: a case study of banking sector. *International journal of industrial engineering computations, 2*(2), 273–282. http://growingscience.com/ijiec/Vol2/IJIEC_2010_20.pdf

[15] Lotfi, F. H., Sadjadi, S. J., Khaki, A., & Najafi, E. (2010). A combined interval net DEA and BSC for evaluating organizational efficiency. *Applied mathematical sciences, 4*(36–39), 1975–1999.

[16] Kianfar, K., Ahadzadeh Namin, M., Alam Tabriz, A., Najafi, E., & Hosseinzadeh Lotfi, F. (2023). Presentation of a novel integrated DEA-BSC model with network structure in multi objective problems. *International journal of data envelopment analysis, 3*(11). http://ijdea.srbiau.ac.ir/article_13513.html

[17] Jaberi Hafshjani, M., Najafi, S. E., Hosseinzadeh Lotfi, F., & Hajimolana, S. M. (2021). A hybrid BSC-DEA model with indeterminate information. *Journal of mathematics, 2021*, 8867135. https://doi.org/10.1155/2021/8867135

[18] Rasinojehdehi, R., & Valami, H. B. (2023). A comprehensive neutrosophic model for evaluating the efficiency of airlines based on SBM model of network DEA. *Decision making: applications in management and engineering, 6*(2), 880–906.

[19] Bagherzadeh Valami, H., & Raeinojehdehi, R. (2016). Ranking units in data envelopment analysis with fuzzy data. *Journal of intelligent & fuzzy systems, 30*, 2505–2516. DOI:10.3233/IFS-151756

[20] Shirin Karami, R. G. Y., & Mousazadegan, F. (2021). Supplier selection and evaluation in the garment supply chain: an integrated DEA–PCA–VIKOR approach. *The journal of the textile institute, 112*(4), 578–595. https://doi.org/10.1080/00405000.2020.1768771

[21] Łozowicka, A., & Lach, B. (2022). CI-DEA: a way to improve the discriminatory power of DEA— using the example of the efficiency assessment of the digitalization in the life of the generation 50+. *Sustainability, 14*(6). https://www.mdpi.com/2071-1050/14/6/3610

[22] Peixoto, M. G. M., Musetti, M. A., & de Mendonça, M. C. A. (2020). Performance management in hospital organizations from the perspective of principal component analysis and data envelopment analysis: the case of federal university hospitals in Brazil. *Computers & industrial engineering, 150*. https://www.sciencedirect.com/science/article/pii/S0360835220305672

[23] Horng, S. J., Su, M. Y., Chen, Y. H., Kao, T. W., Chen, R. J., Lai, J. L., & Perkasa, C. D. (2011). A novel intrusion detection system based on hierarchical clustering and support vector machines. *Expert systems with applications, 38*(1), 306–313. https://www.sciencedirect.com/science/article/pii/S0957417410005701

[24] Ahmad, B., Jian, W., Ali, Z. A., Tanvir, S., & Khan, M. S. (2019). Hybrid anomaly detection by using clustering for wireless sensor network. *Wireless personal communications: an international journal, 106*(4), 1841–1853. https://doi.org/10.1007/s11277-018-5721-6

[25] Tran, D., Ma, W., & Sharma, D. (2008). Network anomaly detection using fuzzy gaussian mixture models. *International journal of future generation communication and networking, 1*(1), 37–42.

[26] Golmah, V. (2014). An efficient hybrid intrusion detection system based on C5. 0 and SVM. *International journal of database theory and application, 7*(2), 59–70. https://www.earticle.net/Article/A230140

[27] Mulak, P., & Talhar, N. (2014). Novel intrusion detection system using hybrid aprroach. *International journal of advanced research in computer science and software engineering, 4*(11). https://www.semanticscholar.org/paper/Novel-Intrusion-Detection-System-Using-Hybrid-Mulak-Talhar/2ea4d19684c15541c803762a0a4853f285c2868b

[28] Takkellapati, V. S., & Prasad, G. (2012). Network intrusion detection system based on feature selection and triangle area support vector machine. *International journal of engineering trends and technology, 3*(4), 466–470. https://ijettjournal.org/assets/volume-3/issue-4/IJETT-V3I4P201.pdf

[29] Ioannis, K., Dimitriou, T., & Freiling, F. C. (2007). Towards intrusion detection in wireless sensor networks. *Proc. of the 13th European wireless conference* (pp. 1–10). http://tassosdimitriou.com/various/IntrusionEW07.pdf

[30] Amini, M., & Jalili, R. (2004). Network-based intrusion detection using unsupervised adaptive resonance theory (art). *Proceedings of the 4th conference on engineering of intelligent systems* (eis 2004) (pp. 1–7). http://sina.sharif.edu/~amini/publications/conferences/2004/

[31] Yang, X., & Zhu, A. (2021). Research on computer network security emergency response systematization. *Journal of physics: conference series, 1771*(1), 1–6. https://dx.doi.org/10.1088/1742-6596/1771/1/012012