SCIENTIFIC OASIS

Decision Making: Applications in Management and Engineering

Journal homepage: www.dmame-journal.org
ISSN: 2560-6018, eISSN: 2620-0104

Evaluation and Selection of a Cybersecurity Platform ー Case of the Power Sector in India

Rakesh Verma[1], Saroj Koul[2,*] Ajaygopal KV[1]

[1] Indian Institute of Management Mumbai, Mumbai, India
[2] Jindal Global Business School, OP Jindal Global University, NCR, India

ARTICLE INFO

Article history:
Received 28 July 2023
Received in revised form 13 October 2023
Accepted 20 November 2023
Available online 28 November 2023

Keywords: Critical infrastructure (CI); Cybersecurity platform; Best-worst method; BWM; COBRA; Best-worst method-improved; BWM-I; Power-grid in India.

ABSTRACT

Maintaining interconnected infrastructures such as transportation, communication, power grids, and pipeline networks is paramount in emerging economies. One of the critical interruptions is the targeted attacks on the operating cyber-physical systems to disconnect operations, inspection, or monitoring of the system. Therefore, adopting a cybersecurity system (or platform) that provides holistic protection is vital for protecting the integrity of critical infrastructure networks. As such, this research aspires to provide a decision support system for cybersecurity managers or practitioners (in the Indian power sector) to select the best and appropriate platform for protection against cyber-attacks. A three-phase method is adopted. First, a literature search followed by an expert panel discussion identified alternatives (cybersecurity platforms) and selection criteria. Next, a questionnaire was developed. Thirdly, a hybrid Best-Worst Improved and COmprehensive distance-Based RAnking (BWM-I and COBRA) method was proposed and applied to evaluate the cybersecurity platform alternatives. Four alternatives (Cloud-Based Platforms, Web-Based Platforms, Application-Based Platforms, and AI-Based Platforms), six primary criteria, and fifteen unique sub-criteria were identified. Responses were collected from 80 power utility managers on a pan-India basis, ranking "End-to-End Coverage" criteria and the AI-Based platform as best. This approach identified the best cybersecurity platform that, if adopted, can be extended to other critical infrastructures, with an appropriate adjustment in the selection criteria. The study can be helpful to practitioners in evaluating cybersecurity platforms. Furthermore, it addresses a research gap in its application in a developing country like India.

1. Introduction

India ranks third globally for *malicious activity* after China and Russia [1]. In the previous two decades, India has seen significant technical advancement, and the usage and abuse of the Internet have expanded throughout the nation. The Government of India's IT Act (2000) [2] defines cybercrime as *any illegal or unethical activity through internet use or using computers as a tool.* The National Crime Records Bureau (NCRB), India [3], which tracks cybercrimes [2], has recorded 52,000

[*] *Corresponding author.*
E-mail address: skoul@jgu.edu.in

https://doi.org/10.31181/dmame712024891

cases since 2021. Major recent cyber-attacks recorded [2] are the Union Bank of India Heist in 2016, Wannacry Ransomware in 2017, Kudankulam Nuclear Power Plant in 2019, and Bharat Earth Movers Limited in 2020 [2]. In April 2022, several Indian electric facilities encountered cyberattacks. Creating appropriate norms and regulations relevant to the industry is one strategy to reduce the possibility of cyberattacks on India's power systems [4].

Kumar *et al*. [5] observed that attackers' intentions have grown from being motivated by financial benefits in organised crimes, such as *trading malware and credit card* information, to attacks that attempt to destroy the country's critical infrastructure and cause havoc [5]. Per the IT Act [2], critical Infrastructure (CI) *is "a computer resource, the incapacitation or destruction of which shall have a debilitating impact on national security, economy, public health, or safety"* [2]. It includes sectors such as Banking, Financial Services and Insurance, Power and Energy, Telecom, Transport, and Public Enterprises. The 2013 National Cyber Security Policy's [6] primary goals are to secure data or information, personal information, banking information, financial information, and sovereign data [7].

Also, in the energy sector, researchers Casanovas and Nghiem [8] at the International Energy Agency (IEA) defines cybersecurity as "*the ability to prevent or defend against cyberattacks and cyber incidents, preserving the availability and integrity of networks and infrastructure and the confidentiality of information"* [8]. To strengthen the cybersecurity policy, the Central Electricity Authority (CEA), under the auspices of the Power Ministry of India, has issued cybersecurity regulations [9] to improve the power sector's protection against cyber threats [10]. As it is the first time to lay out such cybersecurity guidelines for India's power sector, implementing them is still nascent [10]. These guidelines amplify the regulatory framework and effectuate different actions for early detection, management, and cyber-attack responses. For such holistic protection for a critical system, a cybersecurity system needs formulation to integrate the security mechanisms at one platform.

Critical infrastructure (CI), the backbone of any economy, includes transportation networks, communication networks, water and oil pipelines, and power grids [11]. The computer control systems coupled with physical processes achieve real-time monitoring and control. This combination creates a *cyber-physical system* (CPS) and frequently introduces weaknesses, thereby increasing the risk of breaking into the tangible physical system. Additionally, some CIs are interconnected and dependent upon one another. Therefore, a cyberattack on a section of an interdependent system could have cascade consequences [11] and could bring down the entire interconnected CI system. The recent cyber-attack in Denmark [12], where the communication systems were targeted and caused a sudden halt of the trains – is a prime example of interdependency between CI and the cascading effect of such attacks in CI. The dependency on CI can be categorised by Rinaldi *et al*. [13] as follows:

- *Physical*: Physical dependence on the movement of materials from one CI to another, such as when a power grid provides electricity for distribution and water treatment systems.
- *Cyber*: This refers to "Informational Interdependency," which is the dependence of two or more CIs on one another for information flow. For instance, knowledge of the demand from a water distribution system is necessary to calculate the volume of treated water at its water treatment facility.
- *Geographic*: A local environmental event might impact numerous CI components (or geospatial interdependency) due to physical proximity.
- *Association*: Mechanisms that can logically link two or more CIs, such as regulatory systems, legal and policies, are to blame for this dependence.

Cybersecurity is a collection of tools that protects cyberspace and, in turn, organisational and user possessions. According to Perwej [14], "Cybersecurity involves a collection of techniques and procedures that aim to protect computers, networks, databases, and software from unauthorised access, modification, destruction, or attacks" [14]. These include contracts, security models, metrics and vulnerability-controlling tactics, activities, preparation, best practices, assertions, and tools [15]. However, most CIs were built without considering cybersecurity issues; hence, the present CPS poses significant security challenges [15].

The International Telecommunication Union Cybersecurity aims to protect personnel, facilities, software, services, communications networks, information shared and stored in cyber-space, and the security aspects of the business and user resources against interconnected devices. As such, the following details [16] could be crucial for an attack [16]:

- Services, general system structure, hardware, software, network structure, system settings, and technology use
- Security tools, such as including antivirus software and firewalls
- Knowledge of established flaws in these technology components
- Access rights and general information for users.

The main goals of cyberattacks are to seize control of the targeted system, destroy the system, leak data, or stop the targeted system from functioning. Also, authors Enayaty-Ahangar *et al*. [17] noticed several businesses creating various techniques for cybersecurity solutions to use information about security occurrences, security analysis, and potential threat and warning images [17].

The cyber threats can be minimised by designing a suitable cybersecurity platform based on the firm's requirements. Lopez *et al*. [18] define a cybersecurity platform as a centralised system/integration of cybersecurity tools that protect data, networks, and users against cyber threats. Tools and platforms for cybersecurity have been developed to prevent unauthorised access to organisational databases. However, the security tools used in the present time with static signatures will fall short of dealing with malicious actors who frequently change their techniques and tactics to make the system more vulnerable.

Furthermore, malicious code can change slightly enough, making identifying signatures challenging for current security tools [19]. As such, it enables the integration of visibility analysis and control of security layers and data sources, enhancing protection, scalability, and efficiency [20]. Choosing an appropriate cybersecurity platform is a significant challenge for any industry. The challenges faced by enterprise security teams include an abundance of data, an abundance of tools, and a lack of funding [21]. An integrated security platform would help tie everything together in one location because it allows finding a new solution to unify security data, tools, and teams simultaneously. Hence, to identify a holistic, integrated cybersecurity platform that can be effective now and into the future, the following factors need to be considered [22, 23, 24]:

(i) Considerations around moving the data
(ii) Options for deployment
(iii) Connections needed to other tools
(iv) Openness and adaptability of the platform
(v) Orchestration and automation capabilities
(vi) Threat intelligence integration
(vii) Connecting Security Operations Center (SOC) teams
(viii) Risk management and dashboarding capabilities
(ix) Services Support

Many security platforms require moving all data onto that platform to access it. While putting all the data in one place seems like a good idea, it can be complex and expensive [25]. Furthermore, it can mean addressing important privacy and data residency issues. Therefore, from a cost and complexity perspective, it can be beneficial for a platform to connect to the data where it's already located without the need to move it. This approach can complement the existing tools and help optimise investments already made while providing a centralised view and access to data already spread across various agencies [26].

When choosing a platform [27], it can be essential to consider one that's open and flexible enough to support a security program as it changes. Consider whether it offers Open standards, Open-source technology, or Open connections. An open platform connects to third-party tools and supports custom connections and development. As per [27], this approach can help reduce vendor lock-in and promote interoperability with multiple security and Information Technology (IT) tools.

"Security orchestration, automation, and response," commonly named SOAR, are more robust solutions [28] when built into the leading security platform rather than offered separately. Here, they look for a security platform with SOAR as a core function to increase the security team's efficiency across various workflows and security use cases. While SOAR has traditionally been focused on the incident response side of threat management, it can provide benefits, like data security, when built into a more comprehensive platform [29]. In addition, it helps bring together SOC and data security teams.

Security analysts often use a variety of threat feeds and different products to comb through threat intelligence and inform their research and decisions. They [30] consider whether the platform provides threat intelligence reports, how this intellect gets integrated with other capabilities, and what threat intelligence vendors are supported [30]. Integrating threat intelligence into a security platform can reduce a security analyst's workload and allow for more prompt and informed decisions.

Nugraha [31] claimed that many security platforms are geared primarily toward security operations and the SOC. However, SOC teams often need to work with others, such as data security teams, to investigate and resolve incidents. When the platform can make it easier for these teams to collaborate and share information, it can increase efficiency and decrease the reaction time to a threat or breach. Also, Nugraha [31] observed that evaluating security platforms that go beyond the traditional SOC and connect the organisation's security environment more holistically is preferable.

Developing and deploying a specialised model that accurately detects all attacks is challenging due to the diversity of cybersecurity threats. Authors Skoumperdis *et al.* [32] researched the integration of cybersecurity tools into a platform that collectively addresses new possible threats and corrects inaccurate forecasts. It uses the best-performance model per the most current data, which is the key to system protection. Further, with several security tools afloat, security leaders are still trying to process the disparate, subjective definitions of risk generated by their means and prioritising remediation. Security executives seeking to minimise the risk profile need a solution quickly and efficiently that facilitates prioritisation and helps them determine the best action to reduce overall risk [32].

1.1. Research questions and objectives

Choosing an appropriate cybersecurity platform is a significant challenge for any industry. Despite this, through the literature review, it has been observed that no study discussed this issue. As such, the current study resolves the following research questions (RQs):

1. Which criteria are meaningful in choosing a cybersecurity platform from the standpoint of controlling the cyber-attack on CI?
2. Which are the appropriate methods used for the selection of the cyber platform?

The “Hybrid Multi-Criteria Decision Making (HMCDM)” scheme combination of "improved Best Worst Method (BWM-I)" with COBRA is used to assess India's cybersecurity platform for CI protection and act on the above two RQs.

Thus, the objective of this research is to achieve the following research objectives (ROs):

(i) Establish criteria for evaluating a cybersecurity platform for protecting CI in emerging economies.
(ii) Employing the BWM-I method, determine specified cybersecurity platform criteria weights.
(iii) Then, utilise the COBRA technique to select the optimal cyber security platform for mitigating cyber-attacks on CI.
(iv) Examine the potential impact of the proposed research on management.

Section 2 briefly reviews the current literature on cybersecurity advancements and criteria. The approach recommended for selecting a cybersecurity platform for CI management is detailed in section 3. An empirical study is presented in section 4, followed by a summary of findings and implications in section 5. Section 6 offers managerial insights, while section 7 features the conclusion and outlines future research directions. Toward the end, the references used are given.

2. Relevant literature

Critical Infrastructures are operated and monitored through cyber-physical systems. Anything that combines computer, networking, and physical processes is known as a "cyber-physical system (CPS)." An intelligent manufacturing line, for instance [33], may qualify as a CPS if the machines communicate with the materials and goods they are manufacturing to accomplish several tasks.

Atoum and Otoom [34] classified the existing cybersecurity models into seven categories based on their conception and application (Table 1). They conclude their study by highlighting the need for a comprehensive cybersecurity system to tackle a broad spectrum of attack vulnerabilities.

Table 1
Classification of Cybersecurity Models [34]

Cybersecurity Model	Drawback
Standard Model	Customisation is necessary for standard models to be accepted in specific organisational contexts, as they are generally too generic.
Decision Support Model	Decision support models may fail to communicate appropriately with lower-level cybersecurity systems because they are designed to help management.
Privacy Models	While privacy is a crucial objective of an effective cybersecurity model, the goals of privacy models can contradict demands for highly secure systems.
Infrastructure Models	The cybersecurity model dedicated to infrastructures can be resource-intensive, with unnecessary features that do not align with project goals.
Enterprise Models	Enterprise Models are designed to answer "what" rather than "how" questions, often applied at a smaller level.
Generic Models	The applicability of generic models in various cybersecurity contexts is contingent upon an appropriate cybersecurity strategy implementation.
National Models	Although national models safeguard the country's cyberspace, they do not fully mitigate the risks of external threats and may be vulnerable to legacy and political challenges in other cyberspace jurisdictions.

According to Jansen and Jeschke [35], vulnerabilities are weak points in automation or IT systems that hackers could use to attack a CPS. Vulnerability is the "*limitation in any information system, system security procedures, internal controls, or implementation that an attacker may manipulate"* [36]. The terms "*remote access, software, and local area network (LAN)"* are used to categorise vulnerabilities that might affect virtual machines used in cloud services and IT systems [37, 38]. (He *et al*. [39] observed that the most prevalent vulnerabilities are located at each interface between multiple components where information is exchanged. For example, the vulnerability in a SCADA system includes Network Protocols and Communication Networks, Human-Machine Interfaces, Database Servers, Application Servers, Remote Terminals, and Logic Controllers [38, 40].

Many industry devices are compromised [41] for the reasons listed below**:**

1) Many systems have equipment that operates for multiple weeks without security patches or antivirus software.
2) Most controllers used in Industry Control Systems (ICS) networks were created when the issue of cybersecurity was not a priority. As a result, they are susceptible to disruption from incorrectly formed network traffic and large volumes of appropriately constructed traffic.
3) Numerous ICS networks contain multiple entry points that allow cybersecurity threats to penetrate while eluding already-in-place cybersecurity safeguards.
4) As there is no segregation between unrelated networks, still most of the ICS networks are constructed as massive, flat networks.

Implementing a vulnerability assessment methodology is essential to discover and evaluate possible system threats to address these issues [42]. The German Federal Office [37] identifies the following categorisations of cyber threats for Information Security:

1) Undiscovered attack methods with no means of detection made possible by unidentified weaknesses
2) Attacks (indirect type) on the IT systems of the service providers who have authorised external access
3) Direct attacks over external access
4) Harmful malware that affects components without being specifically targeted and reduces their functionality
5) Interference with nearby networks or network segments

Authors [35, 41] mention multiple directed attacks on automation systems, internet-based attacks on decentralised control systems, unauthorised access to production networks from the office, malevolent patterns, and interference in communications from machine to machine. One of the most frequently discussed cyber threats is the "denial of service" attacks.

Making the best decision from a group of options is complicated, but using the MCDM process [43] can simplify things. MCDM involves studying several factors to arrive at the best solution. The problem's solution space can be discrete or continuous, and MCDM methods [44] are adept at managing both issues. For practical applications, the two components of MCDM involve selecting the criteria and their weights and gathering data to evaluate the options using a specific strategy. Two methods for weighing the choice criteria are subjective and objective [43]. The objective approach uses data from each attribute's decision matrix as a weighing variable, while subjective weighting methods consider the decision-maker's (DM) preferences. These methods are essential when accessing the full decision matrix becomes tricky. To simplify the evaluation process - a sub-matrix is constructed for pairwise comparisons of the attributes, revealing any discrepancies in DM preferences [45]. Multiple MCDM techniques exist to process the alternatives, depending on the criteria weights and the performance matrix. Such techniques [46] fall under *outranking methods*, which rank alternatives as objective under the set criteria and their relative significance. MCDM methods make decision-making more effective and can arrive at the best solution effortlessly.

While AHP and ANP are used extensively [47, 48, 49], some of the other existing weight evaluation methods are discussed below:

- *"FUCOM (FUzzy COgnitive Maps)*" [50] is helpful for decision-making when the relationships between variables are complex and uncertain. It can handle both qualitative and quantitative information and allows for considering both positive and negative feedback loops. However, this method can be computationally intensive and requires significant data and expertise to construct and analyse the fuzzy cognitive map [50].
- *"OPA (Objective and Subjective Weighting Approach)"* [51] is valuable where objective and subjective information is available for the criteria or attributes. It can handle both quantitative and qualitative measures and allows for considering both positive and negative criteria. However, the method requires significant data and expertise to specify appropriate weights for the criteria or attributes and to combine the objective and subjective weights [51].
- *"Direct Index-based Benefit Ratio (DIBR)"* [52] is a ratio-based decision-making method when the DM is interested in maximising the benefit of the selected choice. As an easy-to-use procedure, it doesn't require the determination of weights for the criteria or attributes. However, it may not be suitable for decision-making when the requirements or features are not independent or conflicting objectives [52].

Frequent inconsistencies in the pairwise comparison matrix can be attributed to various factors, including lack of concentration on the part of the expert. To make it consistent, experts often revise the ratings. Therefore, per [44], finding alternative methods to address this issue and produce more accurate and consistent results becomes necessary.

Within the domain of MCDM techniques, Rezaei [44] introduced the BWM technique, which contrasts with other methods, such as AHP and ANP, in computing weights through pairwise comparisons. Unlike AHP, BWM does not necessitate DMs to conduct pairwise comparisons regarding all the conditions. Instead, they are required to choose *the most successful and least desirable criteria,* equating them with other criteria using pairwise comparisons [53]. This approach is more efficient and less time-consuming, resulting in more consistent and accurate results than AHP and ANP [54]. Therefore, the BWM approach is more suitable for problems where the number of criteria increases. By utilising the BWM approach, DMs can save time and confidently make more informed decisions.

The prominent distance-based ranking techniques are discussed below:

- *VIKOR (VlseKriterijumska OptimizacijaIKompromisno Resenje)* [55] has been designed to satisfy the need for compromise solutions when there is no clear best alternative. VIKOR is used when multiple criteria need to be considered, and a compromise solution is required to balance each criterion's importance. The VIKOR method operates by initially ranking the alternatives according to each criterion and subsequently determining a compromise measure for each option that considers the distance between the ideal and worst solutions [55].
- In *MABAC (Multi-Attributive Border Approximation Area Comparison),* alternatives are compared with a reference alternative [56], and a border is constructed between the two choices in the multi-attribute space. The method can handle both quantitative and qualitative criteria and allows for considering both positive and negative criteria [56].
- *MARCOS (Multi-Attribute Rating and Classification of Options by Scoring)* [57] is based on the weighted sum model, where dynamic weights are used instead of fixed weights (as in other methods). The approach integrates the idea of dominance, in which an option that is better than another alternative in all criteria is considered to dominate that alternative [57].
- *MAIRCA (Multiple Attribute Interactive Rough Coefficient Analysis)* [58] is based on *rough set theory, a mathematical instrument for dealing with uncertain and incomplete data.* The method involves interactive rough coefficient analysis to determine the importance of each criterion and the degree of affiliation of each alternative to the decision classes [58].

- *LBWA (Linear Bilevel Weighting Approach)* [59] is a two-level decision-making method that involves a leader-follower structure. Here, the DM (leader) determines the weights of the criteria or attributes from which the followers (alternative) are evaluated. The technique uses a weighted sum model, where each option is assessed based on criteria and the weights assigned to each criterion [59].

A commonality among these methods is their utilisation of distance-based ranking from a reference point to evaluate alternatives. However, deciding which way is superior, such as using *ideal*, *anti-ideal*, and *average solutions,* presents a significant challenge. Another challenge is determining whether to utilise Euclidean or Manhattan distances. To address this challenge, Krstić *et al*. [60] have introduced a new comprehensive method, COBRA, which integrates the strengths of distance-based methods discussed previously, thereby removing the need to debate the best approach for ranking alternatives by distance and relation to a solution [60].

2.1 Criteria Selection

Our methodology draws criteria from sources that support fundamental characteristics of reliable cybersecurity systems in the context of the developing field of cybersecurity platform selection, where specialised literature is still developing. An evaluative framework has been created utilising available literature to identify the criteria. The contributions of subject-matter experts made it possible to validate these chosen criteria. This framework for evaluation includes a wide range of standards informed by the varied features of modern cybersecurity platforms. For instance, the Department of Defense Chief Information Officer [61] emphasises the significance of thorough coverage across an organisation's cybersecurity landscape, ranging from network security to endpoint security, in their "The Cybersecurity Resource and Reference Guide." Next, our assessment enhances the platform's capacity to deliver high-performance security solutions, as highlighted in "The Department of Defense Zero Trust Reference Architecture" [62]. Additionally, "The Commercial Facilities Sector: Cybersecurity Framework Implementation Guidance" [63] supports the importance of centralised management and reporting, supporting our focus on these capabilities. Also, “The Cybersecurity Resource and Reference Guide" [61] provides wide-ranging insights to help hybrid deployment and centralised management standards as influential factors.

The guidance provided by "The Vendor Selection Criteria" [64] has significantly influenced our approach to evaluating cost-effectiveness, strengthening our economic evaluation methodology even though some aspects, like openness, may need further exploration due to the lack of existing literature. Our creative framework relies on the *synergy* of research and professional perspectives because there isn't enough literature to draw from. This adaptive methodology guarantees a thorough evaluation of cybersecurity platforms, demonstrating the industry's dynamic nature. Our method emphasises the blending of research, expert knowledge, and creative thinking, which results in a dynamic model for selecting an effective cybersecurity platform.

An esteemed panel of experts was instrumental in helping us refine our selection criteria as we worked towards an in-depth evaluation of cybersecurity platforms. These professionals were chosen based on requirements and had a wealth of experience and accomplishments in cybersecurity. They were selected based on their years of experience, essential roles in reputable organisations, and exceptional contributions to various cybersecurity-related fields, such as cryptography, malware analysis, risk management, and cybersecurity research. The details of the participating experts are provided in Table 2.

Table 2
Participating Experts [Names and Companies hidden on anonymity)

Participant	Expertise	Years of Experience
Expert 1	Cryptography, Privacy, Security	Over 30
Expert 2	Antivirus Software, Cybersecurity Threats	Over 25
Expert 3	Malware Analysis, Cybercrime	Over 30
Expert 4	Cybersecurity Research, Data Analytics	Over 20
Expert 5	Security Program Development	Over 20
Expert 6	Cybersecurity Awareness	Over 30

These distinguished experts were presented with criteria based on existing literature and initial research. The criteria encompassed a range of pertinent aspects crucial for evaluating the efficacy and suitability of cybersecurity platforms. This panel actively validated and fine-tuned the proposed criteria through collaborative discussions and iterative feedback. Their insights, expertise, and critical evaluations ensured that the requirements (criteria) resonated with real-world challenges and industry needs. The compilation of identified criteria is presented in Table 3. The experts introduced three additional measures along with the specified criteria from the literature.

Table 3
Evaluation Criteria

Sub-Criteria	Source
End-to-End Coverage	Department of Defense Chief Information Officer (2021)[61]
Performance Capability	Department of Defense Chief Information Officer (2022) [62]
Hybrid Deployment	Department of Defense Chief Information Officer (2021))[61]
Central Managing and Reporting	Cybersecurity and Infrastructure Security Agency (2021) [63]
Openness	**Expert Addition**
Cost	Center for Internet Security (2023) [64]
End Point Detection	Cybersecurity and Infrastructure Security Agency (2023) [65]
Continuous Protection	Department of Defense Chief Information Officer (2022) [62]
Real-Time Protection	Cybersecurity and Infrastructure Security Agency (2021) [63]
Data Loss Prevention	U.S. Office of Personnel Management (2018) [66]
Auto-Updating of Rules	Cybersecurity and Infrastructure Security Agency (2023) [65]
Accelerated Protection	Cybersecurity and Infrastructure Security Agency (2023) [65]
Insider Threat Protection	Cybersecurity and Infrastructure Security Agency (2023) [65]
Large Detection Spectrum	Center for Internet Security (2023) [64]
Localised Security	Department of Defense Chief Information Officer (2021))[61]
Operating System Flexibility	Department of Defense Chief Information Officer (2021))[61]
Native Integration	Center for Internet Security (2023) [64]
Remote Vendor Access	**Expert Addition**
Central Visibility	Department of Defense Chief Information Officer (2021))[61]
Security Authentication	**Expert Addition**
Complete Privilege Control	Department of Defense Chief Information Officer (2021))[61]

3. Methodology

This section describes the methodology used in this study to evaluate and rank cybersecurity platforms for protecting critical infrastructure. Our method entails a multi-step procedure combining knowledge from domain specialists and existing published literature. The initial relevant criteria were determined by a thorough analysis of pertinent literature and endorsed by a group of senior subject-matter experts. A well-structured questionnaire was then created to include these discovered criteria. The next step was to collect the data, which involved carefully compiling the responses from respondents. Data pre-processing ensured data quality and involved determining geometric means for the ratings obtained.

After building on this foundation, a comprehensive ranking of the cybersecurity platforms based on the established criteria was created by applying the proposed method to the dataset. This methodological approach guarantees the accuracy of our analysis and offers a systematic framework for ranking cybersecurity platforms for the defence of critical infrastructure. Figure 1 depicts the flow of the adopted methodology and the three proposed steps under it are:

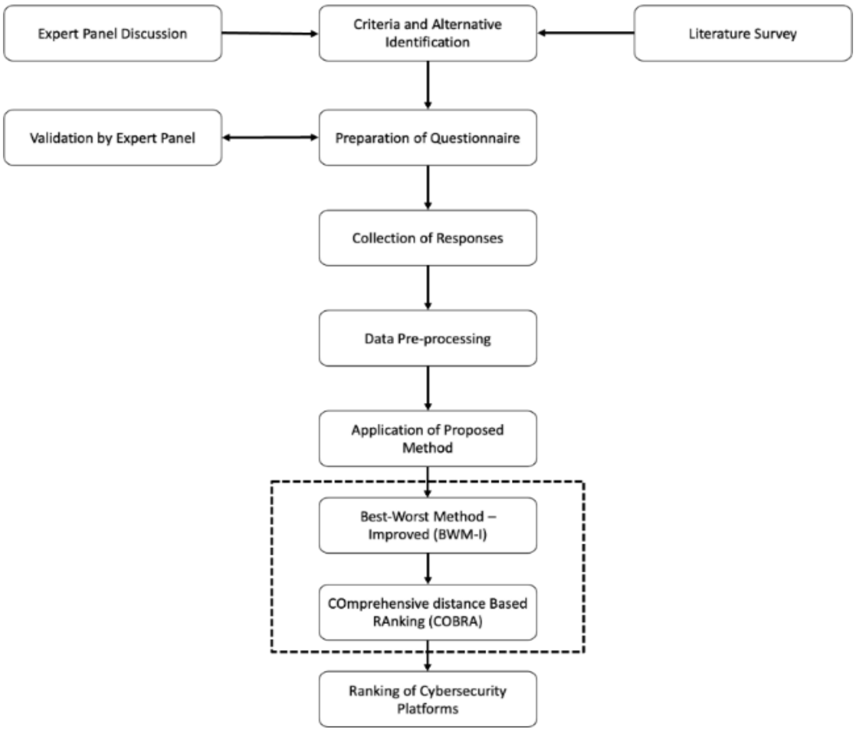
Expert Panel Discussion
Criteria and Alternative Identification
Literature Survey
Validation by Expert Panel
Preparation of Questionnaire
Collection of Responses
Data Pre-processing
Application of Proposed Method
Best-Worst Method – Improved (BWM-I)
COmprehensive distance Based RAnking (COBRA)
Ranking of Cybersecurity Platforms

Fig. 1. Flowchart of the methodology adopted

Step 1: Questionnaire preparation:

A brainstorming session was carried out with a group of six experts consisting of four senior managers from power sectors in India and two academicians working in the field of cybersecurity for power grids. The cybersecurity managers had over ten years of experience, and the academicians had at least two publications. The group of experts in the discussion concurred with the Cybersecurity Guidelines established by the Central Electricity Authority of India [9].

Four types of cybersecurity platform options were identified as a consensus of the discussion session. While also applicable globally, these are as follows:

I. *Cloud-Based Platforms:* administrators secure data in a third-party service's infrastructure, such as Cloud.
II. *Web-Based Platforms:* Protect networks and computer systems from targeted and available software, hardware, or data attacks online.
III. *Application-Based Platforms:* Local security application that protects platform-installed devices.
IV. *AI-Based Platforms:* Utilising Artificial Intelligence (AI) capabilities, Machine Learning techniques, and algorithms.

Following this, the expert group determined multiple evaluation criteria, structured into main criteria and sub-criteria, and the same are presented in Figure 2.

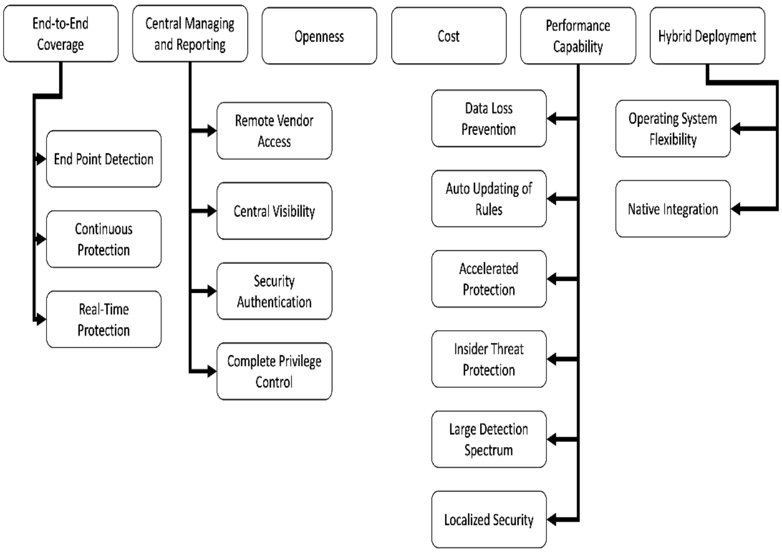

Fig. 2. Main Criteria and Sub-Criteria

Due to the availability of multiple cybersecurity platforms (also applicable globally), making an informed decision on choosing the right platform is difficult. However, no comprehensive framework or method could be obtained from the literature. Therefore, a BWM-I evaluation needs to be carried out by taking responses through a questionnaire, explained in the following section.

Step 2: Data Collection:

The respondents were power utility managers working in pan India with at least five years of experience. The questionnaire (**Annexure A**) consists of two parts: one for evaluating the cybersecurity platforms against the criteria (**Annexure A1**) and the second part for weighing the criteria using BWM and BWM-I (**Annexure A2**).

Taherdoost [67] reports that for rating selection, while shorter scales do not reveal much information about the respondent's evaluation, multiple studies by the author indicate that longer scales (seven-point to nine-point) show more details. Therefore, all variables are subjectively captured using a nine-point Likert scale [68] [1 being *Worst Performing* and 9 being *Best Performing*] for the platform evaluation (first) part and "9" being "Most important" and "1" being "Equally Important" for the criteria weight evaluation (second) part [67, 68].

Step 3: Applying Hybrid BWM-I and COBRA method:

This study uses a hybrid method to assess and choose a cybersecurity platform from the four identified platforms. The hybrid approach combines the "Best Worst Method (BWM)" and "COmprehensive Distance Based Ranking (COBRA)" methods, as explained by Krstić *et al*. [60]. The step-by-step approach is in Figure 3.

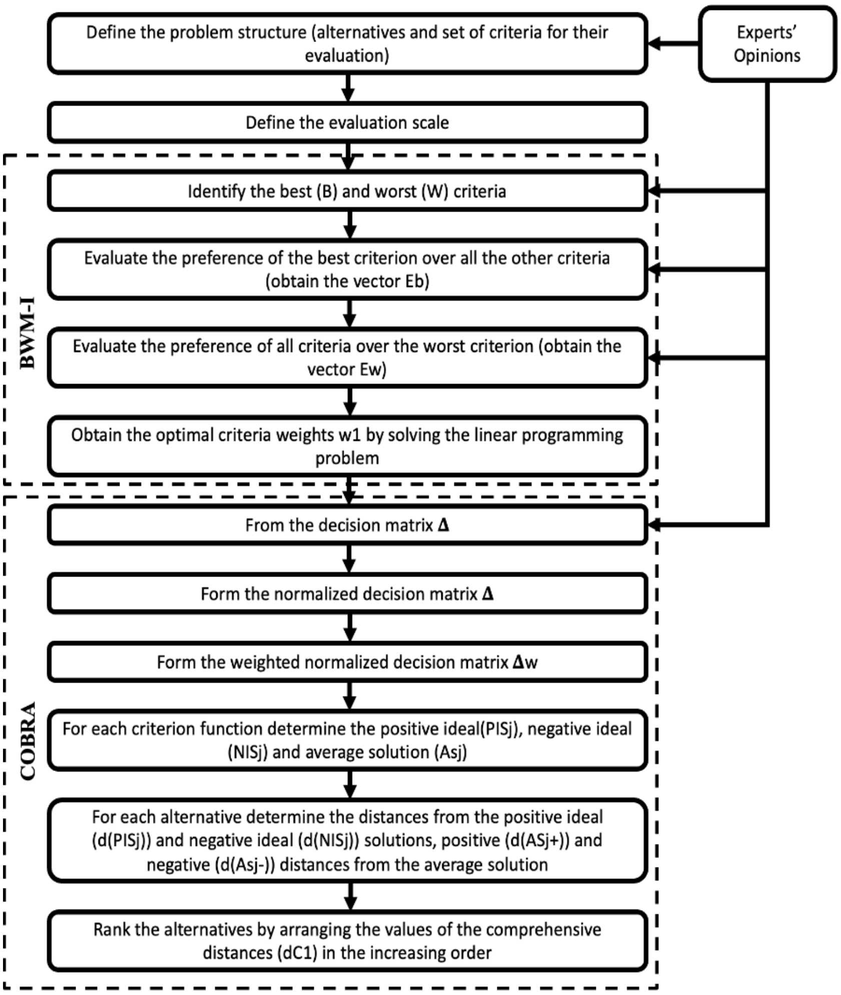
Define the problem structure (alternatives and set of criteria for their evaluation)
Experts' Opinions
Define the evaluation scale
BWM-I
Identify the best (B) and worst (W) criteria
Evaluate the preference of the best criterion over all the other criteria (obtain the vector Eb)
Evaluate the preference of all criteria over the worst criterion (obtain the vector Ew)
Obtain the optimal criteria weights w1 by solving the linear programming problem
COBRA
From the decision matrix **Δ**
Form the normalized decision matrix **Δ**
Form the weighted normalized decision matrix **Δ**w
For each criterion function determine the positive ideal(PISj), negative ideal (NISj) and average solution (Asj)
For each alternative determine the distances from the positive ideal (d(PISj)) and negative ideal (d(NISj)) solutions, positive (d(ASj+)) and negative (d(Asj-)) distances from the average solution
Rank the alternatives by arranging the values of the comprehensive distances (dC1) in the increasing order

Fig. 3. The adopted step-by-step approach (All Authors)

3.1 Best/Worst method

Instead of utilising a comprehensive matrix for pairwise comparisons, BWM proposes [69] comparing each criterion against the 'best criterion' and every other criterion versus the 'worst criterion' [69]. Through pairwise comparisons, the BWM model makes it easier to compare and rank alternatives based on various criteria. Moreover, it assists in structuring decision-making issues and establishing the relative weight of multiple considerations [70]. The subsequent steps outline the BWM methodology:

(i) Determine the best and worst criterion: Let the whole set of 'n' criteria be denoted as $C_1, C_2, \dots, C_n$. From the set of criteria, identify the best and worst criteria {C_B and C_W}.

(ii) Rate best and worst criterion over other criteria using the nine-point Satty scale [46, 71].

$$A_B = (a_{B1}, a_{B2}, \dots, a_{Bn}) \quad [1]$$

$$A_W = (a_{1W}, a_{2W}, \dots, a_{nW}) \quad [2]$$

(iii) Solve the below equation for minimising the maximum absolute difference:

$$Minimize: \ \lambda$$

subject to constraints:

$$\left|\frac{W_B}{W_j} - a_{Bj}\right| \leq \lambda \qquad \textit{for all j}$$

$$\left|\frac{W_j}{W_W} - a_{jW}\right| \le \lambda \qquad \textit{for all j} \qquad [3]$$
$$W_W + W_B + \sum_j W_j = 1$$
$$W_W, W_B, W_j \ge 0 \qquad \textit{for all j}$$

The optimal values of $W_1^*, W_2^*, \dots, W_n^*, W_B^*, and\ W_W^*$ is weights of the criteria.

3.2 Improved Best/Worst method – (BWM-I)

Applying BWM, as detailed in Section 3.1, assumes that the DM can identify one *best* and one *worst* criterion only from the criteria listed. However, where multiple *best and/or worst* criteria exist, the standard BWM approach falls short. Also, Pamučar *et al*. [72] created an enhanced version of the BWM, referred to as BWM-I, to overcome this limitation. This approach accommodates multiple "best and worst criteria" scenarios and calculates criteria weights using a set of equations, as proposed by [72]:

$$Minimize\text{: } \lambda$$

Subject to constraints:

$$\left|\frac{W_B}{m_b W_j} - a_{Bj}\right| \le \lambda \qquad \textit{for all j}$$
$$\left|\frac{W_j}{m_w W_W} - a_{jW}\right| \le \lambda \qquad \textit{for all j} \qquad [4]$$
$$W_W + W_B + \sum_j^{n-m_b-m_w} W_j = 1$$
$$W_W, W_B, W_j \ge 0 \qquad \textit{for all j}$$

By approaching Eq. [4], the weights of all the criteria are calculated. Therefore, when DMs can choose more than one best or worst criterion, BWM-I is more suitable than general BWM.

3.3 COmprehensive distance-Based Ranking (COBRA)

"COmprehensive distance-Based Ranking (COBRA)", an MCDM method, evaluates the distance between each alternative's rating and the *ideal* rating for each criterion. The process then ranks the other options based on their proximity to the *ideal* solution, as proposed in [60]. The COBRA methodology comprises the following steps:

(i) Classify each criterion as a cost or benefit factor, determine each alternative's ratings against every criterion, and form the below decision matrix 'A'.

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix} \qquad [5]$$

(ii) Generate a weighted normalised decision matrix, Δ_w:

$$\Delta_w = [\alpha_{ji}]_{n\times m} \qquad [6]$$

where,

$$\alpha_{ji} = \frac{w_i \times a_{ji}}{\max_j a_{ji}} \quad [7]$$

(iii) Estimate the *positive ideal, negative ideal,* and *average rating* for each criterion as:

$$PIS_i = \max_j \alpha_{ji}\text{, for all } i\ in\ 1,\dots,n, i\ in\ J^B \quad [8]$$

$$NIS_i = \max_j \alpha_{ji}\text{, for all } i\ in\ 1,\dots,n, i\ in\ J^B \quad [9]$$

$$AS_i = \frac{\sum_{j=1}^{m} \alpha_{ji}}{n}\text{, for all } i\ in\ 1,..,n, i\ in\ J^B, J^c \quad [10]$$

here, $J^B\ and\ J^c$ are benefit and cost criteria, respectively

(iv) Evaluate the difference of rating between ideal and average ratings as:

$$d(S_j) = dE(S_j) + \sigma \times dT(S_j) \times dE(S_j)\text{, for all } i = 1,\dots,m \quad [11]$$

here, dE and dT denote the Euclidian and Chebyshev distances [60].

(v) Measure the comprehensive distance and rank in ascending order.

$$dC_i = \frac{d(PIS_i)_j - d(NIS_i)_j - d(AS_i)_j^+ + d(AS_i)_j^-}{4}\text{, for all } i = 1,\dots,m \quad [12]$$

4. Empirical Study – Case of the Indian Power Sector

A country's economy depends on CI, specifically its power grid control system. Trivial cyber-attacks on the power grid's management systems can be potent enough to impact an entire continent or even several nations connected through the grid. A case in point [73] is the impact of grid failure in Bhutan, creating the total grid failure of the Eastern regional grid in India [73]. A power grid control system's risk profile and operation method differ from a conventional information technology system [74, 75]. The threats include effects on human health and mortality and environmental harm. While electrical characteristics, like angle, voltage, or frequency stability, are maintained under desirable levels, the control strategy regulates the actuators and the sensors in field breakers, switches, electronic devices, and generators. The synchronisation of the generator rotor speed with the system frequency is related to angle stability [76]. While delays in communication systems are more lenient, sensors and actuators operate in real-time, making reaction time crucial. Developing and deploying cybersecurity safeguards for power grid control systems is essential [77]. The ramifications of attacks can be minimised by monitoring inter-node traffic, checking for protocol adherence, and spotting unusual control requests. Before any essential component is attacked, specialised honeypots that mimic weak intelligent electronic devices (IEDs) can reveal information about the motivation, behaviour, techniques, and tools of attackers [78]. A holistic cybersecurity platform eliminates a significant portion of the risk.

Under the directives of the Government of India, CEA developed guidelines to reinforce the cybersecurity of the Power Sector in India. The procedures in [9] were aimed mainly at addressing the following policies:

1. Create awareness of cybersecurity.
2. Ensure a safe cyber environment.
3. Strengthen regulatory framework.
4. Develop a system for early detection and response to cyber threats.
5. Enhance vulnerability management.
6. Safeguard remote services and operations.

7. Build resilience of critical infrastructure.

In compliance with the CEA guidelines [9], this study conducted an expert group discussion where six main criteria for cybersecurity platform evaluation were derived:

(i) *End-to-End Coverage*: Comprehensive coverage must include endpoints such as PCs, mobile devices, and IoT devices.

(ii) *Performance Capability*: State-of-the-art efficiency must be provided while also showing an incremental increase in protection efficiency with an additional attachment of tools.

(iii) *Hybrid Deployment*: Users should be able to deploy in any operating system and utilise individual aspects of the platform according to their situational demand.

(iv) *Central Management and Reporting*: Each unique tool needs to be connected to a centralised administration plane that offers customisable role-based access control for various users, views, and functions.

(v) *Openness*: Ability to integrate with other supporting tools from diverse vendors.

(vi) *Cost:* The price of the platform.

Once the criteria and alternatives were identified, a questionnaire was prepared and circulated among managers at all the regional power grids (namely, North, East, West, South and North-Eastern Region). Managers with at least five years of experience were considered for responding. The questionnaire consisted of 16 questions capturing *best* and *worst criteria*, rating criteria as *best criteria* and *worst criteria*, and finally, rating alternatives against all the criteria. The responses were collected between April 2023 and June 2023. A total of 80 responses were considered for further analysis based on input-based consistency.

The analysis was carried out in three phases. In the first stage, *best* and *worst criteria* were identified by respondents among each set of criteria and sub-criteria (Table 4), and BWM-I was used to determine local and global weights for each criterion (Table 5) using Python 3.7. Python is the ultimate tool for efficient data analytics, offering a plethora of libraries and editors. With its impressive growth rate, it's no surprise that Python is the go-to language for data scientists. Moreover, Python's capabilities [79] go beyond mathematical research - a wealth of computational resources are available to support most data analysis studies**.**

Table 4
Best and Worst Criteria (as per respondents' viewpoint)

Main Criteria	*Respondent's view*	Sub-Criteria	*Respondent's view*
End-to-End Coverage	Best	End Point Detection	
		Continuous Protection	Best
		Real-Time Protection	Worst
Performance Capability		Data Loss Prevention	
		Auto-Updating of Rules	Best
		Accelerated Protection	
		Insider Threat Protection	
		Large Detection Spectrum	Best
		Localised Security	Worst
Hybrid Deployment	Best	Operating System Flexibility	Worst
		Native Integration	Best
Central Managing and Reporting		Remote Vendor Access	Best
		Central Visibility	
		Security Authentication	Worst
		Complete Privilege Control	
Openness			
Cost	Worst		

Table 5
Optimal weights for main and sub-criteria

Main Criteria	Weight	Sub-Criteria	Weight	Global Weight
End-to-End Coverage	0.34865	End Point Detection	0.40668	0.14179
		Continuous Protection	0.40969	0.14284
		Real-Time Protection	0.18363	0.06402
Performance Capability	0.13290	Data Loss Prevention	0.18180	0.02416
		Auto-updating of Rules	0.31815	0.04228
		Accelerated Protection	0.09090	0.01208
		Insider Threat Protection	0.06060	0.00805
		Large Detection Spectrum	0.31815	0.04228
		Localised Security	0.03030	0.00402
Hybrid Deployment	0.34865	Operating System Flexibility	0.46667	0.16270
		Native Integration	0.53333	0.18595
Central Managing and Reporting	0.07970	Remote Vendor Access	0.32631	0.02601
		Central Visibility	0.25549	0.02036
		Security Authentication	0.20154	0.01606
		Complete Privilege Control	0.21666	0.01727
Openness	0.05690			0.05690
Cost	0.03320			0.03320

The COBRA method was applied to the second stage's decision matrix in Table 6. First, using Eq. [4-11] described in section 3.3, *positive ideal*, *negative ideal,* and *average* ratings were calculated. After this, Euclidean and Chebyshev's distances were calculated. Finally, using Eq. [12], comprehensive distances were calculated. The alternatives were then ranked by ascending order of the comprehensive distances per the steps detailed in section 3.3 (see Table 7).

Table 6
Decision Matrix

CRITERIA	Cloud-Based	Web-Based	Application-Based	AI-Based
End Point Detection	2	4	2	3
Continuous Protection	4	4	8	4
Real-Time Protection	1	9	2	5
Data Loss Prevention	3	4	6	5
Auto-updating of Rules	4	6	2	3
Accelerated Protection	8	8	4	1
Insider Threat Protection	2	9	1	5
Large Detection Spectrum	5	6	8	5
Localised Security	3	2	9	1
Operating System Flexibility	3	2	2	8
Native Integration	1	8	3	8
Remote Vendor Access	2	1	6	3
Central Visibility	3	1	7	6
Security Authentication	4	8	1	9
Complete Privilege Control	7	4	1	3
Openness	5	3	5	7
Cost	7	4	7	9

Table 7
COmprehensive decision-Based Ranking of Alternatives

	ALTERNATIVES			
	Cloud-Based	*Web-Based*	*Application-Based*	*AI-Based*
d(PIS)	0.1960	0.1340	0.1711	0.0800
d(NIS)	0.0394	0.1663	0.0825	0.1943
d(AS+)	0.0103	0.0742	0.0481	0.0999
d(AS-)	0.0862	0.0430	0.0596	0.0202
dC	0.0581	-0.0158	0.0250	-0.0485
Rank	*4*	*2*	*3*	*1*

The analysis was performed using Python 3.7 [MacBook with Apple M1 Chip, 8 GB memory, and CORE-8].

5. Results and Discussion

This study was driven by two important research questions listed in Section 1. A literature search was conducted to identify evaluation criteria for a cybersecurity platform. Since no study addressed the impacting factors for cybersecurity platform selection, the authors identified six main criteria and 15 corresponding sub-criteria, as in Table 4. The criteria were validated by a six-member expert panel answering the first research question. The proposed methodology answers the second question, and the inferences of the analysis are discussed below.

Based on the information presented in Table 5, it is apparent that the two main criteria, "End-to-End Coverage" and "Hybrid Deployment," carry the most weight. The sub-criterion under End-To-End coverage, viz. "Continuous Protection" is considered the most desirable by experts, indicating a preference for regular, uninterrupted, and robust endpoint detection, whereas real-time detection is deemed the least significant. Furthermore, the second main criterion, "Hybrid Deployment," is ranked first among all the six main criteria, focusing on native integration over operating system flexibility, as the operating system remains consistent.

Although "Performance Capability" seems to be the most important criterion, the experts rank it as the second most important criterion. "Performance Capability" includes six sub-criteria - *Large Detection Spectrum, Auto-updating of Rules, Insider Threat Protection, Data Loss Prevention, Accelerated Protection, and Localised Security*. The *Large Detection Spectrum* is ranked as the most important since *Intrusion Detection* is a preliminary step to counteract cyber-attacks. *Auto-updating of Rules* reduces the work and reinforces security by minimising the delay between identifying and updating outdated rules.

"Openness", ranked third, offers different packages and software to operate together. Hence, firms should weigh the ability of the cybersecurity platform to connect with other packages of their cybersecurity system and function in harmony. "Central Managing and Reporting" is ranked fourth among the main criteria, implying that the control and visibility of security add control to the defenders and resultant robust protection. Finally, the "Cost" is the least important when choosing the right cybersecurity platform, as the potential losses are tremendous. The inputs received (see Decision Matrix Table 6) were fed to Eq. [6-20] sequentially to obtain the comprehensive distances of each alternative, as shown in Table 7.

Thus, it can be concluded that AI-based cybersecurity platforms are most preferred, followed by Web-based, Application-based, and Cloud-based cybersecurity platforms in the same order. However, the outcome seems generic since the cost factor (one of the six identified platform evaluation criteria) is not a constraint for large organisations, as considered in the case study. On the other hand, for minor players, the results may vary as the *Cost* is a significant component in decision-making.

6. Managerial insights

Cybersecurity managers of the power sector have an essential role in protecting critical systems. The power sector is especially vital as other infrastructures, such as transportation and communication, depend highly on the power sector. As such, it becomes a priority for cybersecurity managers to select a suitable application platform. This study proposes a methodology for decision support in this concern.

As inferred by Wirkuttis and Klein [80], the AI-based cybersecurity platform is appropriate for protecting power grid infrastructure as AI has many advantages over industrial cybersecurity applications [80]. Firstly, AI learns more and only more with time. By using machine learning, the AI learns the behaviour of a business and its associated networks. This way, it identifies anomalies and intrusions effortlessly. AI also detects unknown threats by tracking suspicious behaviour in the system. Companies handle a large volume of data on a day-to-day basis. AI is most capable of analysing such data and finding attacks on the system. AI quickly assesses weak points in the design system and networks and focuses on critical tasks. Furthermore, AI has a large detection spectrum that updates its rules automatically, providing accelerated detection and swift response [81].

Moreover, AI provides strong security authentication by analysing user behaviour. AI, with time, learns and understands the patterns of human interaction in the system [82]; hence, it makes the system secure in the case of identity theft, as the attacker mostly cannot replicate the user's pattern, and AI detects a mismatch in the user pattern promptly [82]. However, according to researchers Leszczyna and Leszczyna [83], although AI-based cybersecurity provides the best security solution, the Cost of AI-based cybersecurity platforms is considerably high. Experts and practitioners have given the least weight to cost as they belong to large organisations dealing with crucial data. However, the platform's Cost is significant for small and medium businesses.

Hence, it is the decision of the manager to deploy AI-based cybersecurity platforms based on the level of security required for the firm or industry. In addition, the proposed BWM-I-COBRA method is a valuable tool in group decision-making, which is essential in industry.

7. Conclusion

Cybersecurity is critical in today's digital era. With Cyber-physical systems now in full swing, the requirement for cybersecurity has seen colossal attention. As a result, much literature has been published addressing cybersecurity. In addition, numerous research studies were identified in the literature review, formulating organisational strategies to prevent and counter cyber-attacks. However, no literature provides guidelines for selecting a suitable cybersecurity platform or evaluates the available cybersecurity platforms. Alternatively, we conduct a literature survey followed by field expert validation to determine the evaluation criteria. Further, this study applies the MCDM technique to bridge the gap and assess the most suitable cybersecurity platforms. The study was conducted in three phases:

- Phase one identified the cybersecurity platform alternatives (Cloud-based, Web-based, Application-based, and AI-based) and evaluation criteria. By building upon the literature study and expert opinion - six primary criteria and fifteen unique sub-criteria were identified. A questionnaire with 16 questions was developed and sent to cybersecurity managers in the power sector and academicians in the second phase.
- The proposed BWM-I-COBRA method was applied in the second phase to evaluate the alternatives. Improved BWM was utilised to assess the weight of the criteria. Each respondent

had to rate each criterion (*End-to-End Coverage, Performance Capability, Hybrid Deployment, Central Managing and Reporting, Openness, and Cost*) on a scale of 1 to 9 as the "best and worst criteria." Each alternative's ratings for each criterion were compiled in one place. The weights were determined from the 80 eligible responses using nonlinear BWM-I approaches.

- Finally, the platforms were ranked using the COBRA method in the third phase. The findings of the quantitative analysis show that experts prefer AI-based cybersecurity platforms due to their high capability to reform themselves and provide security. Web-based, application-based, and cloud-based platforms followed them.

This study captured the preference of emerging economies and the same act as the limitation of this study. Also, the criteria identified are limited to the scope of the power sector, restricting the application of specified criteria to the power sector alone. Therefore, capturing the point of view of global cybersecurity managers is an important direction for future studies to observe the commonalities and differences in cybersecurity preferences, thereby extending to identifying cybersecurity criteria applicable to varied sectors of future research.

Author Contributions

Concept visualisation, R.V.; Conceptualization, R.V. and S.K.; Model development, R.V. and A.G.; Model review, S.K.; Data collection, A.G. and S.K., Software Analysis, R.V. and A.G.; Writing – original draft, A.G.; Writing – literature review, editing, and submission completion, S.K.. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Acknowledgement

This research was not funded by any grant. The authors thank the six experts for their time and advice on validating the criteria. Also, the authors thank all participants - senior executives from the power grid companies based in India and the university faculty for their responses from January to April 2023.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Annexure-A (Questionnaire)

MULTI-CRITERIA ANALYSIS FOR EVALUATING CYBERSECURITY PLATFORM

Introduction

Today, technology is developing at a breakneck pace. As a result, businesses can use several technological solutions to drive growth and improve operations. However, while it proves useful for businesses, cyber criminals, too, are utilising such technology to their advantage, making attacks more complex and harder to defend. To prevent different types of cyber-attacks on critical infrastructure, organisations must invest in cyber solutions to ensure they are protected and better equipped to face data breaches. However, selecting and implementing suitable strategies to reduce cyber-attacks is a complex problem. In this context, this research attempts to identify and evaluate preferred adaptation alternatives that help to select appropriate cybersecurity platforms. With this study, we are exploring stakeholders' opinions on adapting other options to cybersecurity platforms.

We intend to evaluate four cybersecurity platforms through a questionnaire to obtain stakeholders' opinions. Respondents use a questionnaire to compare the "best and worst criteria" with specific criteria, as in Figure A1.

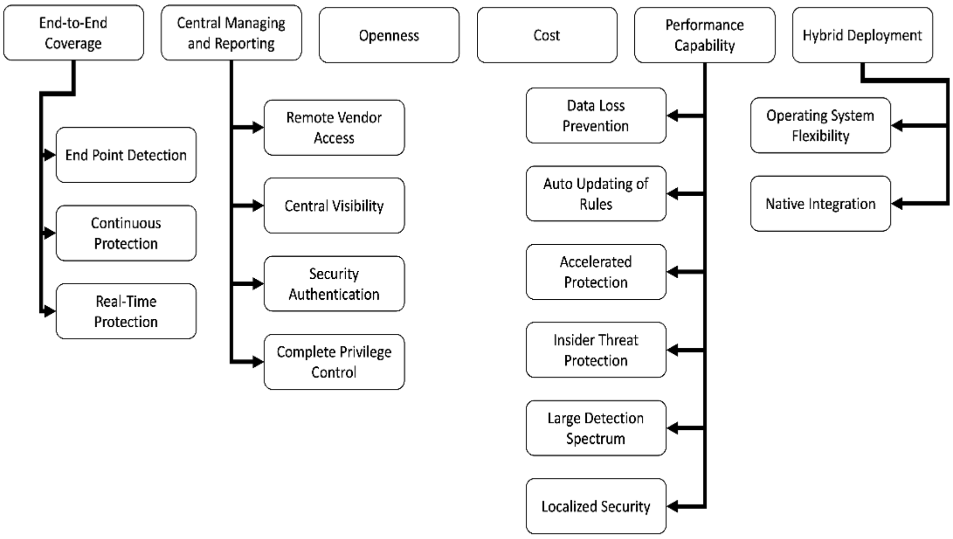

Fig. A1. Selection Criteria

Goal: Cybersecurity Platform Evaluation
Criteria: Six criteria were chosen for the platform evaluation:

(i) *End-to-End Coverage*: Comprehensive coverage must be provided that includes endpoints such as PCs, mobile devices and IoT devices.

(ii) *Performance Capability*: State-of-the-art efficiency must be provided while also showing an incremental increase in protection efficiency with an additional attachment of tools.

(iii) *Hybrid Deployment*: Users should be able to deploy in any operating system and utilise individual aspects of the platform according to their situational demand.

(iv) *Central management and reporting*: Each unique tool needs to be connected to a centralised administration plane that offers customisable role-based access control for various users, views, and functions.

(v) *Openness*: Ability to integrate with other supporting tools from diverse vendors.

(vi) *Cost:* The price of the platform.

Platform Options:
Four types of cybersecurity platform options were identified. These are:

1. *Cloud-Based Platforms*: administrators secure data in a third-party service's infrastructure, such as Cloud.
2. *Web-Based Platforms*: Protect networks and computer systems from targeted and general attacks on software, hardware, or data online.
3. *Application-Based Platforms*: Local security application that protects platform-installed devices.
4. *AI-Based Platforms*: Platforms powered by Artificial Intelligence

Selection Criteria:

Fifteen unique sub-criteria were identified for evaluation of the platform options. These are: 1. Central Visibility, 2. Native Integration, 3. Large Detection Spectrum, 4. Continuous Protection, 5. Insider Threat Protection, 6. Operating System Flexibility, 7. Remote Vendor Access, 8. Complete Privilege Control, 9. Localised Security, 10. Data Loss Prevention, 11. End Point Detection, 12. Real-time Protection, 13. Auto-updating of rules, 14. Security Authentication, 15. Accelerated protection.

We would like to elicit your opinion on selecting among the alternatives in the following sheets. The pairwise comparison scale (Table A1) expresses the importance of one option over the other.

Table A1
Saaty Comparison Scale [46, 71]

	Comparison Scale	*Assigned Numeric Values*
Option One	equally important as option Two	1
	is moderately more important than option Two	3
	is strongly more important than option Two	5
	is very strongly more important than option Two	7
	is extremely more important than option Two	9
For intermediate judgments (use even numbers)		2, 4, 6, 8

Annexure-A1: Sample Questionnaire (partly filled for explanations)

Given Options A and B, as shown below example, one can gauge the relative importance:
Choose the best and the worst criterion among the given. (Multiple "best and worst criteria" allowed)
If you think the option 'End-to-End Coverage' in column A is more important than 'Performance Capability' in column B, mark '5' on the right-hand side. If you think the option 'Hybrid Deployment' in column B is more important than the option 'End-to-End Coverage' in column A, mark '9' on the right-hand side.

Q1. Select the "best and worst criteria" among the main criteria.

Criteria	Selection
End-to-End Coverage	
Performance Capability	Best
Hybrid Deployment	
Central Managing and Reporting	Worst
Openness	
Cost	Best

Q.2. Rate the best criteria over the other criteria.

Criteria	Rating
End-to-End Coverage	3
Performance Capability	1
Hybrid Deployment	5
Central Managing and Reporting	9
Openness	7
Cost	1

Q.3. Rate the other criteria over the worst criteria.

Criteria	Rating
End-to-End Coverage	7
Performance Capability	9
Hybrid Deployment	5
Central Managing and Reporting	1
Openness	3
Cost	9

Q.4. Rate the Alternatives for the selection criteria.

Criteria	Cloud-Based	Web-Based	Application-Based	AI-Based
End Point Detection	9	1	7	4
Continuous Protection	2	6	4	5
Real-Time Protection	4	3	8	4
Data Loss Prevention	7	2	9	4

---- A part of the questionnaire explained ------

Annexure-A2 (Main Questionnaire)

Q1. Select the "best and worst criteria" among the main criteria.

Criteria	Selection
End-to-End Coverage	
Performance Capability	
Hybrid Deployment	
Central Managing and Reporting	
Openness	
Cost	

Q.1.1 Rate the best criteria over the other criteria.

Criteria	Rating
End-to-End Coverage	
Performance Capability	
Hybrid Deployment	
Central Managing and Reporting	
Openness	
Cost	

Q.1.2 Rate the other criteria over the worst criteria.

Criteria	Rating
End-to-End Coverage	
Performance Capability	
Hybrid Deployment	
Central Managing and Reporting	
Openness	
Cost	

Q.2 Select the "best and worst criteria" among the sub-criteria.

Criteria	Selection
End Point Detection	
Continuous Protection	
Real-Time Protection	

Q.2.1 Rate the best criteria over the other criteria.

Criteria	Rating
End Point Detection	
Continuous Protection	
Real-Time Protection	

Q.2.2 Rate the other criteria over the worst criteria.

Criteria	Rating
End Point Detection	
Continuous Protection	
Real-Time Protection	

Q.3 Select the "best and worst criteria" among the sub-criteria.

Criteria	Selection
Data Loss Prevention	
Auto-Updating of Rules	
Accelerated Protection	
Insider Threat Protection	
Large Detection Spectrum	
Localised Security	

Q.3.1 Rate the best criteria over the other criteria.

Criteria	Rating
Data Loss Prevention	
Auto-Updating of Rules	
Accelerated Protection	
Insider Threat Protection	
Large Detection Spectrum	
Localised Security	

Q.3.2 Rate the other criteria over the worst criteria.

Criteria	Rating
Data Loss Prevention	
Auto-Updating of Rules	
Accelerated Protection	
Insider Threat Protection	
Large Detection Spectrum	
Localised Security	

Q.4 Select the "best and worst criteria" among the sub-criteria.

Criteria	Selection
Operating System Flexibility	
Native Integration	

Q.4.1 Rate the best criteria over the other criteria.

Criteria	Rating
Operating System Flexibility	
Native Integration	

Q.4.2 Rate the other criteria over the worst criteria.

Criteria	Rating
Operating System Flexibility	
Native Integration	

Q.5 Select the "best and worst criteria" among the sub-criteria.

Criteria	Selection
Remote Vendor Access	
Central Visibility	
Security Authentication	
Complete Privilege Control	

Q.5.1 Rate the best criteria over the other criteria.

Criteria	Rating
Remote Vendor Access	
Central Visibility	
Security Authentication	
Complete Privilege Control	

Q.5.2 Rate the other criteria over the worst criteria.

Criteria	Rating
Remote Vendor Access	
Central Visibility	
Security Authentication	
Complete Privilege Control	

Q.6 Rate the Alternatives concerning the selection criteria

Criteria	Cloud-Based	Web-Based	Application-Based	AI-Based
End Point Detection				
Continuous Protection				
Real-Time Protection				
Data Loss Prevention				
Auto-updating of Rules				
Accelerated Protection				
Insider Threat Protection				
Large Detection Spectrum				
Localised Security				
Operating System Flexibility				
Native Integration				
Remote Vendor Access				
Central Visibility				
Security Authentication				
Complete Privilege Control				
Openness				
Cost				

---- End of the Questionnaire (16 questions in total) ------

References

[1] Kethineni, S. (2020). Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 305-326. https://doi.org/10.1007/978-3-319-78440-3_7

[2] Govt of India's Information Technology Act 2000 (IT Act 2000) (2000) https://en.wikipedia.org/wiki/ Information_Technology_Act,_2000 Accessed 10 October 2023.

[3] Govt of India's The National Crime Records Bureau (NCRB) (2013) https://ncrb.gov.in/en. Accessed 10 October 2023.

[4] Das, S. (2021, December). Adequacy and Limitations of the Information Technology Act in Addressing Cyber-Security Issues of Indian Power Systems. In 2021 9th IEEE International Conference on Power Systems (ICPS) (pp. 1-6). IEEE. https://doi.org/10.1109/ICPS52420.2021.9670395

[5] Kumar, V. A., Pandey, K. K., & Punia, D. K. (2014). Cyber security threats in the power sector: Need for a domain-specific regulatory framework in India. Energy policy, 65, 126-133. https://doi.org/10.1016/j.enpol.2013.10.025

[6] Govt of India's National Cyber Security Policy (2013). https://en.wikipedia.org/wiki/National_Cyber_Security Policy_2013. Accessed 10 October 2023.

[7] Kumar, G., (2019). Cyber Security System and Policy of India: Challenges and Prospects. Soc. Sci, 6(7), 1937-1943.

[8] Casanovas, M., & Aloys Nghiem, A., (2023 Aug). Cybersecurity – is the power system lagging behind? https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind. Accessed 10 October 2023.

[9] CEA (Cyber Security In Power Sector) Guidelines, 2021 (2022). https://npti.gov.in/cea-cyber-security-power-sector-guidelines-2021. Accessed 10 October 2023.

[10] Pingol, E. (2021). India Releases Cybersecurity Guidelines for Power Sector. https://www.trendmicro.com/en_us/research/21/j/india-releases-cybersecurity-guidelines-for-power-sector.html Accessed 11 October 2023.

[11] Palleti, V. R., Adepu, S., Mishra, V. K., & Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. Cybersecurity, 4(1), 1-19. https://doi.org/10.1186/s42400-021-00071-z

[12] Eduard Kovacs (2022, Nov). Cyberattack Causes Trains to Stop in Denmark. https://www.securityweek.com /cyberattack-causes-trains-stop-denmark. Accessed: 6 October 2023.

[13] Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analysing critical infrastructure interdependencies. IEEE control systems magazine, 21(6),11-25. https://doi.org/10.1109/37.969131

[14] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. International Journal of scientific research and management, 9(12), 669-710. https://doi.org/10.18535/ijsrm/v9i12.ec04

[15] Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in Industry, 114, 103165. https://doi.org/10.1016/j.compind.2019.103165

[16] Alp, Ö. (2018). Cybersecurity in Smart City. M. Sc. Thesis. İstanbul Bilgi University, Social Sciences Institute, İstanbul.

[17] Enayaty-Ahangar, F., Albert, L. A., & DuBois, E. (2020). A survey of optimisation models and methods for cyberinfrastructure security. IISE Transactions, 53(2), 182-198. https://doi.org/10.1080/24725854.2020.1781306

[18] Lopez, M. A., Lombardo, J. M., López, M., Alba, C. M., Velasco, S., Braojos, M. A., & Fuentes-García, M. (2020). Intelligent detection and recovery from cyberattacks for small and medium-sized enterprises. https://doi.org/10.9781/ijimai.2020.08.003

[19] Nayyar, S. (2022). What to look for in Machine Learning for Cybersecurity Solutions? https://www.forbes.com/sites/forbestechcouncil/2022/07/14/what-to-look-for-in-machine-learning-for-cyber security-solutions/?sh=d6129f1b21e5. Accessed 28 October 2023.

[20] Arce, D. G. (2020). Cybersecurity and platform competition in the Cloud. Computers & Security, 93, 101774. https://doi.org/10.1016/j.cose.2020.101774

[21] Sterlini, P., Massacci, F., Kadenko, N., Fiebig, T., & van Eeten, M. (2019). Governance challenges for European cybersecurity policies: Stakeholder views. IEEE Security & Privacy, 18(1), 46-54. https://doi.org/10.1109/MSEC.2019.2945309

[22] Dawson, M. (2018). Applying a holistic cybersecurity framework for global IT organisations. Business Information Review, 35(2), 60-67. https://doi.org/10.1177/0266382118773624

[23] Van Kranenburg, R., and Le Gars, G. (2021). The cybersecurity aspects of new entities need a cybernetic, holistic perspective. International Journal of Cyber Forensics and Advanced Threat Investigations, 2(1), 63-68. https://doi.org/10.46386/ijcfati.v2i1.36

[24] Yohanandhan, R. V., Elavarasan, R. M., Pugazhendhi, R., Premkumar, M., Mihet-Popa, L., & Terzija, V. (2021). A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid–

Part–II: Classification, overview and assessment of CPPS testbeds. International Journal of Electrical Power & Energy Systems, 107721. https://doi.org/10.1016/j.ijepes.2021.107721

[25] Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., & Mostarda, L. (2019). Cyber security threats detection in the Internet of Things using deep learning approach. IEEE Access, 7, 124379-124389. https://doi.org/10.1109/ACCESS.2019.2937326

[26] Atat, R., Liu, L., Wu, J., Li, G., Ye, C., Yang, Y. (2018). Big data meet cyber-physical systems: A panoramic survey. IEEE Access, 6, 73603-73636. https://doi.org/10.1109/ACCESS.2018.2878681

[27] Alamleh, A., Albahri, O. S., Zaidan, A. A., Alamoodi, A. H., Albahri, A. S., Zaidan, B. B., ... & Al-Samarraay, M. S. (2022). Multi-attribute Decision-Making for Intrusion Detection Systems: A Systematic Review. International Journal of Information Technology & Decision Making, 1-48. https://doi.org/10.1142/S021962202230004X

[28] Norem, S., Rice, A.E., Erwin, S., Bridges, R.A., Oesch, S., Weber, B. (2022). A Mathematical Framework for Evaluation of SOAR Tools with Limited Survey Data. In: Computer Security. ESORICS 2021 International Workshops. ESORICS 2021. Lecture Notes in Computer Science, 13106. Springer, Cham. https://doi.org/10.1007/978-3-030-95484-0_32

[29] Agrawal, A., Deep, V., Sharma, P., Mishra, S. (2021). Review of Cybersecurity Post-COVID-19. In: Kumar, N., Tibor, S., Sindhwani, R., Lee, J., Srivastava, P. (eds) Advances in Interdisciplinary Engineering. Lecture Notes in Mechanical Engineering. Springer, Singapore. https://doi.org/10.1007/978-981-15-9956-9_75

[30] Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers & Security, 105, 102258. https://doi.org/10.1016/j.cose.2021.102258

[31] Nugraha, I. P. E. D. (2021). A review of the role of modern SOC in cybersecurity operations. Int. J. Current Sci. Res. Rev., 4(5), 408-414. https://doi.org/10.47191/ijcsrr/V4-i5-13

[32] Skoumperdis, M., Vakakis, N., Diamantaki, M., Medentzidis, C. R., Karanassos, D., Ioannidis, D., & Tzovaras, D. (2023). A Novel Self-learning Cybersecurity System for Smart Grids. In Power Systems Cybersecurity: Methods, Concepts, and Best Practices (pp. 337-362). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-20360-2_14

[33] Gilchrist, A. (2016). Industry 4.0: the industrial Internet of things. Apress. Bangken, Nonthaburi, Thailand.

[34] Atoum, I., & Otoom, A. (2017). A classification scheme for cybersecurity models. International Journal of Security and Its Application, 11(1), 109-120. https://doi.org/10.14257/ijsia.2017.11.1.10

[35] Jansen, C., & Jeschke, S. (2018). Mitigating risks of digitalisation through managed industrial security services. AI & Society, 33(2), 163-173. https://doi.org/10.1007/s00146-018-0812-1

[36] Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, 103, 97-110. https://doi.org/10.1016/j.compind.2018.09.004

[37] Flatt, H., Schriegel, S., Jasperneite, J., Trsek, H., & Adamczyk, H. (2016, September). Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements. In 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA) (pp. 1-4). IEEE. https://doi.org/10.1109/ETFA.2016.7733634

[38] Januário, F., Carvalho, C., Cardoso, A., & Gil, P. (2016, October). Security challenges in SCADA systems over Wireless Sensor and Actuator Networks. In 2016 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT) (pp. 363-368). IEEE. https://doi.org/10.1109/ICUMT.2016.7765386

[39] He, H., Maple, C., Watson, T., Tiwari, A., Mehnen, J., Jin, Y., & Gabrys, B. (2016, July). The security challenges in the IoT enabled cyber-physical systems and opacities for evolutionary computing & other computational intelligence. In 2016 IEEE congress on evolutionary computation (CEC) (pp. 1015-1021). IEEE. https://doi.org/10.1109/CEC.2016.7743900

[40] Corbò, G., Foglietta, C., Palazzo, C., & Panzieri, S. (2018). Smart behavioural filter for industrial Internet of things. Mobile Networks and Applications, 23(4), 809-816. https://doi.org/10.1007/s11036-017-0882-1

[41] Jansen, C. (2017). Stabilising the industrial system: Managed security services' contribution to cyber-peace. IFAC-PapersOnLine, 50(1), 5155-5160. https://doi.org/10.1016/j.ifacol.2017.08.786

[42] Ren, A., Wu, D., Zhang, W., Terpenny, J., & Liu, P. (2017). Cyber security in smart manufacturing: Survey and challenges. In IIE Annual Conference. Proceedings (pp. 716-721). Institute of Industrial and Systems Engineers (IISE).

[43] Guo, S., & Zhao, H. (2017). Fuzzy best-worst multi-criteria decision-making method and its applications. Knowledge-Based Systems, 121, 23-31. https://doi.org/10.1016/j.knosys.2017.01.010

[44] Rezaei, J. (2016). Best-worst multi-criteria decision-making method: Some properties and a linear model. Omega, 64, 126-130. https://doi.org/10.1016/j.omega.2015.12.001

[45] Liu, S., Chan, F. T., & Ran, W. (2016). Decision-making for the selection of cloud vendor: An improved approach under group decision-making with integrated weights and objective/subjective attributes. Expert Systems with Applications, 55, 37-47. https://doi.org/10.1016/j.eswa.2016.01.059

[46] Mohammadi, M., & Rezaei, J. (2023). Ratio product model: A rank-preserving normalisation-agnostic multi-criteria decision-making method. Journal of Multi-Criteria Decision Analysis. https://doi.org/10.1002/mcda.1806

[47] Saaty, T.L. (1980), The Analytical Hierarchy Process, McGraw-Hill, New York, NY. https://doi.org/10.21236/ADA214804

[48] Saaty, T. L. (2004). Fundamentals of the analytic network process—Dependence and feedback in decision-making with a single network. Journal of Systems science and Systems engineering, 13, 129-157. https://doi.org/10.1007/s11518-006-0158-y

[49] Emrouznejad, A., & Marra, M. (2017). The state of the art development of AHP (1979-2017): A literature review with a social network analysis. International journal of production research, 55(22), 6653-6675. https://doi.org/10.1080/00207543.2017.1334976

[50] Ameli, M., Esfandabadi, Z.S., Sadeghi, S., Ranjbari, M., Zanetti, M. C. (2023). COVID-19 and Sustainable Development Goals (SDGs): Scenario analysis through fuzzy cognitive map modeling. Gondwana Research, 114, 138-155. https://doi.org/10.1016/j.gr.2021.12.014

[51] Yazdani, M., Pamucar, D., Erdmann, A., & Toro-Dupouy, L. (2023). Resilient, sustainable investment in digital education technology: A stakeholder-centric decision support model under uncertainty. Technological Forecasting and Social Change, 188, 122282. https://doi.org/10.1016/j.techfore.2022.122282

[52] Deveci, M., Pamucar, D., Gokasar, I., Delen, D., Wu, Q., & Simic, V. (2022). An analytics approach to decision alternative prioritisation for zero-emission zone logistics. Journal of Business Research, 146, 554-570. https://doi.org/10.1016/j.jbusres.2022.03.059

[53] Mou, Q., Xu, Z., & Liao, H. (2016). An intuitionistic fuzzy multiplicative best-worst method for multi-criteria group decision-making. Information Sciences, 374, 224-239. https://doi.org/10.1016/j.ins.2016.08.074

[54] Gupta, P., Anand, S., & Gupta, H. (2017). Developing a roadmap to overcome barriers to energy efficiency in buildings using best worst method. Sustainable Cities and Society, 31, 244-259. https://doi.org/10.1016/j.scs.2017.02.005

[55] Pamučar, D., Stević, Ž., & Sremac, S. (2018). A new model for determining weight coefficients of criteria in MCDM models: Full consistency method (FUCOM). Symmetry, 10(9), 393. https://doi.org/10.3390/sym10090393

[56] Wang, P., Wang, J., Wei, G., Wei, C., & Wei, Y. (2019). The multi-attributive border approximation area comparison (MABAC) for multiple attribute group decision making under 2-tuple linguistic neutrosophic environment. Informatica, 30(4), 799-818. https://doi.org/10.15388/Informatica.2019.230

[57] Hansen, P., & Ombler, F. (2008). A new method for scoring additive multi-attribute value models using pairwise rankings of alternatives. Journal of Multi-Criteria Decision Analysis, 15(3-4), 87-107. https://doi.org/10.1002/mcda.428

[58] Badi, I., & Ballem, M. (2018). Supplier selection using the rough BWM-MAIRCA model: A case study in pharmaceutical supplying in Libya. Decision Making: Applications in Management and Engineering, 1(2), 16-33. https://doi.org/10.31181/dmame1802016b

[59] Zhou, Y., Zheng, C., Zhou, L., & Chen, H. (2023). Selection of a solar water heater for large-scale group decision-making with hesitant fuzzy linguistic preference relations based on the best-worst method. Applied Intelligence, 53(4), 4462-4482. https://doi.org/10.1007/s10489-022-03688-w

[60] Krstić, M., Agnusdei, G. P., Miglietta, P. P., Tadić, S., & Roso, V. (2022). Applicability of Industry 4.0 Technologies in the Reverse Logistics: A Circular Economy Approach Based on COmprehensive Distance Based RAnking (COBRA) Method. Sustainability, 14(9), 5632. https://doi.org/10.3390/su14095632

[61] Department of Defense Chief Information Officer (2021). Cybersecurity Resource and Reference Guide. https://dodcio.defense.gov/Portals/0/Documents/Library/CSResourceReferenceGuide.pdf. Accessed 27 May 2023.

[62] Department of Defense Chief Information Officer (2022). Department of Defense Zero Trust Reference Architecture. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf. Accessed 28 April 2023.

[63] Cybersecurity and Infrastructure Security Agency. (2021). Commercial Facilities Sector: Cybersecurity Framework Implementation Guidance. https://www.cisa.gov/sites/default/files/publications/ Commercial_Facilities_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf. Accessed 27 April 2023.

[64] Center for Internet Security (CIS) (2023). Vendor Selection Criteria. https://www.cisecurity.org/services /cis-cybermarket/vendor-information/selection-criteria. Accessed 26 April 2023.

[65] Cybersecurity and Infrastructure Security Agency. (2023). Guide to Getting Started with a Cybersecurity Risk Assessment. https://www.cisa.gov/sites/default/files/2023-02/22_1201_safecom_guide_to_cyber security _risk_assessment_508-r1.pdf Accessed 27 April 2023.

[66] U.S. Office of Personnel Management. (2018). Interpretive Guidance for Cybersecurity Positions. https://www.opm.gov/policy-data-oversight/classification-qualifications/reference-materials/interpretive-guidance-for-cybersecurity-positions.pdf. Accessed 5 January 2023.

[67] Taherdoost, H. (2019). What is the best response scale for survey and questionnaire design; review of different lengths of rating scale/attitude scale/Likert scale. Hamed Taherdoost, 1-10.

[68] Likert, R. (1932). A technique for the measurement of attitudes. Archives of psychology, 140, 5-53.

[69] Petrudi, S. H. H., Ghomi, H., & Mazaheriasad, M. (2022). An Integrated Fuzzy Delphi and Best Worst Method (BWM) for performance measurement in higher education. Decision Analytics Journal, 4, 100121. https://doi.org/10.1016/j.dajour.2022.100121

[70] Khan, S. A., Gupta, H., Gunasekaran, A., Mubarik, M. S., & Lawal, J. (2023). A hybrid multi-criteria decision-making approach to evaluate interrelationships and impacts of supply chain performance factors on pharmaceutical industry. Journal of Multi-Criteria Decision Analysis, 30(1-2), 62-90. https://doi.org/10.1002/mcda.1800

[71] Wind, Y., & Saaty, T. L. (1980). Marketing applications of the analytic hierarchy process. Management Science, 26(7), 641-658. https://doi.org/10.1287/mnsc.26.7.641

[72] Pamučar, D., Ecer, F., Cirovic, G., & Arlasheedi, M. A. (2020). Application of improved best worst method (BWM) in real-world problems. Mathematics, 8(8), 1342. https://doi.org/10.3390/math8081342

[73] Lai, L. L., Zhang, H. T., Lai, C. S., Xu, F. Y., & Mishra, S. (2013, July). Investigation on july 2012 indian blackout. In 2013 International Conference on Machine Learning and Cybernetics (Vol. 1, pp. 92-97). IEEE. DOI: 10.1109/ICMLC.2013.6890450 https://doi.org/10.1109/ICMLC.2013.6890450

[74] Boeding, M., Boswell, K., Hempel, M., Sharif, H., Lopez Jr, J., & Perumalla, K. (2022). Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid. Energies, 15(22), 8692. https://doi.org/10.3390/en15228692

[75] ur Rehman, O., Ali, Y., & Sabir, M. (2022). Risk assessment and mitigation for electric power sectors: A developing country's perspective. International Journal of Critical Infrastructure Protection, 36, 100507. https://doi.org/10.1016/j.ijcip.2021.100507

[76] Jarmakiewicz, J., Parobczak, K., & Maślanka, K. (2017). Cybersecurity protection for power grid control infrastructures. International Journal of Critical Infrastructure Protection, 18, 20-33. https://doi.org/10.1016/j.ijcip.2017.07.002

[77] Randall, R. G., & Allen, S. (2021). Cybersecurity professionals information sharing sources and networks in the US electrical power industry. International Journal of Critical Infrastructure Protection, 34, 100454. https://doi.org/10.1016/j.ijcip.2021.100454

[78] Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. NIST special publication, 800(82), 1-16.

[79] Butwall, M., Ranka, P., & Shah, S. (2019). Python in the field of data science: a review. International Journal of Computer Applications, 178(49), 20-24. https://doi.org/10.5120/ijca2019919404

[80] Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. Cyber, Intelligence, and Security, 1(1), 103-119.

[81] Atkinson, J., Miorelli, S., & Ljungmark, C. (2022, April). Benefits of AI-Based Cybersecurity Tools for De-Manning Existing Offshore Platforms. In Offshore Technology Conference. OnePetro. https://doi.org/10.4043/31766-MS

[82] Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review. International Journal of Software Engineering & Applications (IJSEA), 13(5). https://doi.org/10.5121/ijsea.2022.13502

[83] Leszczyna, R., & Leszczyna, R. (2019). Cost of cybersecurity management. Cybersecurity in the Electricity Sector: Managing Critical Infrastructure, 127-147. https://doi.org/10.1007/978-3-030-19538-0_5