Application of Rank-Weight Methods to Blockchain Cybersecurity Vulnerability Assessment Framework

Sri Nikhil Gupta Gourisetti
Pacific Northwest National Laboratory
Richland, WA
srinikhil.gourisetti@pnnl.gov

Michael Mylrea
Pacific Northwest National Laboratory
Richland, WA
michael.mylrea@pnnl.gov

Hirak Patangia
University of Arkansas – Little Rock
Little Rock, AR
hcpatangia@ualr.edu

***Abstract*—Cybersecurity vulnerability assessment tools, frameworks, and methodologies are used to understand the cybersecurity maturity of a system or a facility. However, these tools are strictly developed based on standards defined by organizations such as the National Institute of Standards and Technology (NIST) and the U.S. Department of Energy; the majority of these tools and frameworks do not provide a platform to prioritize the requirements to reach a desired cybersecurity maturity. To address that challenge, we have been developing a framework and software application called cybersecurity vulnerability mitigation framework through empirical paradigm (CyFEr). CyFEr treats the problem at hand as a multi-criteria decision analysis (MCDA) problem, which requires that various criteria be weighed relatively. Defining those weights is non-trivial and often leads to subjective decisions leading to undesired complications. To facilitate such a weighting system in CyFEr, we evaluated the application of various rank-weight methods (such as rank sum, reciprocal rank, rank exponent, and rank order centroid). The efficacy of those rank-weight methods was evaluated by applying them and testing against the blockchain cybersecurity framework (BC2F). BC2F was developed using the NIST cybersecurity framework to evaluate the cybersecurity posture of the blockchain nodes and networks in a given blockchain application or use-case. This paper provides 1) technical insights on the application of rank-weight methods to cybersecurity vulnerability assessments, 2) an overview of BC2F, 3) the application of rank-weight methods to BC2F, and 4) a depiction of the integration of the discussed rank-weight methods in CyFEr.**

Keywords—cybersecurity vulnerability assessment, cybersecurity framework, blockchain cybersecurity, cyber risk mitigation, criteria ranking

I. Nomenclature

Symbol	Description
n	Total number of criteria. For CSF, $n=23$
i	A particular criterion, $i=1, 2, \ldots, n$. For CSF $i=1, 2, \ldots, 23$
r	Rank of a criterion i
p	Scaling exponent factor for rank exponent method
j	Criteria incrementor used in rank order centroid
α	Representative factor for a rank-weight method
RS	Rank sum
W_i^{RS}	Rank sum weight of criterion i
$W_{i\mid norm}^{RS}$	Normalized rank sum weight of criterion i
RR	Reciprocal rank
W_i^{RR}	Reciprocal rank weight of criterion i
$W_{i\mid norm}^{RR}$	Normalized reciprocal rank weight of criterion i
RE	Rank exponent
W_i^{RE}	Rank exponent weight of criterion i
$W_{i\mid norm}^{RE}$	Normalized rank exponent weight of criterion i
ROC	Rank order centroid
W_i^{ROC}	Rank order centroid weight of criterion i
$W_{i\mid norm}^{ROC}$	Normalized rank order centroid weight of criterion i

II. Introduction

Recognizing the need to address cybersecurity policy compliance challenges, researchers attempted to design various vulnerability assessment tools and methodologies [1]-[8]. Most of these methodologies tend to address challenges at the systems level. These methodologies are designed for specific applications such as the power grid, and they cannot be adopted towards other applications. It has been observed that frameworks such as the cybersecurity capability maturity model (C2M2) [5], NIST cybersecurity framework (CSF) [9], and risk management framework (RMF) [10] can provide a detailed cybersecurity analysis of a system, but they may not have an extended platform to provide mitigation plans. The core architectures of CSF and C2M2 are designed so that they can be adopted to any particular application that focuses primarily on cybersecurity policies. A major disadvantage with most of these methods is the lack of a way to provide implementable "next-steps" through a weighted criterion (organizational priorities) approach. These tools are efficient in identifying vulnerabilities, but only engage the user base to an extent to perform the assessment through and across various organizational teams such as information technology (IT) team, operational technology (OT) team, human resources (HR) team, etc. However, the tools were not designed with a mechanism to incorporate the priorities of the organization. Therefore, there is a risk of not obtaining a sequential quantified approach from these tools to mitigate the discovered vulnerabilities. Based on this risk, the ongoing research evaluates various aspects of CSF and C2M2 to develop a mitigation system called cybersecurity vulnerability mitigation framework through empirical paradigm (CyFEr). To achieve full maturity of CyFEr, a detailed interconnected rank-weight computation system is required. This system can be used to prioritize, rank, and weigh the criteria. This paper focuses on evaluating various rank-weight methods by applying them to a blockchain cybersecurity framework. Blockchain technology has been gaining a large amount of interest from various research and application areas [11]-[17]. To ensure secure use of this technology, evaluating the cybersecurity aspects associated with the blockchain technology is imperative. Therefore, this paper introduces a cybersecurity framework for blockchain and the proposed rank-weight methods that were tested on it.

III. Technical Background

In criteria-based decision-making calculations where various available criteria can be assigned with weights and priorities, the ranking can often tend towards being very

978-1-7281-0554-3/19/$31.00©2019 IEEE

subjective. Accurate quantitative decision-making calculations require validated datasets [18]. Availability of data has always been a major roadblock, both in cybersecurity and blockchain research areas. In similar data constrained scenarios, researchers often looked towards using various rank-weight methods [18]-[23]. Similar techniques have not been observed in the literature for cybersecurity vulnerability assessment areas. One of the many reasons may be the lack of condensed cybersecurity controls that can be adapted towards an application.

Any cybersecurity vulnerability assessment involves analyzing the system, network, or facility through a set of controls. Depending on the tool or framework used (e.g., C2M2, CSF, RMF), the total number of controls may range from 100 to over 500. Therefore, without a comprehensive list of prioritized criteria, it is almost impossible to estimate the ideal cybersecurity posture. This complexity leads us to the use of a multi-criteria decision analysis (MCDA). MCDA has gained a significant application efficacy-based reputation in transportation and the social sciences, among others [18]-[20] and [23]. In a typical MCDA problem, certain weights are assigned to a set of criteria and the weight is normalized to a scale of 1 or 100 before proceeding to the decision-making process. As noted in [21], this approach often adds another layer of complexity to an already complex problem. This is due to the ambiguity in answering certain questions, including how one assigns weights to the criteria and how one chooses a weight value for a criterion? Instead of assigning weights, if the decision-making processes is achieved through simply ranking the criteria, the problem is simplified. Beyond that, the computational algorithm would calculate the relative weights. There are various rank-weight calculation methods that have been rigorously analyzed and used [24]. Depending on the processes involved in decision making, some rank-weight methods may outperform others. So far, the application of rank-weight methods coupled with MCDA techniques to solve cybersecurity mitigation problems has not been observed. The following section will provide an overview of the rank-weight methods evaluated, while also introducing a use case that will be used to potentially facilitate a method to prioritize various criteria in a vulnerability assessment tool. This paper will also describe the formulation of various rank-weight methods along with its application in a cybersecurity vulnerability assessment.

IV. Rank-Weight Methods

A common feature across cybersecurity vulnerability assessment tools and methodologies is a clear division of controls across a range of domains and subdomains. For example, the cybersecurity framework coined by NIST is divided into five domains and 23 subdomains (see Fig. 1) and C2M2 is divided into 10 domains and about 30 subdomains. The focus of this paper will be to illustrate the differences between various rank-weight methods evaluated through a numerical problem. The four rank-weight methods that are promising in extending vulnerability assessment tools for a holistic gap analysis are: 1) rank sum, 2) reciprocal rank, 3) rank exponent, 4) rank order centroid.

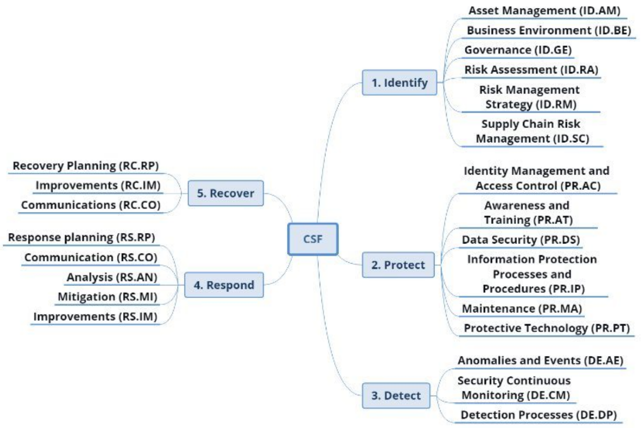
CSF
1. Identify
Asset Management (ID.AM)
Business Environment (ID.BE)
Governance (ID.GE)
Risk Assessment (ID.RA)
Risk Management Strategy (ID.RM)
Supply Chain Risk Management (ID.SC)
2. Protect
Identity Management and Access Control (PR.AC)
Awareness and Training (PR.AT)
Data Security (PR.DS)
Information Protection Processes and Procedures (PR.IP)
Maintenance (PR.MA)
Protective Technology (PR.PT)
3. Detect
Anomalies and Events (DE.AE)
Security Continuous Monitoring (DE.CM)
Detection Processes (DE.DP)
4. Respond
Response planning (RS.RP)
Communication (RS.CO)
Analysis (RS.AN)
Mitigation (RS.MI)
Improvements (RS.IM)
5. Recover
Recovery Planning (RC.RP)
Improvements (RC.IM)
Communications (RC.CO)

Fig. 1. Overview of Cybersecurity Framework domains and subdomains

A. Rank Sum

The rank sum (RS) [25] is defined as the following: for n number of criteria, the weight of criteria i of rank r is:

$$W_i^{RS} = n - r + 1 \tag{1}$$

The normalized weight of criteria i is calculated as:

$$W_{i|norm}^{RS} = \frac{W_i^{RS}}{\sum_{i=1}^{n} W_i^{RS}} = \frac{n-r+1}{\sum_{i=1}^{n} W_i^{RS}} \tag{2}$$

Equations (1) and (2) can also be written as:

$$W_i^{RS} = 2(n-r+1) \tag{3}$$

$$W_{i|norm}^{RS} = \frac{W_i^{RS}}{n(n+1)} = \frac{2(n-r+1)}{n(n+1)} \tag{4}$$

B. Reciprocal Rank

Reciprocal rank [25] is defined as the following: for n number of criteria, the weight of criteria i of rank r is:

$$W_i^{RR} = \frac{1}{r} \tag{5}$$

The normalized weight of criteria i is calculated as:

$$W_{i|norm}^{RR} = \frac{W_i^{RR}}{\sum_{i=1}^{n} W_i^{RR}} = \frac{\left(1/r\right)}{\sum_{i=1}^{n} W_i^{RR}} \tag{6}$$

C. Rank Exponent

Rank exponent [24] is defined as the following: for n number of criteria, the weight of criteria i of rank r is:

$$W_i^{RE} = \left(n-r+1\right)^p \tag{7}$$

where p is the controllability parameter to vary the weight distribution across criteria. Note that if the scaling exponent $p = 0$, weights of all criteria are equal; if $p = 1$, Equation (7) is exactly same as Equation (1), which will lead to a *rank sum* calculation. This relationship is shown in Equation (8):

$$W_i^{RE} = \begin{cases} \left(n-r+1\right)^p, & \forall p \in (0,1) \wedge (1,\infty) \Rightarrow \forall p \in (0,\infty) \,\&\, p \neq 0,1,\infty \\ 1 & if\ p=0 \\ Rank\ Sum & if\ p=1 \end{cases} \tag{8}$$

For this rank-weight method, the normalized weight of criteria i is calculated as:

$$W_{i|norm}^{RE} = \frac{W_i^{RE}}{\sum_{i=1}^{n} W_i^{RE}} = \frac{(n-r+1)^p}{\sum_{i=1}^{n} W_i^{RE}} \tag{9}$$

D. Rank Order Centroid

Rank order centroid [26] is defined as the following: for n number of criteria, the weight of criteria i of rank r is given by:

$$W_i^{ROC} = W_{i|norm}^{ROC} = \frac{1}{n}\sum_{j=i}^{n}\frac{1}{j} \tag{10}$$

The summation of normalized weights of all criteria is always equal to 1. Therefore, Equations (2), (4), (6), (9), and (10) will always abide by the following constraint:

$$\sum_{i=1}^{n} W_{i|norm}^{\alpha} = 1, \alpha \in \{RS, RR, RE, ROC\} \tag{11}$$

The normalized relative weights computed through Equations (1) – (11) are used later in the paper to identify the ideal solution(s) that will result in a desired cybersecurity posture. Later sections of this paper evaluate the application of those techniques to the cybersecurity vulnerability assessment tool with multiple attributes or criteria.

V. BlocKhain Cybersecurity Framework Definitions

The Blockchain Cybersecurity Framework (BC2F) will be used to demonstrate the proposed rank-weight methodology. BC2F is designed following the core cybersecurity framework designed by National Institute of Standards and Technology (NIST) [9]. The objective of BC2F is to evaluate the cybersecurity of the environment (or node) that is going to be part of a blockchain application. The output of BC2F highlights cybersecurity gaps and vulnerabilities to be addressed to ensure that cybersecure transactions are executed across the blockchain platform. BC2F also has a mathematical mitigation system that recommends the targeted cybersecurity posture based on the user requirements. This mitigation system has various elements such as rank-weight analysis, multi-tier solution discovery, prioritized gap analysis, and maturity determination based on a weighted performance score. This paper introduces the BC2F by defining all the domains and subdomains and exploring the application of rank-weight methods. All of the other elements of the mitigation system are beyond the scope of this paper and will be discussed in future publications. Since BC2F is inherited from NIST CSF, the core domains and subdomains remained unchanged, and the 23 subdomains from BCF are used as the attributes or criteria. Therefore, the decision maker should rank these subdomains (otherwise referred to as criteria) in a prioritized order. Fig. 1 shows the nomenclature of domains and subdomains. Also, listed below are definitions of BC2F domains and subdomains.

1. Identify–Asset Management (ID.AM): This criterion addresses aspects such as the ability to catalog the blockchain nodes and inventory of the blockchain assets (e.g., physical devices and systems, smart contracts). Architectural elements of this criteria include:
   a. Identification and mapping of data flows across various nodes during the transactional processes.
   b. Prioritization of blockchain nodes based on their involvement, criticality, and value added to the blockchain, and their frequency of transactions.

   Addressing the above elements should lead to the establishment of cybersecurity roles and responsibilities for the blockchain nodes (e.g., reader, writer, validator, trusted third party, etc.).
2. Identify–Business Environment (ID.BE): This criterion addresses aspects such as the identification of roles for the blockchain nodes; their importance and criticality in the network participation; and prioritization of blockchain purpose, objectives, and activities. Effective communication of all this information would act as a prerequisite to the following:
   a. Establishment of dependencies and critical functions for successful operation of the blockchain.
   b. Establishment of blockchain resilience requirements to support cyber secure peer-to-peer transactions and execution of smart contracts.
3. Identify–Governance (ID.GV): This criterion addresses aspects such as awareness of security policy in the blockchain network and surveillance for fraudulent activities. This could potentially lead to the following:
   a. Coordination and alignment of security roles and responsibilities for all the participating nodes and the associated IT/OT infrastructure.
   b. Understanding and management of blockchain legal and regulatory requirements for cyber secure peer-to-peer transactions, privacy, and obligations of the participating nodes.

   The above elements would assist in evaluating governance and risk management processes that can potentially address the cybersecurity risks posed to the blockchain nodes (and on the blockchain network).
4. Identify–Risk Assessment (ID.RA): This criterion addresses aspects such as obtaining threat and vulnerability information from information sharing sources to facilitate implementation of the following:
   a. Identification, documentation, and assessment of the blockchain vulnerabilities using a cyber secure risk assessment process.
   b. Identification and documentation of internal and external threats.
   c. Identification and documentation of threats and vulnerabilities to assist in determining potential business impacts and the likelihood of attacks.
   d. Obtaining information about identified threats, vulnerabilities, likelihoods, and business impacts and utilizing that information to determine possible risks to blockchain nodes and their transactions.

   Using the above information, responses to the possible risks can be identified and prioritized.
5. Identify–Risk Management Strategy (RM): This criterion addresses aspects such as the management and

agreement of established risk management processes by the list of validators (otherwise known as authority nodes) and the blockchain nodes to determine risk tolerance with respect to the blockchain (authority nodes are present only in proof-of-authority. Consensus models such as proof-of-work do not have authority nodes. In such cases, all nodes may be treated with equal authority). Determination of risk tolerance could potentially enable the blockchain nodes to be aware of its criticality and importance. This information can be used to determine if the nodes are required to meet the objectives of a security program or cybersecurity risk management plan associated with their contracts.

6. Identify–Supply Chain and Risk Management (ID.SC): This criterion addresses the following aspects:
   a. Assessment, management, and agreement of identified and established supply chain risk management processes by the authority nodes.
   b. Testing of response and recovery planning with the blockchain vendor and blockchain participants could lead to identification, prioritization, and assessment of the critical information about the suppliers and partners in the supply chain process using a cyber supply chain risk assessment process.
   c. The ability to obtain critical information about the suppliers and partners in order to test response and recovery plans with them. This can determine if the suppliers and partners are required to meet the objectives of the security program or cyber secure risk management plan defined by contract. Once the decision is made, the suppliers and partners could be monitored to verify if the objectives are met.
7. Protect–Identity Management and Access Control (PR.AC): This criterion addresses the following:
   a. Management of identities and credentials for authorized blockchain nodes and network integrity protection by incorporating network segregation (as required) to enable management of the physical and remote access to the assets in the blockchain network (this includes the blockchain nodes and other assets that are on the same network).
   b. Verification of identities of the operating *human* participants in the blockchain by asserting the issued credentials in appropriate interactions. Verification of identities would assist in the access permissions, management and authorizations by incorporating the least privilege principle and separation of duties to facilitate access controls.
8. Protect–Awareness and Training (PR.AT): This criterion addresses the following aspects:
   a. Understanding of cybersecurity roles and responsibilities by the physical and information security personnel to perform periodic evaluations of the blockchain nodes (including the list of validators or authority nodes).
   b. Periodic inspection of the blockchain users, supplier/manufacturer, and associated partners to assess their awareness of roles and responsibilities.
9. Protect–Data Security (PR.DS): Implementing data leak protection would ensure that both data-at-rest and data-in-transit are protected. This criterion addresses aspects such as formal management of blockchain nodes and users throughout the process of removal, transfers, and disposition. This facilitates availability maintenance in the blockchain. Data leak protection and management of assets can also incorporate integrity verification.
10. Protect–Information Protection Processes and Procedures (PR.IP): Sharing effectiveness of protection technologies with users would allow them to verify:
    a. Creation and maintenance of the baseline configuration of blockchain network systems to incorporate security principles and validate:
       i. Use of system development life cycle (SDLC) to manage assets participating in blockchain
       ii. Appropriate placement of configuration change control processes
       iii. The process of maintenance and periodic testing of blockchain asset data backups.
    b. Whether policy and regulations are met while deploying physical systems in the blockchain.

    Policy and regulations regarding the blockchain nodes, maintenance, and periodic testing of information backups would ensure that data is maintained according to the established policy. Baseline configuration of the blockchain network systems, backups of the asset information, testing response and recovery plans, and development and implementation of vulnerability management plans will result in the establishment of strong protection processes.
11. Protect–Maintenance (PR.MA): This criterion addresses aspects such as periodic *preventive* maintenance of blockchain nodes (and networks) to prevent events such as unauthorized access.
12. Protect–Protective Technology (PR.PT): Protection of the blockchain assets and network would require:
    a. Protection and restrictive use of removable media according to established policies.
    b. Incorporation of the least functionality/privilege principle to the blockchain users by providing only essential capabilities.
    c. Operation of all the blockchain nodes in predefined functional states (e.g., under duress, under attack, during recovery, normal operations) to achieve availability.
    d. Determination, documentation, implementation, and review of audit and log records of all the blockchain nodes according to established policies.

    Implementation of the above processes can potentially catch and regulate cyberattacks that target the wallet, nodes, and the transactions.
13. Detect–Anomalies and Events (DE.AE): This criterion addresses aspects such as the establishment and management of expected data flows and baselines across the blockchain network among the participating nodes. This could potentially assist in analyzing detected blockchain cyber events. This could also possibly result in gaining total understanding of the

cyber-attack targets and methods. Data acquired from the analysis of detected cyber events can also be aggregated and correlated from multiple sources. Finally, impact determination of detected events on the blockchain can assist in the establishment of a threshold for cyber incident alert.

14. Detect–Security Continuous Monitoring (DE.CM): Monitoring the blockchain network and nodes include:
    a. Monitoring of individual operations/activities performed by the participating nodes to
        i. detect malicious code for smart contracts
        ii. detect unauthorized mobile code.
    b. Monitoring for unauthorized nodes and unauthorized access attempts.
15. Detect–Detection Processes (DE.DP): This criterion addresses aspects such as testing and evaluating the blockchain nodes according to organization compliance requirements. Furthermore, this criterion also highlights the importance and implementation of various detection processes. Some of the high-level elements include:
    a. Effective communication of the cyber event detection information to appropriate participating nodes. This can lead to ensuring accountability by defining the roles and responsibilities to delineate, differentiate, and ultimately detect a cyber event in the blockchain environment.
    b. Continuous improvement of detection processes
16. Respond–Response Planning (RE.RP): This criterion addresses aspects such as determining if a well-designed response plan is in place that incorporates blockchain nodes, associated data, smart contracts, participant identity, and the validity of the transactions.
17. Respond–Communications (RE.CO): This criterion addresses aspects such as consistency of reported events with established criteria. Some of the elements include:
    a. Consistency of shared information with all the blockchain nodes along with the response plans.
    b. Evaluation and implementation of processes to voluntarily share the information with the blockchain nodes to achieve broader cybersecurity situational awareness.

    The above elements can facilitate the coordination among the blockchain nodes (especially among the list of validators or authority nodes) and stay consistent with the incident response plans.
18. Respond–Analysis (RE.AN): This criterion addresses aspects such as investigation of detected anomalies in the blockchain network. This includes verification of consistency in established incident categorization with the response plans. Consistency in incident categorization can assist in understanding impacts of cybersecurity events and in performing cyber forensics.
19. Respond–Mitigation (RE.MI): This criterion addresses aspects such as containment of the incidents detected in the blockchain network and availability of the necessary amount of time to mitigate events. This criterion also emphasizes documentation of the vulnerabilities and updating the list of accepted risks and response plans.
20. Respond–Improvements (RE.IM): This criterion addresses aspects such as periodically update response strategies to incorporate the lessons learned.
21. Recover–Recovery Planning (RC.RP): This criterion addresses aspects such as determining if a well-designed recovery plan is in place to recover the blockchain nodes and network. Test the smart contract executions for consistency and behavior checks.
22. Recover–Improvements (RC.IM): This criterion addresses aspects such as periodically update recovery strategies to incorporate lessons learned.
23. Recover–Communications (RC.CO): This criterion addresses aspects such as management of relations with associated entities in the blockchain through effective communication of recovery activities. This can expedite the repair of reputation after an incident.

VI. Illustrative Application of Rank-Weights to BC2F

With the understanding and evaluation of the blockchain cybersecurity framework, this section demonstrates the application of the rank-weight methods discussed in previous sections to BC2F. Table – 1 (see Fig. 1 for descriptions of the abbreviations in column-1) shows the criteria, illustrated ranks, and the relative weights computed based on the given ranks. Note that the controllability parameter *p* for the *rank exponent* method is assumed to be "2". Fig. 2 shows a comparative evaluation between the calculated weights through the four rank-weight methods. It is important to note that the use of a particular method may depend on the purpose of the intended analysis (e.g., connecting the results to a financial investment decision, developing a risk calculation model, etc.). It is evident from Fig. 2 that the weight distribution pattern is fairly similar in all the methods across all criteria except for the criterion that is ranked as 1 (the most important criterion). This difference may be significant depending on the use of this data. For example, if a decision is to be made to allocate resources based on these weights, through the *reciprocal rank* approach, the highest ranked criteria (rank = 1) demands over 25% of overall resources. Therefore, one of the discussed rank-weights methods should be used based on the extended application requirements.

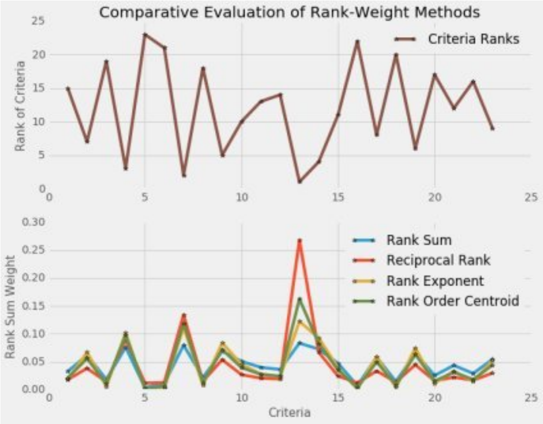

Fig. 2. Comparative Summary of all the Rank-Weight methods

Table 1. Criteria, Illustrated Ranks, and Calculated Weights

Criteria	**Rank**	$W_{i\|norm}^{RS}$	$W_{i\|norm}^{RR}$	$W_{i\|norm}^{RE}$	$W_{i\|norm}^{ROC}$
ID.AM	15	0.0326	0.0179	0.0187	0.021

ID.BE	7	0.0616	0.0383	0.0668	0.0558
ID.GV	19	0.0181	0.0141	0.0058	0.0104
ID.RA	3	0.0761	0.0893	0.102	0.0971
ID.RM	23	0.0036	0.0116	0.0002	0.0019
ID.SC	21	0.0109	0.0128	0.0021	0.0059
PR.AC	2	0.0797	0.1339	0.1119	0.1189
PR.AT	18	0.0217	0.0149	0.0083	0.0128
PR.DS	5	0.0688	0.0536	0.0835	0.0718
PR.IP	10	0.0507	0.0268	0.0453	0.0394
PR.MA	13	0.0399	0.0206	0.028	0.0274
PR.PT	14	0.0362	0.0191	0.0231	0.0241
DE.AE	1	0.0833	0.2678	0.1223	0.1624
DE.CM	4	0.0725	0.0669	0.0925	0.0827
DE.DP	11	0.0471	0.0243	0.0391	0.035
RS.RP	22	0.0072	0.0122	0.0009	0.0039
RS.CO	8	0.058	0.0335	0.0592	0.0496
RS.AN	20	0.0145	0.0134	0.0037	0.0081
RS.MI	6	0.0652	0.0446	0.0749	0.0631
RS.IM	17	0.0254	0.0158	0.0113	0.0154
RC.RP	12	0.0435	0.0223	0.0333	0.0311
RC.IM	16	0.029	0.0167	0.0148	0.0181
RC.CO	9	0.0543	0.0298	0.052	0.0442

A comparative analysis of the data from Table – 1 are depicted on polar plots shown in Fig. 3 to Fig. 12. Note that the x-axis in Fig. 3 to Fig. 12 is the range of ranks and weights, the y-axis shows the sub-domains or criteria.

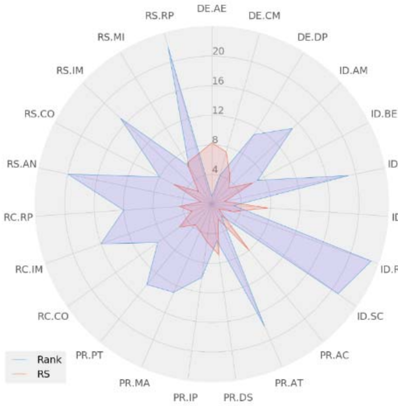

Fig. 3. Rank vs Rank Sum Weights

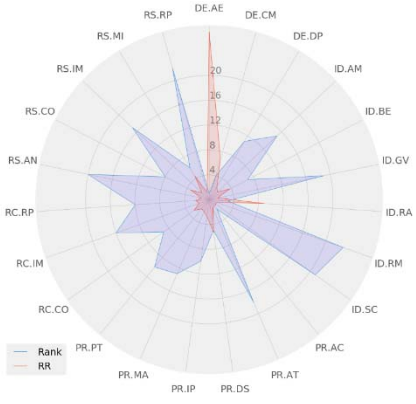

Fig. 4. Rank vs Reciprocal Rank Weights

It is evident from Fig. 3 to Fig. 6 that the behavioral variations of the weights acquired from all the rank-weight methods are consistent with the ranks. Note that for the legibility purposes, column 3–6 (indicates the rank-weights) of Table 1 are scaled by multiplying them with 100. An interesting and significant observation is that there is a noteworthy emphasis on the top-ranking criterion (rank = 1) in the reciprocal rank method. Weight distribution is very balanced in the RS, followed by RE, and ROC methods.

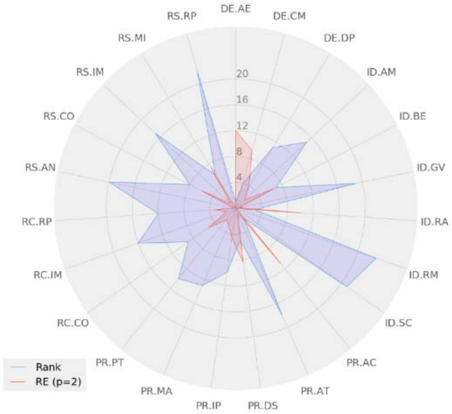

Fig. 5. Rank vs Rank Exponent (p=2) Weights

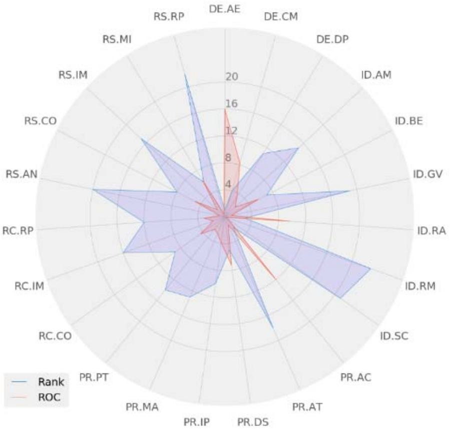

Fig. 6. Rank vs Rank Order Centroid Weights

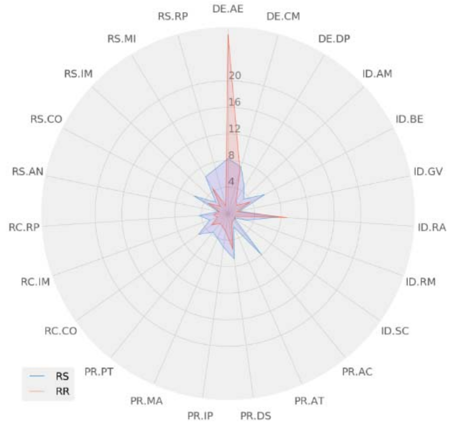

Fig. 7. Rank Sum vs Reciprocal Rank Weights

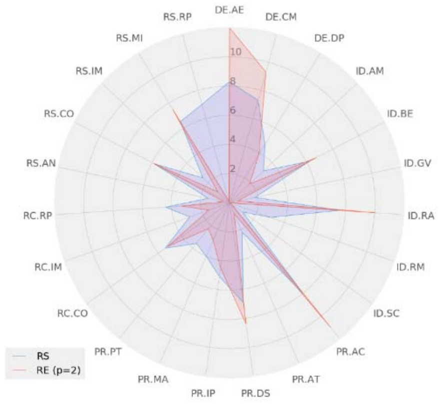

Fig. 8. Rank Sum vs Rank Exponent (p=2) Weights

Another observation is that the rank distribution pattern is almost exactly the same in the RE and ROC methods, but shows a slight difference in the magnitude (see Fig. 5, Fig. 6, and Fig. 12). Equations (1) and (7) indicate that the RS and RE are expected to be the same (if p = 1, RE = RE), but an interesting inference is that the RE pattern is closer to the ROC pattern. It may be quite possible to acquire very close weights between the RE and ROC if the value of p is adjusted. A detailed comparative analysis between the four rank-weight methods is shown in Fig. 7 to Fig. 12.

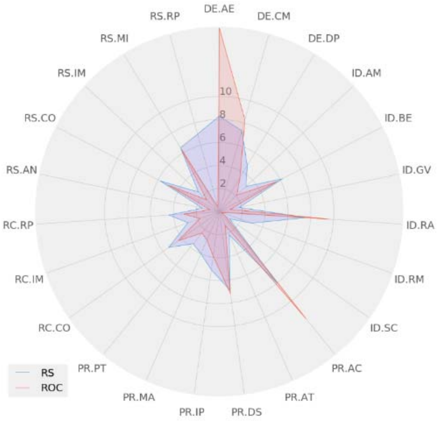

Fig. 9. Rank Sum vs Rank Order Centroid Weights

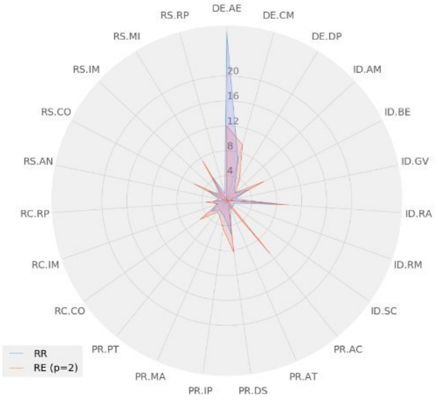

Fig. 10. Reciprocal Rank vs Rank Exponent (p=2) Weights

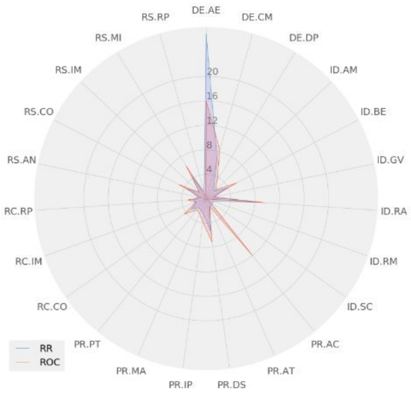

Fig. 11. Reciprocal Rank vs Rank Order Centroid Weights

Lastly, the boxplot shown in Fig. 13 indicate that for the given rank distribution (rank 1 to rank 23), the RS weight distribution is very balanced, the RR is tightly distributed (except for the criteria with rank = 1), the RE and ROC weights are distributed around close magnitudes. To further evaluate the behavior of the RE method, the value of *p* was varied; it can be seen from Fig. 14 that the weight distribution changes significantly. Therefore, choosing the *p* value is critical with the RE method. Overall, each of the methods has advantages and disadvantages. Ultimately, specific application requirements will determine the type of rank-weight method to be used.

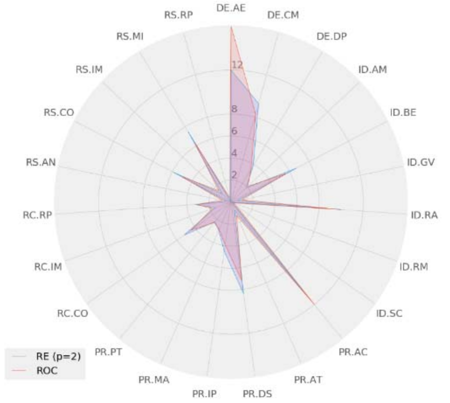

Fig. 12. Rank Exponent (p=2) vs Rank Order Centroid Weights

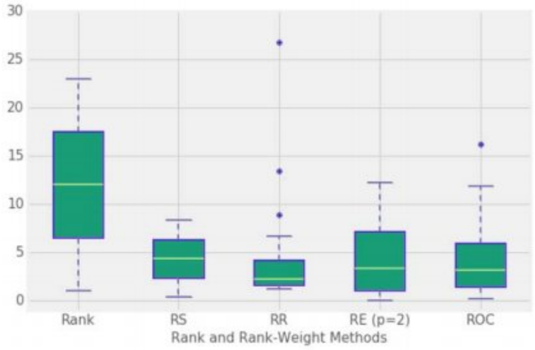

Fig. 13. Boxplot representation of ranks vs rank-weight methods

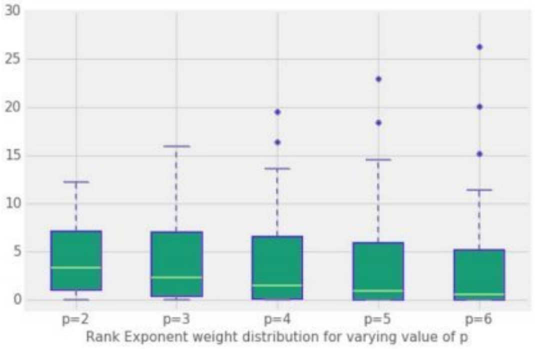

Fig. 14. Comparison of Rank Exponent weights for varying *p*

VII. Future Work and Conclusion

The paper presented the use of various rank-weight methods to use in the enhancement of cybersecurity vulnerability assessments. Since assigning weight to a criterion relative to the remaining criteria is a non-trivial task, the use of rank-weight methods simplifies the process significantly. This paper also demonstrated the differences between discussed rank-weight methods by applying them to a blockchain cybersecurity framework. The use of rank-weight methods is advantageous to solve a multi-criteria decision analysis (MCDA) problem such as the presented BC2F methodology: 1) rank-weight methods eliminate the need to define weights across a potentially non-relatively large spectrum of criteria. Defining criteria weights is often non-trivial and becomes very subjective. Using the rank-weight methods, the criticality of criteria can be captured while avoid the risk of extensive subjective analysis; 2) the outcome of rank-weight methods can be fed into decision-making algorithms that can ingest the translated weights (from the assigned ranks) for complex analysis such as criteria-based resource allocation, prioritized vulnerability mitigation, and periodic quantitative cybersecurity maturity analysis; 3) rank-weight methods are not complicated. They have been used and tested in other research areas such as logistics, transportation, systems engineering, etc. Therefore, the presented rank-weight methods have been well-vetted by researchers and engineers. Despite the above advantages, rank-weight methods have some disadvantages that need to be addressed with further research: 1) they are not highly used in cybersecurity vulnerability analysis. Therefore, further vetting and rigorous testing is required to demonstrate their efficacy; 2) although rank-weight methods eliminate significant amount of subjective decision-making processes, they still require some level of subjective analysis at the initial stages; 3) since all the presented rank-weight methods have similar behavioral patterns, deciding upon the method to choose can be a delicate decision to make.

With the tests performed and the results depicted in this paper, ongoing and future work has been focusing on integrating these methods into the CyFEr framework and software application. Some of the future work will also focus on addressing the disadvantages discussed in the previous paragraph. The objective of CyFEr is to understand user requirements and identify the target cybersecurity maturity state, which may also be viewed as the ideal state. Future publications will provide details about the individual elements of the CyFEr framework and software applications along with its application in cybersecurity vulnerability assessment tools and methodologies. Fig. 15 shows a fragment of the CyFEr framework, highlighting the integration & working mechanism of rank-weight methods.

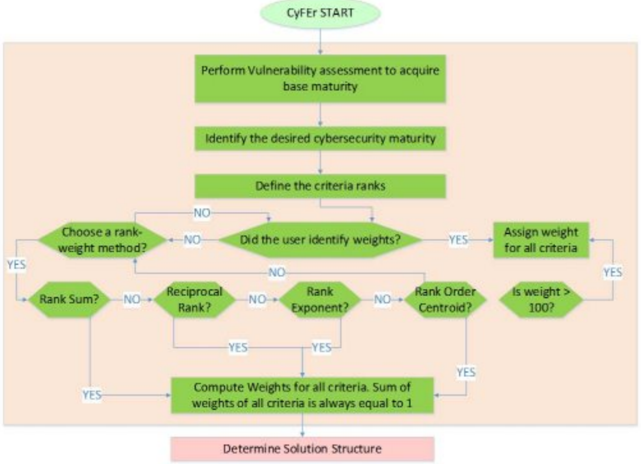
CyFEr START
Perform Vulnerability assessment to acquire base maturity
Identify the desired cybersecurity maturity
Define the criteria ranks
NO
Choose a rank-weight method?
NO
Did the user identify weights?
YES
Assign weight for all criteria
YES
NO
YES
Rank Sum?
NO
Reciprocal Rank?
NO
Rank Exponent?
NO
Rank Order Centroid?
Is weight > 100?
YES
YES
YES
YES
Compute Weights for all criteria. Sum of weights of all criteria is always equal to 1
Determine Solution Structure

Fig. 15. Depiction of rank-weight integration in CyFEr framework

VIII. References

[1] M. Mylrea, S. Gourisetti, C. Larimer and C. Noonan, "Insider Threat Cybersecurity Framework Webtool & Methodology: Defending Against Complex Cyber-Physical Threats," in WRIT, USA, 2018.

[2] S. Gourisetti, et al, "Multi-Scenario Use Case based Demonstration of Buildings Cybersecurity Framework Webtool," IEEE Symposium on Computational Intelligence Applications in Smart Grid, 2017.

[3] M. Mylrea, et al, "An Introduction to Buildings Cybersecurity Framework (BCF)," in IEEE Symposium on Computational Intelligence Applications in Smart Grid, USA, 2017.

[4] M. Mylrea and S. Gourisetti, "Cybersecurity and Optimization in Smart “Autonomous” Buildings," in Autonomy and Artificial Intelligence: A Threat or Savior?, Springer, 2017, pp. 263-294.

[5] C. Glantz, et al, "Evaluating the Maturity of Cybersecurity Programs for Building Control Systems," Technical Report, PNNL, 2016.

[6] C. Ten, et al, "Cybersecurity for Critical infrastructures: Attack and Defense Modeling," IEEE Trans. on Sys., MAN, and Cybernetics: Part A: Systems and Humans, vol. 40, no. 4, pp. 853-865, 2010.

[7] C. Ten, C. Liu and M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees," in IEEE Power Engineering Society General Meeting, USA, 2007.

[8] C. Ten, C. Liu and M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems," IEEE Transactions on Power Systems, vol. 23, no. 4, pp. 1836-1846, 2008.

[9] NIST, "Framework for Improving Critical Infrastructure Cybersecurity V1.1," NIST, 2018.

[10] NIST, "Risk Management Framework," NIST, 2018.

[11] A. Hahn, et al, "Smart contract-based campus demonstration of decentralized transactive energy auctions," IEEE PES Innovative Smart Grid Technologies Conference, Washington, DC, 2017.

[12] A. Laszka, et al, "Providing privacy, safety, and security in IoT-based transactive energy systems using distributed ledgers," Intl. Conference on the Internet of Things, Linz, Austria, 2017.

[13] M. Mylrea et al, "Blockchain Keyless Signature Infrastructure: Facilitating NERC CIP Compliance and Responding to Evolving Cyber Threats and Vulnerabilities to Energy Infrastructure," IEEE/PES T&D Conference and Exposition, USA, 2018.

[14] M. Mylrea and S. Gourisetti, "Blockchain for Smart Grid Resilience: Exchanging Distributed Energy at Speed, Scale and Security," in IEEE Resilience Week, USA, 2017.

[15] M. Mylrea et al, "Blockchain for Supply Chain Cybersecurity, Optimization, and Compliance," Resilience Week, Denver, 2018.

[16] M. Mylrea et al, "Blockchain: A Path to Grid Modernization and Cyber Resiliency," North American Power Symposium, USA, 2017.

[17] M. Mylrea et al, "Blockchain: Next Generation Supply Chain Security for Energy Infrastructure and NERC Critical Infrastructure Protection (CIP) Compliance," Resilience Week, USA, 2018.

[18] W. Edwards, "How to Use Multiattribute Utility Measurement for Social Decisionmaking," IEEE Transactions on Systems, MAN, and Cybernetics, vol. 7, no. 5, pp. 326-340, 1977.

[19] M. Barfod et al, “Multi-criteria decision analysis for use in transport decision making”, Denmark: DTU Lyngby, 2014.

[20] F. Barron and B. Barrett, "The efficacy of SMARTER - Simple Multi-Attribute Rating Technique Extended to Ranking," Elsevier Acta Psychologica, vol. 93, pp. 23-36, 1996.

[21] R. Roberts and P. Goodwin, "Weight Approximations in Multi-attribute Decision Models," Journal of Multi-Criteria Decision Analysis, vol. 11, pp. 291-303, 2002.

[22] A. Filho, T. Clemente, D. Morais and A. Almedia, "Preference modeling experiments with surrogate weighting procedures for the PROMETHEE method," European Hournal of Operational Research, vol. 264, no. 2, pp. 453-461, 2018.

[23] H. Chi and V. Yu, "Ranking generalized fuzzy numbers based on centroid and rank index," Elsevier Journal on Applied Soft Computing, vol. 68, pp. 283-292, 2018.

[24] GITTA, "Geographical Information Technology Training Alliance," Nov 2013. [Online]. Available: http://www.gitta.info/Suitability /en/html/Normalisatio_learningObject1.html. [Accessed Jan 2018].

[25] W. G. Stillwell, et al, "A comparison of weight approximation techniques in multiattribute utility decision making," Organizational Behavior and Human Performance, pp. 62-77, 1981.

[26] F. H. Barron, "Selecting a best multiattribute alternative with partial information about attribute weights," Acta Psychologica, 1992.