A Weighting Model of Cybersecurity Parameters Used for Service Placement

https://doi.org/10.3991/ijoe.v19i07.39285

Luan Gashi[1(✉)], Artan Luma[1], Marika Apostolova[1], Ylber Januzaj[2]
[1]South East European University, Tetovo, N. Macedonia
[2]University of Business "Haxhi Zeka", Peja, Kosovo
lg29758@seeu.edu.mk

Abstract—Most cybersecurity frameworks are based on three major components such as confidentiality, integrity, and availability. All these components have their parameters that are used to secure network nodes. But finding the most cyber secure node in a network needs a measurement method. The aim of the paper is to offer a model that can be used to find the most secure network nodes considering these cybersecurity components and their parameters. This is achieved by modelling numeric values of respective weights for parameters of confidentiality, integrity, and availability. The model is applied to a simulated environment where random values standing for cybersecurity parameters are given to 30 wireless network nodes that are used as an example. Then the weighted values are processed with Python programming language by giving the most secure nodes according to needed cybersecurity components. This model can be used to recommend the right network node that can be used to deploy services securely while avoiding potential vulnerabilities and cyber-attacks.

Keywords—cybersecurity parameters, service placement, security measurements, clustering

1 Introduction

Nowadays, cybersecurity has become one of the most concerns regarding information systems. The challenge of having a secure node within a wireless communication network, where a service would take place in a secure manner, requires updated treatment according to technological developments and modern threads. Accordingly, researchers are contributing with their studies to mitigate the issue of cybersecurity vulnerabilities by proposing different technology utilizations like the blockchain [1] or enhancing different algorithms of machine learning and deep learning methods ensuring all data remain secure and solve the cybersecurity problems [2, 3].

In addition, except rapid and reliable way of developing cybersecurity teaching and learning courses [4], there are several frameworks which defines and treat the cybersecurity like the Information Systems Audit and Control Association (ISACA), the National Institute of Standards and Technology (NIST), and the International Organization for Standardization (ISO) and the International Electrotechnical Commission

(ISO/IEC) 27001 standard series, commonly through the CIA triad components [5, 6, 7]. The CIA triad consists of three components which include confidentiality, integrity, and availability. These components and their respective parameters are the fundamentals of cybersecurity. Because values of such cybersecurity parameters are not numerical values, it is difficult to measure them, so they need to be more deeply analyzed to find specific values which present the weight of CIA triad components. This gives the crucial possibility of placing a network service to a secure network node according to cybersecurity requirements. By being based on a cybersecurity comprehensive study, it is shown that the CIA triad is the sufficient framework about cybersecurity at wireless networks, since it is proved that all other cybersecurity attributes used by the authors belong to the components of CIA triad such as confidentiality, integrity, and availability [8]. Furthermore, an interesting and motivated approach on service placement is that of using the state of the underlying community networks to optimize service deployment where a new placement heuristic based on bandwidth and availability is used to deploy the service [9].

Since there is commonly to find performance measurement models about network nodes or different technology utilizations, the aim of this paper is to offer a distinctive model which provides the weight of parameters used in CIA triad components that would make possible finding the network node which fulfils the cybersecurity requirements for service placement. To fulfil this task, firstly in the next section, the respective parameters of confidentiality, integrity and availability are defined. Section 3 deals with proposed model, where the used method of making the defined parameters numerically weighable is shown. This allows the possibility of applying selective techniques for specific network nodes presented at Section 4 as an example of application of the proposed model, while Section 5 summarizes the findings and concludes the paper.

2 Parameters of confidentiality, integrity and availability

According to NIST, the CIA triad stands for three pillars of information security. These pillars, as mentioned earlier, include confidentiality, integrity, and availability. This statement is followed by other institutions such as the European Union Agency for Cybersecurity (ENISA) as well [10]. It is also used as a baseline guide by many cybersecurity providers such as SecurityScorecard, Fortinet, F5, Kobalt and many others [11–13].

2.1 Confidentiality parameters

Confidentiality is keeping authorized restrictions on information access and disclosures in place, including safeguards for personal privacy and proprietary information [14], [15]. According to this, confidentiality is covered by the Access Control parameters which consists of mandatory, discretionary, role-based, rule-based or attribute-based access control and, encryption which can be symmetric or asymmetric consisting of respective algorithms parameters such as data encryption standards,

triple data encryption standards, advanced encryption standards, Ron's cypher or code, Blowfish and Twofish, international encryption algorithm, one-time pads, Ron Rivest, Adi Shamir and Leonard Adleman algorithm, Diffie-Hellman algorithm and Elliptic Curve Cryptography [16].

2.2 Integrity parameters

Integrity is protecting against modification of information or destruction and ensuring that information has authenticity and no-repudiation [14], [15]. According to this, the Integrity is covered by hashing algorithms parameters such as secure and message digest algorithms, integrity primitives' evaluation message digest, local area network manager, new technology local area network manager and hash-based authentication code [16].

2.3 Availability parameters

Availability ensures prompt and reliable access to and use of information [13], [14]. According to this, the Availability is covered by parameters and techniques that ensure continuity of provided services such as distributive allocation, high availability, redundancy, fault tolerance, redundant array of independent discs and disaster recovery [16].

3 Weighting the parameters of confidentiality, integrity, and availability

To weight the parameters of confidentiality, integrity and availability defined in the earlier section, we have built table models by processing data through the Excel formulas that are shown at following. The calculation of weight for the selected parameters is done according to basic equitation (1)

$$w_{xy} = \frac{N_{xy}}{N} \tag{1}$$

where:

- w_{xy} – stands for the weight of specific parameters which can have the maximum value of one
- N_{xy} – is the ranked number of the specific parameter which is sorted incrementally by one and have the values up to the number of taken parameters.
- N – is the total number of parameters

Then, the parameters of confidentiality are separated into three modelled tables. This is done considering that there are three distinct types of parameters to provide the Confidentiality, respectively the parameters of Access Control, Symmetric Encryption and Asymmetric Encryption.

Table 1 presents the Access Control (AC) parameters, where the first column shows the acronyms explained in the fourth column. The second column presents the number of parameters sorted incrementally by security (N_{AC}), while the second column shows the respective weight (w_{AC}). It is considered that the total sum of Confidentiality's parameters to be between 0.00 to 1.00 so w_{AC} is 1/3 of this sum, respectively can take values between 0.00 to 0.33 and are distributed constantly at considered parameters.

Consequently, the applied equitation (2),

$$w_{AC} = \frac{\frac{N_{AC}}{5}}{3} \tag{2}$$

gives results of Table 1.

Table 1. Table of access the access control parameters

Access Control (AC)	N_{AC}	Weight (w_{AC})	Acronyms Explained (AC)
NA	0	0.00	**NA**-Not applied
DAC	1	0.07	**DAC**-Discretionary Access Control
MAC	2	0.13	**MAC**-Mandatory Access control
RoBAC	3	0.20	**RoBAC**-Role-Based Access Control
RuBAC	4	0.27	**RuBAC**-Rule-Based Access Control
ABAC	5	0.33	**ABAC**-Attribute-based Access Control

Similarly, are generated the weighted parameters for the Symmetric Encryption (E_S) shown at Table 2. By applying the equitation (3),

$$w_{ES} = \frac{\frac{N_{ES}}{7}}{3} \tag{3}$$

the following results (Table 2) are obtained.

Table 2. Table of the symmetric encryption parameters

Encryption (E_S)	N_{ES}	Weight (w_{ES})	Acronyms Explained (E_S)
NA	0	0.00	**NA**-Not applied
DES	1	0.05	**DES**-Data Encryption Standard algorithm
3DES	2	0.10	**3DES**-Triple-DES algorithm
AES	3	0.14	**AES**-Advanced Encryption Standard algorithm
RC	4	0.19	**RC**-Ron's Cipher or Ron's Code algorithm
BT	5	0.24	**BT**-Blowfish and Twofish algorithm
IDEA	6	0.29	**IDEA**-International Data Encryption Algorithm
OP	7	0.33	**OP**-One-time Pads algorithm

Finally, the weighted parameters for the Asymmetric Encryption (E_A) are generated at show at Table 3. By applying the equitation (4),

$$w_{EA} = \frac{\frac{N_{EA}}{3}}{3} \tag{4}$$

the following results shown in Table 3 are obtained.

Table 3. Table of asymmetric encryption parameters

Encryption (E_A)	N_{EA}	Weight (w_{EA})	Acronyms Explained (E_A)
NA	0	0.00	**NA**-Not applied
RSA	1	0.11	**RSA**-Ron Rivest, Adi Shamir and Leonard Adleman algorithm
DH	2	0.22	**DH**-Diffie-Hellman algorithm
EEC	3	0.33	**EEC**-Elliptic Curve Cryptography algorithm

Same approach is followed to generate the weighted parameters for the component of the Integrity (I). Since there is found only one type of parameters to provide integrity as a cybersecurity component, which is the hashing technique (H), the equitation is:

$$w_I = \frac{N_I}{6} \tag{5}$$

that gives the following results shown at Table 4.

Table 4. Table of integrity parameters

Hashing (H)	N_I	Weight (w_I)	Acronyms Explained (H)
NA	0	0.0	**NA**-Not applied
SHA	1	0.2	**SHA**-Secure Hash Algorithm
MD	2	0.3	**MD**-Message Digest algorithm
RIPEMD	3	0.5	**RIPEMD**-RACE Integrity Primitives Evaluation Message Digest
LANMAN	4	0.7	**LANMAN**-Local Area Network Manager
NTLM	5	0.8	**NTLM**-New Technology LAN Manager
HMAC	6	1.0	**HMAC**-Hash-based Message Authentication Code

And lastly are generated the weighted parameters for the component of the Availability (A). Since there is found only one type of parameters to provide availability as a cybersecurity component, the equitation is:

$$w_A = \frac{N_A}{6} \tag{6}$$

and gives the following results shown at Table 5.

Table 5. Table of the availability parameters

Availability (*A*)	N_A	Weight (w_A)	Acronyms Explained (*A*)
NA	0	0.00	**NA**-Not applied
DA	1	0.17	**DA**-Distributive allocation
HA	2	0.33	**HA**-High availability
R	3	0.50	**R**-Redundancy
FT	4	0.67	**FT**-Fault tolerance
RAID	5	0.83	**RAID**-Redundant Array of Independent Disks
DR	6	1.00	**DR**-Disaster recovery

This weighting model of cybersecurity parameters can be used to find the distinctive network node for service placement according to security requirements.

4 Example of application of the proposed model

The model of weighting cybersecurity parameters is applied to a simulated environment. To achieve reliable results, the environment is considered at least 30 wireless networks nodes. At each node, the respective weight of cybersecurity parameters is given randomly, pre-processed according to the respective models shown at Section 3.

Table 6 shows the generated results.

Table 6. Table of CIA weighted parameters

Node ID	Confidentiality Weights			Integrity Weights	Availability Weights
	(w_{AC})	(w_{ES})	(w_{EA})	(w_I)	(w_A)
Node 1	0.33	0.1	0	0.17	1
Node 2	0.2	0.29	0	1	0.33
Node 3	0.27	0.29	0	0.67	0.83
Node 4	0	0.29	0	1	0.67
Node 5	0.27	0.19	0.11	0.17	0.33
Node 6	0.2	0.24	0.22	0.17	0.5
Node 7	0.13	0.19	0.33	0	0.33
Node 8	0.07	0.33	0.22	0.33	0.17
Node 9	0.07	0.1	0.11	1	0.5
Node 10	0.2	0.1	0.11	1	0.67
Node 11	0.07	0.33	0.33	0.5	0.67
Node 12	0.33	0.29	0.33	0.5	0
Node 13	0.2	0	0.22	1	0.5
Node 14	0.33	0.33	0	0.83	0.5
Node 15	0.27	0.33	0	0	0.17
Node 16	0.27	0.05	0	0.17	0.5
Node 17	0	0.19	0.33	0.17	0.33
Node 18	0	0	0.33	0.5	1

(Continued)

Table 6. Table of CIA weighted parameters *(Continued)*

Node ID	Confidentiality Weights			Integrity Weights	Availability Weights
	(w_{AC})	(w_{ES})	(w_{EA})	(w_I)	(w_A)
Node 19	0	0.1	0	1	0.67
Node 20	0.33	0.14	0.22	0.17	1
Node 21	0.27	0.29	0	0	0.5
Node 22	0.27	0	0.11	1	0
Node 23	0.27	0	0.22	0.5	0.67
Node 24	0.13	0.14	0.11	0.17	0.17
Node 25	0.2	0.14	0.33	0.5	0.83
Node 26	0.13	0.1	0	0.83	0.17
Node 27	0.07	0.24	0	1	0.5
Node 28	0.27	0.29	0.22	0.67	1
Node 29	0	0.33	0.11	0.83	0
Node 30	0.13	0.14	0	0.83	0.17

Then, the values are processed by using the Python programming language, version 3.11.1 running on a computer with Intel Core i5 processor and 8GB of memory RAM.

Firstly, the dataset is processed by using the clustering technique to define the number of clusters. This is done by using the K-means Elbow method [13], while the results are shown in Figure 1.

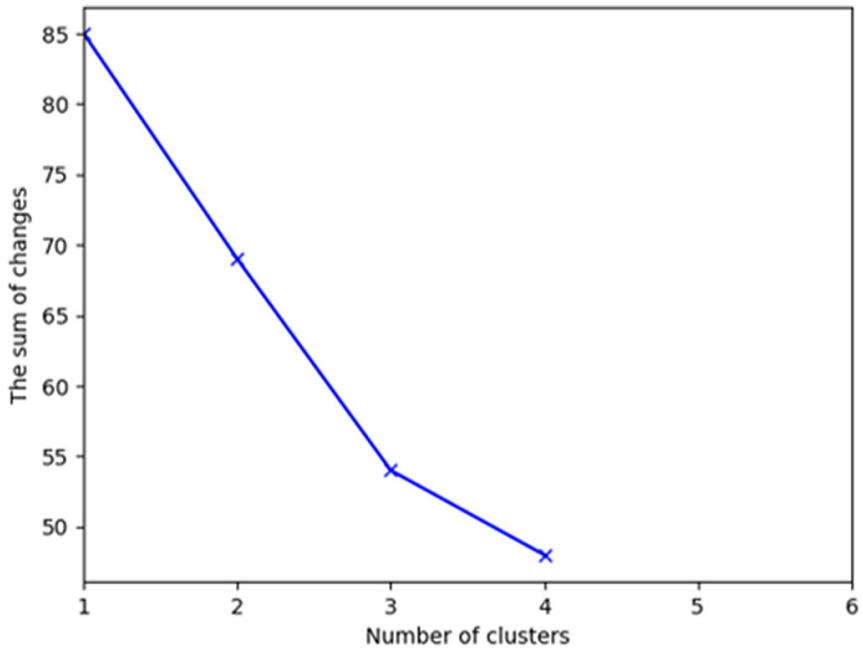

Fig. 1. Determining the optimal number of clusters in used dataset

According to Figure 1, it shows that the optimal number of clusters to be used is three. This corresponds to the number of CIA components and is used to find further results on the study's aim.

Next, we have considered that if a node has the weight (w_C, w_I, w_A) of parameters above the value 0.9 to be selected as a secure node of that network. Accordingly, nodes that have the highest weight values of confidentiality parameters are extracted and shown at Table 7.

Table 7. Table of nodes by the confidentiality

Node ID	Type of Cluster	Confidentiality Weights	Integrity Weights	Availability Weights
		(w_C)	(w_I)	(w_A)
Node 15	2	0.95	0.50	0.00
Node 18	0	0.93	0.00	0.17

From this extraction (Table 7) is shown that Node 15 and Node 18 have the highest weight values and are considered the most secure nodes for placing a service if confidentiality is needed. Node 15 has the highest weight and belongs to the third cluster.

Similarly, are extracted nodes to be considered for integrity. Table 8 shows the most secure nodes that can be considered by integrity.

Table 8. Table of nodes by the integrity

Node ID	Type of Cluster	Confidentiality Weights	Integrity Weights	Availability Weights
		(w_C)	(w_I)	(w_A)
Node 2	0	0.49	1.00	0.33
Node 10	0	0.38	1.00	0.00
Node 12	0	0.31	1.00	0.50
Node 16	0	0.53	1.00	0.50
Node 20	0	0.32	1.00	0.67
Node 27	0	0.29	1.00	0.67
Node 28	0	0.46	1.00	0.50
Node 29	0	0.59	1.00	0.67

From this (Table 8) it is shown that there are eight nodes that have the highest weight values of integrity and are considered the most secure nodes for placing a service if integrity is needed. Since all nodes have the same values, the node that has the highest weight values of other components is chosen, which is the Node 29 and belongs to the first cluster.

Then is found the node about availability. At Table 9 are shown the most secure nodes that can be considered by availability.

Table 9. Table of nodes by the availability

Node ID	Type of Cluster	Confidentiality Weights	Integrity Weights	Availability Weights
		(w_C)	(w_I)	(w_A)
Node 1	1	0.43	0.17	1.00
Node 8	2	0.33	0.50	1.00
Node 9	1	0.69	0.17	1.00
Node 25	0	0.66	0.67	1.00

From this (Table 9) it is shown that there are four nodes that have the highest weight values of availability and are considered the most secure nodes for placing a service if availability is needed. Since all nodes have same values, the node that has the highest weight values of other components is chosen, which is the Node 25 and belongs to the first cluster.

Lastly, the most secure node of all three components is extracted and shown in Table 10.

Table 10. Table of the most secure node

Node ID	Type of Cluster	Confidentiality Weight	Integrity Weight	Availability Weight
		(w_C)	(w_I)	(w_A)
Node 25	0	0.66	0.67	1.00

From this (Table 10) it is shown that considering all cybersecurity parameters, the most secure node for service placement is Node 25, which belongs to the first cluster.

5 Conclusion

The paper presents a weighting model of cybersecurity components, respectively their parameters of confidentiality, integrity, and availability, which is a distinctive method applied at network nodes. This is an attempt of a proposed model that can be used to select network nodes based on their cybersecurity fulfilments if such property is needed.

By weighting security parameters, the model gives the possibility to choose secure nodes when a specific cybersecurity component is needed like confidentiality, integrity, or availability. It also gives the possibility to choose the most secure node within a clustered network if all cybersecurity components are needed. This is the reason for proposing this model because it provides the node where a service placement can be deployed securely, avoiding vulnerabilities and potential cyberattacks.

The model uses a certain number of parameters that are weighed based on their well-known provided security mechanisms. This can be changeable if more or other parameters are found to be applied for different network nodes, so this issue should be considered. Also, values are given randomly, leading our future work on experimenting, and applying the model with an on-premises network.

6 References

[1] Mohd Fazli Mohd Sam, Albert Feisal Muhd Feisal Ismail, Kamarudin Abu Bakar, Amiruddin Ahamat, & Muhammad Imran Qureshi. (2022). *The Effectiveness of IoT Based Wearable Devices and Potential Cybersecurity Risks: A Systematic Literature Review from the Last Decade.* International Journal of Online and Biomedical Engineering (IJOE), 18(09), 56–73. https://doi.org/10.3991/ijoe.v18i09.32255

[2] Alyoubi, K. H. (2022). *An Efficient Kernel Density Based Algorithm of Big Data in Cybersecurity for Enhancing Smart City.* International Journal of Online and Biomedical Engineering (IJOE), 18(01), 52–64. https://doi.org/10.3991/ijoe.v18i01.27875

[3] I. Alghamdi, M. (2020). *Survey on Applications of Deep Learning and Machine Learning Techniques for Cyber Security.* International Journal of Interactive Mobile Technologies (IJIM), 14(16), 210. https://doi.org/10.3991/ijim.v14i16.16953

[4] Hodhod, R., Khan, S., & Wang, S. (2019). *CyberMaster: An Expert System to Guide the Development of Cybersecurity Curricula.* International Journal of Online and Biomedical Engineering (IJOE), 15(03), 70. https://doi.org/10.3991/ijoe.v15i03.9890

[5] ISACA. "Frameworks, Standards and Models." (n.d.). [Online]. Available: https://www.isaca.org/resources/frameworks-standards-and-models [Accessed Jan 10, 2023].

[6] NIST. "Executive Summary—SP 1800-25 documentation." (n.d.). [Online]. Available: https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html [Accessed Jan 12, 2023].

[7] ISO/IEC 27001:2013(en). "Information technology—Security techniques—Information security management systems—Requirements." (n.d.). [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en [Accessed Jan 15, 2023].

[8] Gashi, L., Luma, A., & Aliu, A. (2022). *A comprehensive review of cybersecurity perspective for Wireless Sensor Networks.* International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT2022), 392–395. https://doi.org/10.1109/ISMSIT56059.2022.9932788

[9] Selimi, M., Cerdà-Alabern, L., Freitag, F., Veiga, L., Sathiaseelan, A., & Crowcroft, J. (2019). *A Lightweight Service Placement Approach for Community Network Micro-Clouds.* Journal of Grid Computing, 17(1), 169–189. https://doi.org/10.1007/s10723-018-9437-3

[10] ENISA. "Security measures." (n.d.). [Online]. Available: https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/security-measures [Accessed Jan 15, 2023].

[11] SecurityScorecard. "What is the CIA Triad? Definition and Examples." (n.d.). [Online]. Available: https://securityscorecard.com/blog/what-is-the-cia-triad [Accessed Jan 15, 2023].

[12] Walkowski, D. (2019, July 9). "What Is The CIA Triad? F5 Labs." [Online]. Available: https://www.f5.com/labs/articles/education/what-is-the-cia-triad [Accessed Jan 17, 2023].

[13] Chang, R. (2021, November 5). *Confidentiality, Integrity and Availability in Cyber Security. Kobalt.Io.* [Online]. Available: https://kobalt.io/blogpost/confidentiality-integrity-and-availability-in-cyber-security/ [Accessed Jan 25, 2023].

[14] McCallister, E., Grance, T., & Scarfone, K. A. (2010). *Guide to protecting the confidentiality of Personally Identifiable Information (PII) (NIST SP 800-122; 0 ed., p. NIST SP 800-122). National Institute of Standards and Technology.* [Online]. Available: https://doi.org/10.6028/NIST.SP.800-122 [Accessed Jan 25, 2023].

[15] Nieles, M., Dempsey, K., & Pillitteri, V. (2017). *An Introduction to Information Security (NIST Special Publication (SP) 800-12 Rev. 1). National Institute of Standards and Technology.* [Online]. Available: https://doi.org/10.6028/NIST.SP.800-12r1 [Accessed Jan 25, 2023].

[16] Stallings, W., & Brown, L. (2017). Computer security: Principles and practice, Pearson, NY, 2017, (pp. 122–387).
[17] Python. – "Kmeans Elbow method." (n.d.). [Online]. Available: https://pythonprogramminglanguage.com/kmeans-elbow-method/ [Accessed Feb 10, 2023].

7 Authors

Luan Gashi – has graduated in Faculty of Computer Science and Engineering in UBT College in Prishtina. He is a Senior Computer Networks and Systems Engineer, currently working as Cybersecurity Officer at energy sector and Senior University Lecturer. He is doing doctoral studies (candidate) in Computer Science at South-East European University in Tetovo. Area of research is focused on Cyber/ICT Protection at Critical Infrastructures (email: lg29758@seeu.edu.mk).

Artan Luma – has graduated in Faculty of Contemporary Sciences in University of Tetova in Tetovo. He holds a PhD diploma in Computer Sciences from 2010. He is Full Professor in South East European University. His scientific research is cryptography and cyber security (email: a.luma@seeu.edu.mk).

Marika Apostolova – is an Associate Professor at South East European University and Director of the eLearning Center; involved as a researcher and administrator in Horizon2020; coordinating the integrated study program between German Federal Government of Development Cooperation and SEEU; mentoring bachelor, master and PhD students (email: m.apostolova@seeu.edu.mk).

Ylber Januzaj – is an Assistant Professor in University "Haxhi Zeka", Peja, Faculty of Business, Kosovo. He is Professor in the area of Informatics. He holds a PhD diploma on E-Technologies. His research interests areas are: Machine Learning, Computer Networks, and Database (email: ylber.januzaj@unhz.eu).

Article submitted 2023-03-02. Resubmitted 2023-04-02. Final acceptance 2023-04-03. Final version published as submitted by the authors.