Cybersecurity Assessments Based on Combining TODIM Method and STRIDE Model for Learning Management Systems

Taras Lechachenko[a], Tomasz Gancarczyk[b], Taras Lobur[a] and Andrii Postoliuk[a]

[a] *Ternopil Ivan Pulyuj National Technical University, Ruska, 56, Ternopil, 46001, Ukraine*
[b] *University of Bielsko-Biala, Willowa St. 2, Bielsko-Biala, 43-300, Poland*

Abstract
The algorithm of cybersecurity assessments for learning management systems (LMS) based on the STRIDE and a multi-criteria decision support TODIM method was developed in the study. Fuzzy sets were used in the proposed algorithm to formalize the values of TODIM criteria. Numerical result of the algorithm application for evaluating cyber threats for LMS was presented.

Keywords 1
STRIDE, TODIM, intuitionistic fuzzy sets, cybersecurity, LMS

1. Introduction

In the context of hybrid warfare and mass digitalization of society in Industry 4.0, protecting against cyber attacks has become an increasingly pressing challenge. In the era of Industry 4.0, cyber attacks pose a significant threat to critical sectors of the economy and can disrupt their stable functioning. Ensuring secure operation of information systems in cyberspace is a complex task, as the multi-vector nature of cyber threats and the wide range of software vulnerabilities associated with specific cyber attacks make it difficult to ensure the security of these systems.

The issue of security in Learning Management Systems (LMS) requires particular attention, as these systems are instrumental in training future professionals, including those in the field of cybersecurity. In some cases, Learning Management Systems can be seen as operating within the interdisciplinary cyberspace. This is due to the involvement of stakeholders who participate in the preparation of specialists through these software solutions. These stakeholders include not only educational institutions but also employers, as they contribute to curriculum development and serve as practice bases and providers of educational courses. Thus, the reliability and quality of preparing future professionals depend on the level of security in Learning Management Systems.

The initial step of ensuring the security of any software solution involves diagnosing its vulnerabilities and assessing the associated risks. This research addresses the objective of constructing a risk assessment algorithm for cybersecurity threats targeting Learning Management Systems during their implementation phase, employing comparative analysis as the methodology.

2. Literature Review

In the scientific discourse, studies have been presented that address the issue of analyzing the security of learning management systems (LMS). In [1], a security profile for administering online exams in LMS Moodle is presented. It is noted that Moodle can be effectively utilized for knowledge assessment, provided that the system is properly configured and deployed within a secure infrastructure. In the research conducted in [2], an analysis of vulnerabilities in 15 distance learning

CITI'2023: 1st International Workshop on Computer Information Technologies in Industry 4.0, June 14–16, 2023, Ternopil, Ukraine
EMAIL: taras5a@ukr.net (A. 1); tgan@ath.bielsko.pl (A2); lobut_t@tntu.edu.ua (A. 3); mrapostoliuk@gmail.com (A. 4);
ORCID: 0000-0003-1185-6448 (A. 1); 0000-0002-9709-0860 (A2); 0000-0001-8318-3815 (A. 3); 0009-0004-0169-3379 (A. 4);

platforms is performed using Netsparker and Acunetix scanners. A total of approximately 12 vulnerabilities are identified in this study, with the highest proportion consisting of HTTP authentication and XSS vulnerabilities. It is worth noting that this research employed automated vulnerability detection tools, which should also be critically interpreted by experts. In the study [3], vulnerabilities and protection of M-learning platforms in cloud environments are examined. The authors provide examples of cyber-attacks on cloud services, including DDOS, malware injection attacks, side channel attacks, authentication and MITM attacks, and virtual machine escape. It should be noted that the study focuses on attacks and vulnerabilities primarily related to the deployment infrastructure of M-learning. In the study [4], an analysis of 11 web threats related to LMS is conducted, along with proposed measures for their mitigation. It should be noted that the study has, in particular, an overview character. In the work [5], the authors propose a functional model of information system security, which is based on decomposing the system into individual functions and identifying stakeholders interacting with the system. An example of applying the developed model is provided in the work, focusing on the registration functionality of the learning management system and associated vulnerabilities and potential cyber-attacks. The study presents numerical results obtained from applying the model.

Analyzing the cited studies, it should be noted that the problem of quantitative risk assessment of cyber-attacks and vulnerabilities in learning management systems (LMS) is insufficiently addressed in the scientific discourse. In particular, there is a lack of research on comprehensive expert assessment of cyber risks in LMS, considering the comparative evaluation of alternative systems during their implementation, i.e., ranking alternatives based on criteria. This study proposes an algorithm for assessing cyber threat risks in LMS using multi-criteria analysis of alternatives based on selected criteria.

3. Models and methods

Among the risk assessment models, it is worth noting the PASTA model [6], which consists of seven steps: goal definition, technical environment identification, decomposition and analysis application, threat analysis, weakness and vulnerability analysis, attack simulation and modeling, risk analysis and management. Another risk analysis model is LINDUNN [7], which consists of the following steps: constructing a data flow diagram, identifying security threats to the elements of the data flow diagram, defining negative scenarios, prioritizing risks, defining security requirements, and selecting security improvement solutions. The Fault Tree Analysis method [8], is based on decomposing an undesired event into possible components that led to its occurrence. The research [9] describes the OCTAVE threat assessment method, which consists of the following phases: constructing a threat profile based on assets, identifying infrastructure vulnerabilities, and developing security strategies and plans. Each phase, in turn, encompasses specific processes.

This study utilizes the STRIDE cyber threat risk analysis model [10], which assesses the following security threats: Spoofing: Masquerading of a legitimate user, processor system element. Tampering: Modification/editing of legitimate information. Repudiation: Denying or disowning a certain action executed in the system. Information disclosure: Data breach or unauthorized access to confidential information. Denial of Service (DoS): Disruption of service for legitimate users. Elevation of privilege: Getting higher privilege access to a system element by a user with restricted authority. The selection of the STRIDE risk assessment model is associated with criteria describing fundamental and core cybersecurity threats, which are critical to the operation of learning management systems. It should be noted that the threats in the STRIDE model, due to their foundational nature, are comprehensive and encompass various subtypes and methods that implement each threat. The algorithm for assessing the security of learning management systems (LMS) against cyber threats based on the STRIDE model will consist of the following steps:

1. Formation of the evaluation criteria set based on STRIDE.
2. Selection of experts for assessment.
3. Assignment of linguistic evaluations by the experts for each evaluation criterion.
4. Translation of linguistic variables into numbers of fuzzy sets.
5. Aggregation of fuzzy evaluations.

6. Determination of the comparative security assessment of LMS using Multiple Criteria Decision Making (MCDM) with the representation of alternative rankings.

In this study, the TODIM [11] method of Multiple Criteria Decision Making (MCMD), belonging to the family of decision support methods, is chosen to be used. The MCMD methods are based on the comparative analysis of alternatives by finding the distances of criterion evaluations from absolute minimum and maximum values or by assessing the dominance of alternatives among each other. The motivation for using the TODIM method in this study is its ability to consider the decision maker's attitude towards losses when ranking alternatives. The TODIM method incorporates a coefficient that mitigates the effect of losses based on prospect theory. This characteristic of the TODIM method is an important factor in assessing the risks of cyber threats, as cybersecurity threats are complex and may involve various tools for their realization using different types of vulnerabilities, requiring critical prioritization.

Let's present the algorithm of the TODIM [12] method. Let $\{a_1, a_2, ...a_m\}$ be a set of alternatives, $\{c_1, c_2, ...c_n\}$ be a set of criteria with their corresponding $\{w_1, w_2, ...c_n\}$ weights satisfying the condition $w_i \in [0,1]$ and $\sum_{i=1}^{n} w_i = 1$. We construct a matrix $a = [d_{ij}]_{m \times n}$, d_{ij} where represents the evaluation of alternative $a_i (i = 1,2,...m)$ based on criterion $c_j (j = 1,2,...n)$. Let's assume that $w_{jk} = w_j / w_k$ are the relative weights for each criterion c_j, c_t where $w_k = max(w_j)$ $k, j = 1,2...,n$. The TODIM method consists of the following steps:

1. Normalization $a = [d_{ij}]_{m \times x}$ into $a' = [d'_{ij}]_{m \times x}$.

2. Calculation of alternative a_i dominance over a_t alternative based on criterion c_j. In this case, consider the factor ρ as a mitigating factor for loss effects. Thus, the calculation is as follows:

$$\delta(a_i, a_t) = \sum_{j=1}^{n} \upsilon_j(a_i, a_t) (i,t = 1,2...,m)$$

$$\upsilon_j(a_i, a_t) = \begin{cases} \sqrt{w_{ik}(d_{ij} - d_{tj}) / \sum_{j=1}^{n} w_{jk}} & if\ d_{ij} - d_{tj} > 0 \\ 0 & if\ d_{ij} - d_{tj} = 0 \\ -\frac{1}{\rho}\sqrt{(\sum_{j=1}^{n} w_{jk})(d_{ij} - d_{tj}) / w_{jk}} & if\ d_{ij} - d_{tj} < 0 \end{cases} \quad (1)$$

Where $\upsilon_j(a_i, a_t)(d_{ij} - d_{tj} > 0)$ represents advantage and $\upsilon_j(a_i, a_t)(d_{ij} - d_{tj} < 0)$ represents loss.

3. Calculation of the overall evaluation according to the formula:

$$\delta(a_i) = \frac{\sum_{t=1}^{m} \delta(a_i, a_t) - min\left\{\sum_{1}^{m} \delta(a_i, a_t)\right\}}{max\left\{\sum_{1}^{m} \delta(a_i, a_t)\right\} - min\left\{\sum_{1}^{m} \delta(a_i, a_t)\right\}} \quad (2)$$

4. Selection of the best $\delta(a_i)$ alternative with the highest value.

To evaluate the alternatives, it has been decided to use intuitionistic fuzzy sets [13] and the corresponding scale of linguistic variables as in the work [14]:

Table 1
Intuitionistic linguistic variables

Linguistic terms	IFNs
Extremely Good (EG)	[1.00; 0.00; 0.00]
Very Good (VG)	[0.85; 0,05; 0.10]
Good (G)	[0.70; 0.20; 0.10]
Medium Bad (MB)	[0.50; 0.50; 0.00]
Bad (B)	[0.40; 0.50; 0.10]
Very Bad (VB)	[0.25; 0.60; 0.15]
Extremely Bad (EB)	[0.00; 0.90; 0.10]

The aggregation of experts' opinions is determined using the formula [15]:

$$d_{ij} = IFWAr_{\lambda}(r_{ij}^{(1)}, r_{ij}^{(2)}, ..., r_{ij}^{(k)}) = \lambda_1 r_{ij}^{(1)}, \lambda_2 r_{ij}^{(2)}, ..., \lambda_k r_{ij}^{(k)}$$
$$= \left[1 - \prod_{l=1}^{k} (1 - \mu_{ij}^{l})^{\lambda_l}, \prod_{l=1}^{k} (v_{ij}^{(l)})^{\lambda_l}, \prod_{l=1}^{k} (1 - \mu_{ij}^{l})^{\lambda_l} - \prod_{l=1}^{k} (v_{ij}^{(l)})^{\lambda_l} \right]. \quad (3)$$

Where $r_{ij}^{(k)}$ represents the *i*- assessment of *k*-expert on j criterion, λ_k - represents the weight of the expert, and $\mu_{ij}^{l}, v_{ij}^{(l)}$ are fuzzy intuitionistic numbers.

The distance between intuitionistic numbers A and B are calculated using the distance [16]:

$$d_H(A,B) = \frac{1}{2n} \sum_{i=1}^{n} \left(|\mu_A(x_i) - \mu_B(x_i)| + |v_A(x_i) - v_B(x_i)| + |\pi_A(x_i) - \pi_B(x_i)| \right) \quad (4)$$

To ensure accurate representation of calculations involving fuzzy intuitionistic numbers, we modify the conditions for determining distances in the TODIM method as follows:

$$\upsilon_j(a_i, a_t) = \begin{cases} \sqrt{w_{ik}(d_{ij} - d_{tj}) / \sum_{j=1}^{n} w_{jk}} & if\ d_{ij} > d_{tj} \\ 0 & if\ d_{ij} = d_{tj} \\ -\frac{1}{\rho} \sqrt{(\sum_{j=1}^{n} w_{jk})(d_{ij} - d_{tj}) / w_{jk}} & if\ d_{ij} < d_{tj} \end{cases} \quad (5)$$

Where $\upsilon_j(a_i, a_t)(d_{ij} > d_{tj})$ represents advantage and $\upsilon_j(a_i, a_t)(d_{ij} < d_{tj})$ represents loss.

4. Results

The assessment of LMS vulnerabilities to STRIDE cyber threats is conducted using the most popular learning management systems within both international and domestic educational environments, including Moodle, Atutor, and Ilias,. Three experts have been selected to evaluate the degree of security of the LMS. The educational background of the experts aligns with the field of cybersecurity, and they have a minimum of 3 years of experience in this domain.

The results of the learning management systems assessment using linguistic variables by experts are presented in Table 2.

Table 2
Expert assessments using linguistic variables

Treats	Ilias			Atutor			Moodle		
	DM1	DM2	DM3	DM1	DM2	DM3	DM1	DM2	DM3
Spoofing	VB	B	B	B	MB	B	B	MB	B
Tampering	B	VB	VB	MB	B	MB	MB	B	B
Repudation	G	MB	MB	G	B	G	G	VG	G
Information disclosure	B	B	MB	G	VG	G	G	G	G
Denial of service	G	MB	G	G	G	G	VG	G	VG
Elevation of privilege	B	B	B	B	B	B	B	B	MB

The weights of the STRIDE method criteria are presented in Table 3.

Table 3
The weights of the criteria

Treats	Weights
Spoofing	0,319
Tampering	0,159
Repudation	0,039
Information disclosure	0,159
Denial of service	0,002
Elevation of privilege	0,319

The aggregated assessments of experts in intuitionistic fuzzy numbers are presented in Table 4.

Table 4
The fuzzy intuitionistic assessments of the experts

Treats	Ilias			Atutor			Moodle		
	DM1	DM2	DM3	DM1	DM2	DM3	DM1	DM2	DM3
Spoofing	0,350	0,534	0,114	0,432	0,503	0,064	0,432	0,503	0,064
Tampering	0,301	0,567	0,130	0,465	0,503	0,031	0,432	0,503	0,064
Repudation	0,574	0,372	0,053	0,618	0,275	0,106	0,758	0,128	0,112
Information disclosure	0,432	0,503	0,064	0,758	0,128	0,112	0,696	0,203	0,100
Denial of service	0,640	0,275	0,084	0,696	0,203	0,100	0,807	0,081	0,110
Elevation of privilege	0,396	0,5034	0,099	0,396	0,503	0,099	0,432	0,503	0,064

The intermediate calculations of alternative dominance in Table 5.

Table 5
The $\delta(a_i, a_t)$ values of alternative dominance

Ilias	Atutor	Moodle
-9,975	0,643	0,760
-14,063	-9,055	-0,939

The ranking of prioritized alternatives is presented in Table 6.

Table 6
Ranked alternatives

Alternatives	Value	Rating
Ilias	0,00	3
Atutor	0,65	2
Moodle	1	1

According to the obtained results presented in Table 6, the best alternatives among those studied, according to the experts, are Moodle in second place, Atutor, and Ilias in last place. It should be noted that assessing the security of learning management systems is a complex and challenging task. Experts used both automated software tools and expert evaluation of the system components security, conducting a comprehensive interpretation of the identified vulnerabilities.

5. Conclusion

According to the obtained results, it can be asserted that significant threats to the security of learning management systems are cyber risks associated with Spoofing, Tampering, and Elevation of privilege. It is worth noting that some of the analyzed learning management systems require differentiation of system access for teachers and students, as well as the implementation of dual verification during system login.

The prospect for further research lies in the development of a multi-criteria decision support method to assess risks in order to prevent them, in particular for cyber-physical biosensor systems [17-19], taking into account their security issues [20, 21].

6. References

[1] Ally, Said. "Review of Online Examination Security for the Moodle Learning Management System." International Journal of Education and Development using Information and Communication Technology 18.1 (2022): 107-124.

[2] M. Bhatia and J. K. Maitra, "E-learning Platforms Security Issues and Vulnerability Analysis," 2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES*)*, Lucknow, India, 2018, pp. 276-285, doi: 10.1109/CCTES.2018.8674115.

[3] Adejo, Olugbenga W., et al. "E-learning to m-learning: Framework for data protection and security in cloud infrastructure." International Journal of Information Technology and Computer Science (IJITCS) 10.4 (2018): 1-9, doi: 10.5815/ijitcs.2018.04.01

[4] H. Ibrahim, S. Karabatak and A. A. Abdullahi, "A Study on Cybersecurity Challenges in E-learning and Database Management System," *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, Beirut, Lebanon, 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116415.

[5] N. Rjaibi, and L.B.A. Rabai. Functional Specification to Support Security Risk Assessment of Large Systems, in: Software Engineering and Algorithms in Intelligent Systems: Proceedings of 7th Computer Science On-line Conference 2018, Volume 1 7, Springer International Publishing, pp. 84-89., 2019.

[6] G. Kaur, ZH. Lashkari, AH. Lashkari . Understanding Cybersecurity Management in FinTech. Springer International Publishing, 2021. doi.org/10.1007/978-3-030-79915-1

[7] K. Wuyts, R. Scandariato, W. Joosen, M. Deng, B. Preneel,: LINDDUN: a privacy threat analysis framework,. DistriNet, 2019. pp. 1–23URL: https://people.cs.kuleuven.be/~kim.wuyts/LINDDUN/LINDDUN.pdf

[8] D. Ionita. Current established risk assessment methodologies and tools. MS thesis. University of Twente, Netherlands, 2013.

[9] G. Sabaliauskaite, AP. Mathur. Aligning cyber-physical system safety and security. Complex Systems Design & Management Asia: Designing Smart Cities: Proceedings of the First Asia-Pacific Conference on Complex Systems Design & Management, CSD&M Asia 2014. Springer International Publishing, 2015, pp. 41-53. doi.org/10.1007/978-3-319-12544-2_4
[10] R. Khan, K. McLaughlin, D. Laverty and S. Sezer, STRIDE-based threat modeling for cyber-physical systems, 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Turin, Italy, 2017, pp. 1-6, doi: 10.1109/ISGTEurope.2017.8260283.
[11] Gomes, L.F.A.M.; Lima, M.M.P.P. Todim: Basic and application to multicriteria ranking of projects with environmental impacts. Found. Comput. Decis. Sci. 16, (1991) 113–127.
[12] J. Wang, G. Wei, M. Lu. TODIM Method for Multiple Attribute Group Decision Making under 2-Tuple Linguistic Neutrosophic Environment. Symmetry 10 (2018), 486. https://doi.org/10.3390/sym10100486
[13] K.T. Atanassov, and K.T. Atanassov. Intuitionistic fuzzy sets. Physica-Verlag HD. 1999. pp. 1-137
[14] BD. Rouyendegh. The Intuitionistic Fuzzy ELECTRE model, International Journal of Management Science and Engineering Management, 13:2 (2018) 139-145. doi: 10.1080/17509653.2017.1349625
[15] L. Abdullah, L. Najib . Sustainable energy planning decision using the intuitionistic fuzzy analytic hierarchy process: choosing energy technology in Malaysia. International Journal of Sustainable Energy 35.4 (2016): 360-377. doi.org/10.1080/14786451.2014.907292
[16] E. Szmidt, J. Kacprzyk. Distances between intuitionistic fuzzy sets. Fuzzy sets and systems 114.3 (2000): 505-518. doi.org/10.1016/S0165-0114(98)00244-9
[17] V.Martsenyuk, A. Sverstiuk, O. Bahrii-Zaiats, Y. Rudyak, B. Shelestovskyi, Software complex in the study of the mathematical model of cyber-physical systems, in: CEUR Workshop Proceedings, volume 2762, 2020, pp. 87–97.
[18] V. Martsenyuk, A. Sverstiuk., A. Klos-Witkowska, N. Kozodii, O. Bagriy-Zayats, I. Zubenko, Numerical Analysis of Results Simulation of Cyber-Physical Biosensor Systems, in: 1st International Workshop Information-Communication Techologies&Embedded Systems, 14-15 November, Mykolaiv, Volume 1, 2019, pp. 149–164.
[19] V. Martsenyuk, A. Sverstiuk, O. Bahrii-Zaiats, A. Klos-Witkowska, Qualitative and Quantitative Comparative Analysis of Results of Numerical Simulation of Cyber-Physical Biosensor Systems, in: CEUR Workshop Proceedings, 2022, 3309, pp. 134–149.
[20] R. Alguliyev, Y. Imamverdiyev, L. Sukhostat, Cyber-physical systems and their security issues, Computers in Industry, Volume 100, 2018, pp. 212-223, https://doi.org/10.1016/j.compind.2018.04.017.
[21] Lypak, H., Rzheuskyi, A., Kunanets, N., Pasichnyk, V. Formation of a Consolidated Information Resource by Means of Cloud Technologies. 2018 International Scientific-Practical Conference on Problems of Infocommunications Science and Technology, PIC S and T 2018 – Proceedings, pp. 157-160.