A TOPSIS-Based Approach to Evaluate Alternative Solutions for GDPR-Compliant Smart-City Services Implementation

Lelio Campanile[1], Mauro Iacono[1], Michele Mastroianni[2(✉)], Christian Riccio[1], and Bruna Viscardi[3]

[1] DMF, Università degli Studi della Campania "L. Vanvitelli", viale Lincoln 5, 81100 Caserta, Italy
{lelio.campanile,mauro.iacono,christian.riccio}@unicampania.it
[2] DAFNE, Università degli Studi di Foggia, Via A. Gramsci 89/91, 71122 Foggia, Italy
michele.mastroianni@unifg.it
[3] Caserta, Italy

Abstract. Adapting or designing a system which operates on personal data in EU is impacted by the privacy-by-design and privacy-by-default principles because of the prescriptions of the GDPR.

In this paper we propose an approach to decision making which is based on TOPSIS (Technique for Order Preference by Similarity to Ideal Solution). The approach is applied to a GDPR system compliance design process, based on a case study about system performance evaluation by means of queuing networks, but is absolutely general with respect to analogous problems, in which cost issues should be balanced with technical performances and risk exposure.

Keywords: Privacy · GDPR · Decision support · Performance evaluation · Queuing networks · Data management · Risk Analysis · Risk Assessment · Information systems

1 Introduction

Adapting or designing a system which operates on personal data in EU is impacted by the privacy-by-design and privacy-by-default principles because of the prescriptions of the GDPR. The GDPR imposes that privacy should be involved into the design process since the earliest stages, introducing mandatory non-functional specifications [5], and that non-compliant systems must be adapted in order to continue operations.

Anyway, in coherence with the praxes of European regulations[1], the GDPR does not specify how privacy-by-default or privacy-by-design principles can be

B. Viscardi—Independent Expert.

[1] Differently from this case, for example, technical regulations issued according to the Italian legal tradition do explicitly specify how to be technically compliant with technical regulations when posing limitations.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2026
O. Gervasi et al. (Eds.): ICCSA 2025 Workshops, LNCS 15893, pp. 303–316, 2026.
https://doi.org/10.1007/978-3-031-97645-2_20

satisfied in a design, nor there is any technical regulation or standard describing a compliance procedure. This implies that specific investments should be put on the compliance and related implementation issues in a new design, and that this is anyway not granting that, in case of incidents, the system will be considered compliant notwithstanding the efforts, exposing the owner of the system to significant risk of liability depending exclusively on the opinion of experts delegated by the court, with little possibility for opposing unquestionable arguments or exhibiting universally accepted proofs of compliance. In the case of existing systems, moreover, each deployed copy should be properly updated and related maintenance procedures should be consistently changed, implying a fixed evolutionary update cost per deployed item, which may involve unplanned hardware costs and introduce potential bugs and security vulnerabilities, and possibly a different cost for periodic maintenance and different maintaining procedure and personnel, still with the same risk in case of incidents; or replacement may be needed, falling back in the previous case, before the end of the planned operational life of the system, before the amortization of the asset, if no fix is possible or viable.

These costs should be careful taken into consideration for a business. Depending of their amount and the nature of the system, on one hand the manufacturer of the system may continue selling it without any actual privacy-related action claiming for compliance, estimating a low risk of involvement in case the user may incur into an incident with a third party, hypothesizing a sloppy behavior of the user running the system with reference to the obligation to report privacy breaches, so a direct responsibility of the user; on the other hand, the user owning an already installed system may decide not to take any action to make it compliant, aiming at reaching the end of its operational life without incidents and replacing it with a compliant one afterward, or fixing the system at the first major update, estimating a low risk of incidents before.

Such decisions are not necessarily originated by malicious intentions. They may just be needed because the manufacturer or the user could not take the extra costs and related burden without suffering significant consequences, jeopardizing their survival in their field, or because decisions are taken on the basis of partial information, erroneous self confidence or naive decision processes. This is more likely in the case of subjects which operate in the small scale of their sector. Anyway, the related decision process is not to be inscribed in the sphere of strategy, as in the long term new products or new versions are generally taking the place of the problematic one, so the horizon is the mid term, and the decision level is on the tactical level; nevertheless, the mid term is still exposing to non negligible risk, which should be considered.

In this paper we propose an approach to decision making which is based on TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) [26]. The approach is applied to a GDPR system compliance design process, based on a case study about system performance evaluation by means of queuing networks [6], but is absolutely general with respect to analogous problems, in which cost issues should be balanced with technical performances and risk exposure.

This paper is organized as follows: next Section provides backgound and related work, followed by a section in which TOPSIS computation has been detailed. In the following in Sect. 4 the used approach is described, while in Sect. 5 the case study is detailed, and Sect. 6 presents the results of the analysis and the last Section is devoted to conclusions and future work.

2 Background

2.1 TOPSIS and Evaluation of Alternatives

The *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS), introduced in 1981 by Hwang and Yoon [13], is a consolidated method in the family of multicriteria decision analysis techniques that provides support to complex decisions, characterized by multiple contrasting criteria, in a wide range of application scenarios [26,28]. Methodologically, TOPSIS is grounded on the identification and comparison of one ideal positive solution (i.e. the best one, composed of the most advantageous criteria under consideration) and an ideal negative solution (the worst one, composed of the less desirable values a criteria might take) [3]. The decision process starts from the construction of a decision matrix, in which rows identify alternatives and columns the criteria under evaluation. The rationale is to identify the best choice in a series of alternatives applying the principles of compromise solutions. The compromise solution can be viewed as selecting the option having the minimal Euclidean distance from the ideal solution and the maximal Euclidean distance from the negative ideal solution.

In the context of Information and Communication Technology (ICT), TOPSIS has found a vast amount of applications thanks to its efficacy in the evaluation of various aspects, such as technical performances, reliability of systems, data security, and associated operation costs [11,15,23]. Moreover, TOPSIS is employed in many scholarly and applied research projects to compare hardware and software configurations, cybersecurity approaches, and network protocols [1,17,23].

In the last years, there has been an increasing interest in TOPSIS to simultaneously analyze operational performance criteria while preserving privacy, especially in advanced technological contexts such as 5G networks, storage systems such as both Cloud and distributed ledgers (i.e., Blockchain-based systems [7]), as well as Cloud computing and Internet of Things (IoT) [20,21,30]. In [4] the relevance is emphasized of having a systematic approach, which includes specific risk criteria due to the exposure of sensitive data, to correctly balance the trade-off between operation efficiency and security.

2.2 Privacy and GDPR

The growing importance of data protection to individuals has seriously reshaped the European regulatory agenda, and, to this end, the General Data Protection

Regulation (GDPR)[2] came into force [19,22]. The GDPR has its foundations built on a host of underlying concepts, including privacy-by-design and privacy-by-default, which are outlined in Article 25. This principle asserts that security and data protection safeguards must be ingrained in systems seamlessly right at the outset of their design. Hence, all such data systems dealing with personal information shall provide negligible (or nil) chances of unlawful treatments, more so keeping the potential contraventions at bay [12].

The GDPR is under rigorous rules as regards data privacy with strict monetary penalties, which may constutute a major risk exposure to all organizations operating in EU or handling European residents' personal data, irrespective of their size. Notably, in 2023, Ireland Data Protection Commission imposed a massive penalty of €1.2 billions on Meta Platforms Limited for the transfer of EU citizens' personal data to the United States without implementing adequate protection measures. This fine constitutes the largest fine ever imposed under the GDPR to date[3].

The regulation establishes roles and responsibilities for well-defined key figures, such as the data controller and data processor (presented in Article 4, paragraphs 7 and 8). These figures are compelled to implement all feasible technical and organizational measures to ensure compliance with the regulation[4]. Although international organizations like the European Data Protection Board (EDPB) and the International Organization for Standardization (ISO) have published guidelines and best practices to help organizations implement the privacy-by-design and privacy-by-default principles in practice, the GDPR does not provide detailed operational guidelines. This leaves room for interpretation, particularly when it comes to precisely identifying the organizational and technical measures that are required, managing the responsibilities between controller and processor, and defining audit and compliance verification procedures. Different recent studies, among them the one in [4], suggest how this gap can be filled through the adoption of structured methods, such as the multicriteria TOPSIS technique, capable of systematically addressing the decision-making complexity arising from the need to balance technical performance, security, and privacy [1,14,16]. By enabling thorough and reliable comparisons between various design choices, the application of structured methodological approaches—like TOPSIS makes it easier to choose the best solutions and lowers the possibility of facing fines for regulatory infractions. Through proactive and strategic management of data security issues, this approach encourages more thoughtful management of technical and operational resources, such as IT infrastructures, security software, specialized personnel, and internal regulatory compliance procedures, which can be successfully integrated among the evaluation criteria adopted in the TOPSIS methodology for a more informed and methodical decision-making process [2].

[2] https://gdpr-info.eu.

[3] https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland.

[4] Their obligations and responsibilities are explored in depth respectively in Article 24 and 28.

3 The TOPSIS Method

The formalism adopted in *Technique for Order Preference by Similarity to Ideal Solution (TOPSIS)* is described in the following subsections [3].

3.1 Step 1: Construct the Decision Matrix

Given m alternatives and n criteria, the decision matrix X is:

$$X = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix} \tag{1}$$

where x_{ij} represents the performance of alternative i on criterion j.

3.2 Step 2: Normalize the Decision Matrix

The normalized decision matrix R is calculated using:

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \quad \text{for } i = 1, \ldots, m; j = 1, \ldots, n \tag{2}$$

3.3 Step 3: Calculate (or Set) the Weights of the Criteria

In the scientific literature, scholars have tested many different techniques to determine weight values [31]. In this work, we choose to use the Entropy method [18] due to the vast adoption. The advantages of Entropy method to compute weights value are:

- the value of weights are based on data dispersion, avoiding subjective bias from decision-makers;
- uses the dataset variability to assign weights, making it statistically robust: higher entropy (more dispersion) in a criterion leads to a higher weight, indicating greater importance;
- widely applicable and simple to compute.

The disadvantages are that this kind of computation is purely data-based, so it may overlook expert knowledge or policy requirements, and it is sensitive to data quality. Due to the choice done, the following steps are devoted to present the details on Entropy weight computation.

Calculate the Entropy Measure
For each criterion j, compute the entropy measure e_j:

$$e_j = -k \sum_{i=1}^{m} f_{ij} \ln f_{ij} \tag{3}$$

where:

$$f_{ij} = \frac{r_{ij}}{\sum_{i=1}^{m} r_{ij}}$$
$$k = \frac{1}{\ln m} \quad \text{(normalization factor)}$$

Calculate the Degree of Diversion

$$d_j = 1 - e_j \tag{4}$$

Calculate the Entropy Weights

$$w_j = \frac{d_j}{\sum_{j=1}^{n} d_j} \tag{5}$$

3.4 Step 4: Construct the Weighted Normalized Decision Matrix

Multiply the normalized decision matrix by the entropy weights:

$$V = [v_{ij}]_{m\times n} = [w_j \cdot r_{ij}]_{m\times n} \tag{6}$$

3.5 Step 5: Determine the Ideal and Negative-Ideal Solutions

$$A^+ = \left\{v_1^+, v_2^+, \ldots, v_n^+\right\} = \left\{\left(\max_i v_{ij} \mid j \in J\right), \left(\min_i v_{ij} \mid j \in J'\right)\right\} \tag{7}$$
$$A^- = \left\{v_1^-, v_2^-, \ldots, v_n^-\right\} = \left\{\left(\min_i v_{ij} \mid j \in J\right), \left(\max_i v_{ij} \mid j \in J'\right)\right\} \tag{8}$$

where:

- J is the set of benefit criteria (larger is better)
- J' is the set of cost criteria (smaller is better)

3.6 Step 6: Calculate the Separation Measures

$$S_i^+ = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^+\right)^2} \quad \text{(Distance to ideal solution)} \tag{9}$$

$$S_i^- = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^-\right)^2} \quad \text{(Distance to negative-ideal solution)} \tag{10}$$

3.7 Step 7: Calculate the Relative Closeness to the Ideal Solution

$$C_i = \frac{S_i^-}{S_i^+ + S_i^-}, \quad 0 \leq C_i \leq 1 \tag{11}$$

3.8 Step 8: Rank the Alternatives

Rank the alternatives in descending order of C_i values. The alternative with the highest C_i value is the best choice.

4 Approach

Our approach is based on a decision process considering system performances, risk and costs in an as-is and a to-be implementations of the same system. In order to apply TOPSIS, three quantitative metrics must be identified, one per decision parameter: the metrics will be evaluated in the same regime conditions for the as-is and the to-be implementation, to allow a comparison.

The metric for system performances should consider the same operational conditions with respect to the actual application for which the system is supposed to be used, evaluated in the two implementations. As the implementations may have different architecture, a possibility is offered by the workload: as the workload must be invariant with respect to the implementation and is defined by the environment in which the system operates, the common reference can be properly provided by the workload. The behavior of the two implementations may be modeled by means of an analytical [8] or a simulative approach [10], which do not rely on actual implementation details, as functional specifications and basic dimensioning of non functional performance parameters suffice: evaluating a suitable performance index (e.g., the throughput of a relevant component or the time needed to perform a relevant processing operation) on models under the same workload provides the first metric.

The metric for risk may be obtained by means of common risk analysis techniques; in the chosen domain, the risk parameter should combine the privacy risk level estimated by an expert per exposure, the number of potential exposure events in a reference period and the duration of the use of the system until its end of life. A good reference may be obtained by exploiting the throughput of the component processing risk related items and the duration of each processing operation as provided by the performance model.

The metric for costs should consider the cost of being fined considering the estimated probability of being fined until the end of life of the system, the processing cost per item in the two implementations and the fixed cost of the substitution of the as-is with the to-be implementation.

5 A Case Study

To assess the feasibility of the TOPSIS approach, the same case study presented in [6] was adopted. This is a smart city information system in which

data is affected by privacy and security issues. In fact, images, videos, and other information from the various IoT sensors on the road are the type of data captured. The system collects information from the urban environment (moving vehicles, plate numbers, images of people on board, and even people walking on the pavement or crossing the street), and there is a privacy-sensitive data process that should be handled with extreme caution. The most obvious solution to the problem would be to invoke the law by turning all persons involved into data controllers (GDPR, Art. 28). This would put one in a defensive position from a legal point of view. Leaving out the regulatory path, a solution can be found at the level of planning the data management cycle by adding an initial unplanned protection phase [6]. In Fig. 1 a life cycle model indicated with the name *as-is* is shown, while in Fig. 3 a similar model called *to-be*, presents the addition of a protection phase. The diagrams were designed following the UML state machine method. In these data workflows, there are five common phases: collection, preparation, analysis, storage, and sharing. Below, common phases in the as-is and the to-be models:

- *Collection phase*: aggregation of a heterogeneous volume of data. The input of this phase is a 'job' performed as described in the subsystem designed in Fig. 2;
- *Preparation phase*: raw data are processed automatically without human intervention;
- *Analysis phase*: transition from data to information;
- *Storage phase*: the cleaned data and their metadata are generated in the desired form and made available;
- *Sharing phase*: data are delivered to users following a request; since the use of the data is subject to acceptance by the client.

The actors involved in the process are the *Data Collectors* who collect data from road cameras and IoT sensors and send them to the *Data Broker* who is the second actor and has the role of managing and processing the acquired data that must be sent to the last of the actors in this system, the *Data consumers* or final recipients of the data. Since there is a risk of privacy violation, a protection phase was added to the original model to improve it. The proposed solution is fully automatic, and the process consists of anonymization and pseudo-anonymization of data through encryption and automatic handling of the extreme case of spurious data acquisition through deletion. This new phase is inserted without complications as in the to-be model. One can see that the analysis phase, which is the first to operate on semantically valid information, can be extended by including a further sub-phase in charge of an automatic privacy risk assessment. At this point, artificial intelligence could be used to distinguish and select nonsensitive cases from sensitive cases, as studied in [25], in which authors demonstrate how machine learning models automate sensitivity classification through pattern recognition in unstructured data. Finally, it must be added that there could also be cases that must be handled by human inspection.

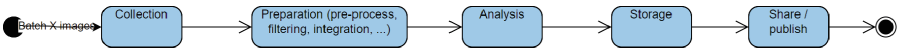

Fig. 1. As-is data workflow

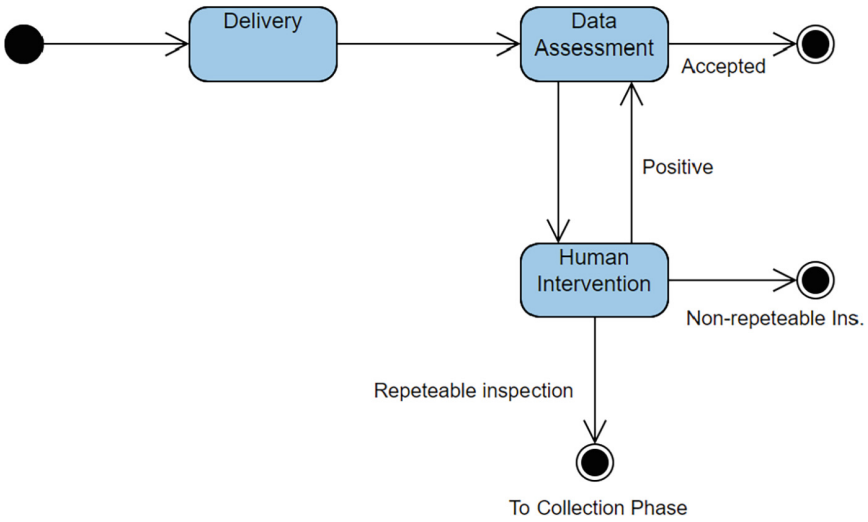

Fig. 2. As-is subsystem diagram

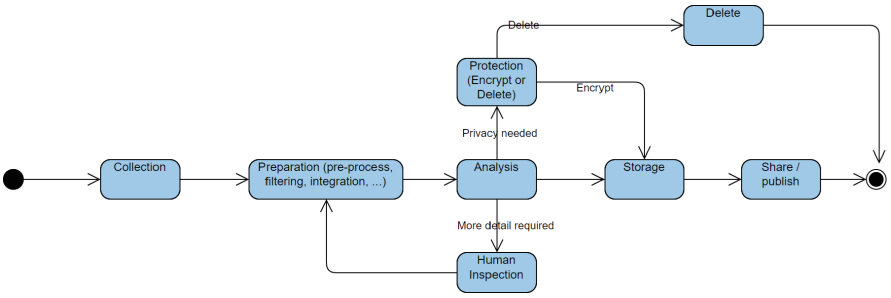

Fig. 3. To-be data workflow

In [6], a performance model for this system, in the two alternate implementations, has been proposed: this allowed the authors to state that the to-be model is proved to be valid. The comparison of the simulation results of the two models carried out in the cited work yielded positive results: the average response time of the as-is model is 43.86 [s] while that of the to-be model is 66.82 [s], the

system throughput presents an average value of more than 0.5 [s] for both models, and finally, the results of the what-if analysis suggest that by increasing the service capacity of the privacy protection station the average response time of the system throughput improves. Therefore, the trade-off between lower performance and low risk compliance is beneficial and quantifiable, and the proposed approach is feasible. The results obtained therefore proved the validity of the solution. This result was effective, which is also the reason why this case study was chosen.

In this paper, instead, the issue we want to address is to compare, on the basis of a cost-benefit comparison, the two different implementations using a quantitative method based on TOPSIS.

6 Comparison of Alternatives and Results

The first step of the evaluation process is to define the alternatives for the as-is implementation, described in Fig. 1, and the to-be system, described in Fig. 3. Taking into account the impact of possible administrative fines on the costs of the system, we choose to include in the TOPSIS comparison a third alternative, which is the as-is alternative in which costs are increased due to a penalty imposed by national data protection authority.

The three alternatives are the following:

1. **AS-IS-1**: the original system, designed without concern about GDPR;
2. **AS-IS-2**: the original system with costs increased due to a fine (other criteria have the same value of the previous);
3. **TO-BE**: the system designed to be GDPR-compliant.

Afterwards, it is necessary to define the criteria, i.e., a series of parameters related to different characteristics of the alternative solutions and to apply TOPSIS to evaluate which of those alternative is the best suited.

To do so, we define three different criteria:

1. **COST** of the alternative solution;
2. **ART** Average Response time in seconds;
3. **IMG**, the rate of images standing in "non-safe" zone (unencrypted).

Regarding the cost for the alternatives, at this time the real implementation of architecture to evaluate is not yet estimated, but there are several studies to estimate the ratio of a GDPR compliant modification of an existing architecture in a smart city environment [9,24,27,29]. So a 4/1 ratio was chosen between the cost of AS-IS-1 and TO-DO solutions; taking into account the possibility of fines by Personal Data Authorities, we estimate that the amount of the fine due to GDPR violation can double the cost of the whole system (so, Cost = 2 for AS-IS-2).

Regarding the average response time for the alternatives, we use the values of simulated systems as shown in [6]. So, for AS-IS-1 and AS-IS-2 the value is 43.86 s and for TO-DO is 66.82 s.

Using the simulator values as in the previous sentence, we obtain a value of 240 img/s for AS-IS-1 and AS-IS-2 and 10 img/s in TO-DO.

For the computation, we used the TOPSIS online tool implemented by OnlineOutput[5]. Given that the tool do not implement the computation of weight using entropy technique, the weight have been manually computed using Formula 5.

The Decision matrix (Formula 1) is the following (Table 1):

Table 1. The decision matrix for the system alternatives

	COST	ART	IMG
AS-IS-1	1.00	43,86	240.00
AS-IS-2	2.00	43,86	240.00
TO-DO	4.00	66,82	77.00

After the computation of the formula 2, the normalized decision matrix is (Table 2):

Table 2. The Normalized decision matrix and the weights computed using the Entropy method

	COST	ART	IMG
AS-IS-1	0,218	0,481	0,69
AS-IS-2	0,436	0,481	0,69
TO-DO	0,873	0,733	0,221
Weights	0.200	0.154	0.646

The results of the final comparison, shown also in Fig. 4, are:

1. **TO-BE**, score = 0.687;
2. **AS-IS-1**, score = 0.313;
3. **AS-IS-2**, score = 0.239.

From the final comparison results, it is clear that the system implemented in the "TO-BE" mode is the better alternative, and the distance between the two AS-IS solutions is even more evident when it is taken into account costs eventually due to fines from Authorities. It should be noted that, in the case the weights have been set at the same value = 0,33 (Equal weights), the rank is different, as highlighted in Fig. 4. In this case, the first two values are very similar, with a slight advantage to the "AS-IS-1"; this means that both solutions

[5] https://onlineoutput.com/topsis-software/.

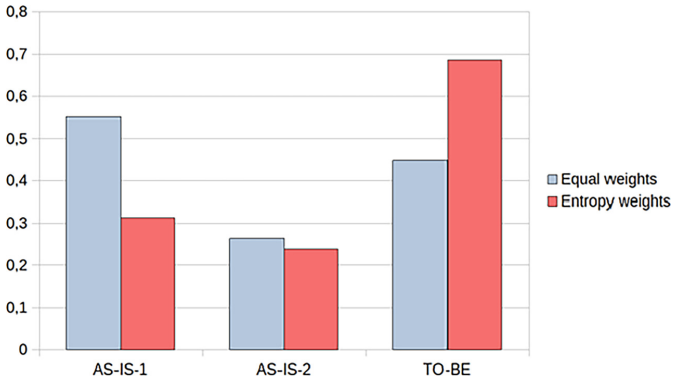

Fig. 4. TOPSIS ranking of all presented alternatives using Entropy-computed weight (red bars) vs. ranking of the same alternatives computed using equal weights = 0.33 (light blue bars). (Color figure online)

have similar efficiency (the greater cost of the second solution is compensated by the better privacy performance), but in the case of fines by authority (AS-IS-2) the increase of cost due to the high amount of penalty results in a much higher efficiency of the "TO-BE" solution. An in-depth analysis of the impact of the weights in the evaluation of alternatives is out of the scope of this work, and will be faced in future work.

7 Conclusion and Future Work

In this paper a TOPSIS-based approach to select the best design alternatives in privacy-aware environment has been proposed. In the case study presented, a massive image storage system for smart roads, the method used highlight that the privacy compliant system could be the best alternative.

Future work will split in two main directions: i) redact a more precise design of the alternatives with the aim of better compute costs and other values; and ii) define other quantitative metrics for privacy purposes to test a more comprehensive analysis using TOPSIS.

Acknowledgements. This research was partially funded by MUR PRIN PNRR 2022 grant number P20227W8ZC.

References

1. Adebiyi, S.O., Olayemi, G.A.: Predicting the consequences of perceived data privacy risks on consumer behaviour: an entropy-TOPSIS approach. Studia Humana **11**(2) (2022)

2. Ali, Z., et al.: A generic internet of things (IoT) middleware for smart city applications. Sustainability (2022). https://api.semanticscholar.org/CorpusID:255737292
3. Behzadian, M., Khanmohammadi Otaghsara, S., Yazdani, M., Ignatius, J.: A state-of the-art survey of TOPSIS applications. Expert Syst. Appl. **39**(17), 13051–13069 (2012). https://doi.org/10.1016/j.eswa.2012.05.056
4. Campanile, L., Iacono, M., Levis, A.H., Marulli, F., Mastroianni, M.: Privacy regulations, smart roads, blockchain, and liability insurance: putting technologies to work. IEEE Secur. Priv. **19**(1), 34–43 (2021). https://doi.org/10.1109/MSEC.2020.3012059
5. Campanile, L., Iacono, M., Mastroianni, M.: Towards privacy-aware software design in small and medium enterprises (2022). https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927958
6. Campanile, L., Iacono, M., Mastroianni, M., Viscardi, B.: Estimating performance costs of enabling privacy-awareness in data lifecycles. In: Proceedings of the The 1st International Conference on Modeling, Simulation and Computer Technology. Springer (2024)
7. Feng, Q., He, D., Zeadally, S., Khan, M.K., Kumar, N.: A survey on privacy protection in blockchain system. J. Netw. Comput. Appl. **126**, 45–58 (2019)
8. Franceschinis, G., Gribaudo, M., Iacono, M., Mazzocca, N., Vittorini, V.: DrawNET++: model objects to support performance analysis and simulation of systems. LNCS (LNAILNB), vol. 2324, pp. 233–238 (2002). https://doi.org/10.1007/3-540-46029-2_18
9. Frey, C.B., Presidente, G.: Privacy regulation and firm performance: estimating the GDPR effect globally. Econ. Inq. **62**(3), 1074–1089 (2024). https://doi.org/10.1111/ecin.13213
10. Gribaudo, M., Iacono, M., Manini, D.: Improving reliability and performances in large scale distributed applications with erasure codes and replication. Futur. Gener. Comput. Syst. **56**, 773–782 (2016). https://doi.org/10.1016/j.future.2015.07.006
11. Hoe, L.W., Siew, L.W., Fai, L.K.: Performance analysis on telecommunication companies in Malaysia with TOPSIS model. Indonesian J. Electric. Eng. Comput. Sci. **13**(2), 744–751 (2019)
12. Hong, P., Ahn, N.Y., Jung, E.: Linkage role of ICT and big data in covid-19: a case of Korea's digital and social communication practices. J. Inf. Commun. Ethics Soc. **21**(2), 161–180 (2023)
13. Hwang, C.L., Yoon, K.: Methods for multiple attribute decision making, pp. 58–191. Springer, Heidelberg (1981). https://doi.org/10.1007/978-3-642-48318-9_3
14. Jiang, H., Pei, J., Yu, D., Yu, J., Gong, B., Cheng, X.: Applications of differential privacy in social network analysis: a survey. IEEE Trans. Knowl. Data Eng. **35**, 108–127 (2023). https://api.semanticscholar.org/CorpusID:235083200
15. Khan, A.W., Khan, M.U., Khan, J.A., Khan, J., Gul, W.: Identification and prioritization of security challenges of big data on cloud computing based on SLR: a fuzzy-TOPSIS analysis approach. J. Softw. Evol. Process **33**(12), e2387 (2021)
16. Khumalo, Z.P.: Privacy and security for applications and services in future generation smart grids. https://api.semanticscholar.org/CorpusID:252019773
17. Koss, R., Champagne, S., Battles, J.: Toward an optimal patient safety information system (TOPSIS)
18. Le Roux, D., Olivès, R., Neveu, P.: Combining entropy weight and TOPSIS method for selection of tank geometry and filler material of a packed-bed thermal energy storage system. J. Clean. Prod. **414**, 137588 (2023). https://doi.org/10.1016/j.jclepro.2023.137588

19. Lokare, D.A., Pathan, S.M., Dhotre, P.S.: Exploring privacy challenges: a survey of issues, research gaps, and strategies for protection. In: 2025 1st International Conference on AIML-Applications for Engineering & Technology (ICAET), pp. 1–6. IEEE (2025)
20. Maček, D., Magdalenić, I., Reep, N.B.: A systematic literature review on the application of multicriteria decision making methods for information security risk assessment. Int. J. Saf. Secur. Eng. **10**(2), 161–174 (2020)
21. Ogonji, M.M., Okeyo, G., Wafula, J.M.: A survey on privacy and security of internet of things. Comput. Sci. Rev. **38**, 100312 (2020)
22. Oyewole, A.T., Oguejiofor, B.B., Eneh, N.E., Akpuokwe, C.U., Bakare, S.S.: Data privacy laws and their impact on financial technology companies: a review. Comput. Sci. IT Res. J. **5**(3), 628–650 (2024)
23. Park, J.H., Younas, M., Arabnia, H.R., Chilamkurti, N.: Emerging ICT applications and services—big data, IoT, and cloud computing (2021)
24. Rimba, P., Tran, A.B., Weber, I., Staples, M., Ponomarev, A., Xu, X.: Comparing blockchain and cloud services for business process execution. In: 2017 IEEE International Conference on Software Architecture (ICSA), pp. 257–260 (2017). https://doi.org/10.1109/ICSA.2017.44
25. Sebastian, G.: Privacy and data protection in ChatGPT and other AI chatbots: strategies for securing user information. Int. J. Secur. Priv. Pervasive Comput. (IJSPPC) **15**(1), 1–14 (2023)
26. Setiawan, H., Istiyanto, J.E., Wardoyo, R., Santoso, P.: The group decision support system to evaluate the ICT project performance using the hybrid method of AHP, TOPSIS and Copeland score. Int. J. Adv. Comput. Sci. Appl. **7**(4) (2016)
27. Stefanouli, M., Economou, C.: Data protection in smart cities: application of the EU GDPR. In: Nathanail, E.G., Karakikes, I.D. (eds.) Data Analytics: Paving the Way to Sustainable Urban Mobility, pp. 748–755. Springer International Publishing, Cham (2019)
28. Tohidi, M., Homayoun, S., RezaHoseini, A., Ehsani, R., Bagherpour, M.: Sustainability-driven supplier selection: insights from supplier life value and Z-numbers. Sustainability **16**(5), 2046 (2024)
29. Vandercruysse, L., Buts, C., Dooms, M.: A typology of smart city services: the case of data protection impact assessment. Cities **104**, 102731 (2020). https://doi.org/10.1016/j.cities.2020.102731
30. Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H.: A survey on security and privacy issues in internet-of-things. IEEE Internet Things J. **4**(5), 1250–1258 (2017)
31. Çelikbilek, Y., Tüysüz, F.: An in-depth review of theory of the TOPSIS method: an experimental analysis. J. Manag. Anal. **7**(2), 281–300 (2020). https://doi.org/10.1080/23270012.2020.1748528