Noname manuscript No.
(will be inserted by the editor)

Fuzzy-based Approach to Assess and Prioritize Privacy Risks

Stephen Harth · Anna Lisa Ferrara · Federica Paci

Received: date / Accepted: date

Abstract The New General Data Protection Regulation (GDPR) requires organizations to conduct a data protection impact assessment (DPIA) when the processing of personal information may result in high risk to individual rights and freedoms. DPIA allows organizations to identify, assess and prioritize the risks related to the processing of personal information and select suitable mitigations to reduce the severity of the risks. The existing DPIA methodologies measure the severity of privacy risks according to analysts' opinions about the likelihood and the impact factors of the threats. The assessment is therefore subjective to the expertise of the analysts. To reduce subjectivity we propose a set of well-defined criteria that analysts can use to measure the likelihood and the impact of a privacy risk. Then, we adopt the fuzzy multi-criteria decision-making approach to systematically measure the severity of privacy risks while modeling the imprecision and vagueness inherent in linguistic assessment. Our approach is illustrated for a realistic scenario with respect to LINDDUN threat categories.

Keywords Privacy risks · Privacy Risk Assessment · Fuzzy Set Theory

1 Introduction

The advent of new technologies like cloud computing, the Internet of Things and Big Data Analytic have enabled public and private organizations to collect, store and analyze huge volume of consumers' personal information. In particular, Big Data Analytic represents a competitive advantage for organizations because it reveals who their customers are, how they spend their time, and what kind of products and offers engage them. However, consumers are really concerned about the privacy risks resulting from the collection and processing of their personal information.

To minimize consumers' privacy risk, the new European General Data Protection Regulation (GDPR) has introduced stringent obligations for organizations on the collection, processing, storage and dissemination of consumers' personal information. In particular, organizations must always conduct a data protection impact assessment (DPIA) when the processing of consumers' personal information could result in a high risk to the consumers' rights and freedoms. The GDPR does not specify which methodology to follow to conduct a DPIA but sets out the minimum requirements a DPIA methodology should satisfy [19]:

- a description of the envisaged processing operations and the purposes of the processing;
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to the rights and freedoms of data subjects in terms of their likelihood and impact;
- the measures envisaged to address the risks and demonstrate compliance with this Regulation.

However, existing methodologies to conduct a DPIA [5,9,1,13] do not provide a systematic approach to assess the severity of a privacy risk based on likelihood and impact and they often adopt similar processes to the one used to rate security risks. However, the same process cannot be applied to rate security risks and privacy risks. First, security risk assessment techniques, rely on security analysts to rate impact and likelihood

Anna Lisa Ferrara
Universitá del Molise
E-mail: anna.lisa.ferrara@gmail.com

of threats with respect to simple linguistic scales, e.g. from very low to very high, with no well-specified criteria on how to determine the position on this scale. Thus, these ratings result to be extremely subjective, they may be interpreted differently by different analysts and the resulting risk ratings may not be well grounded or accurate. To reduce subjectivity, some methodologies for risk assessment define the scales for likelihood and impact evaluation based on a set of well-defined criteria. However, these criteria cannot be applied to evaluate the impact of a privacy risk because the impact of a security risk is rated only from the perspective of an organization rather than from the perspective of the data subject. The criteria are also considered equally important in assessing the impact but this does not hold for privacy attacks where the effectiveness of the criteria to estimate the impact strongly depends on the circumstances of the specific attack. For example, the scale of a data breach e.g number of records disclosed is an effective criteria in rating the impact of the breach but not for an attack where an individual has been identified into a data set, where only one record is affected.

A systematic approach to assess the severity of a privacy risk is also needed in privacy threat analysis [7], which is a similar process to DPIA, but with the goal of identifying privacy threats and translating them into viable strategies and solutions that can be mapped into privacy-enhancing technologies. Threat analysis identifies several risks that needs to be prioritized. For example, the LINDDUN methodology [20] requires to rate risk scores, but does not state specifically how these scores should be determined; as for DPIA the analyst is referred to established risk assessment techniques. Consequently, a team of privacy analysts typically faces two important challenges when prioritising privacy threats. First, the need for a consistent and clear definition of appropriate criteria to systematically measure the severity of privacy risks; secondly a way to take into account all team members' opinions while modeling the imprecision, subjectivity and vagueness inherent in linguistic assessment. The fuzzy multi-criteria decision-making problem (FMCDM) [10] has proven essential in dealing with such limitations in several settings including information security risk assessment [16]. Accordingly, we investigate the possibility of adapting the FMCDM problem to address the problem of prioritizing privacy threats when linguistic variables are used to get experts' opinion for weights of criteria and rate of alternatives.

Details about our contributions follow.

Contribution. In this paper we propose a methodology to measure the severity of privacy risks.

- We first associate the impact and likelihood of privacy risks to well-defined criteria. Since criteria are more specific than the high-level concepts of impact and likelihood, they represent more fine-grained units of measurement that make risk metrics more understandable and convenient. Risks measured using the same unit can be meaningfully aggregated, in particular when putting together several decision makers opinions, and directly compared, for example when considering different threats to prioritize. We assess the relevance of the criteria proposed with respect to one of the largest recent security breaches: the *Cyber Equifax attack*.
- Then, we adapt the fuzzy multi-criteria decision-making problem to measure likelihood and impact of threats.
  A multi-criteria decision-making (MCDM) problem consists of determining the best option among several alternatives when multiple criteria can be utilized to rate the alternatives. In our setting, criteria corresponds to those identified to characterize the likelihood and the impact of privacy threats; the alternatives correspond to the threats to be prioritized according to their likelihood and impact. Since ratings for alternatives consist of analysts' opinions, we consider *fuzzy* MCDM as fuzzy set theory is an efficient way for modeling the imprecision and vagueness inherent in linguistic assessment.
- Finally, we illustrate our methodology for a realistic scenario that, inspired by the Equifax attack, provides a proof of concept for the appropriateness of our approach. Specifically, we consider an online car insurance company and focus on privacy threats targeting the database storing customers' information. We stress that our methodology can be adopted within any framework that requires to prioritize privacy risks based on their severity. However, to put it in context, our case study illustrates our results with respect to three threat categories of the LINDDUN taxonomy [20]: linkability, information disclosure, and non compliance.

Organisation. The remainder of the paper is structured as follows. In Section 2 we review methodologies for security and privacy risk assessment. In Section 3 we provide an overview of LINDDUN methodology and we introduce the basic concepts of fuzzy set theory. Then, in Section 4 we introduce a set of criteria to evaluate likelihood and impact of privacy risks, and our methodology to assess privacy risks. We illustrate the steps of the methodology in Section 5 using a realistic scenario. We conclude the paper in Section 6 by outlining future research directions.

2 Related Works

In this section we review the existing approaches to assess security and privacy risks and discuss their limitations.

2.1 Security Risk Assessment

Several security risk assessment methods and standards have been proposed in the last years. Regardless the specific process, they all require to rate the likelihood and impact of a cyber attack to prioritize security risks and guide the selection of appropriate mitigation.

However, these methods and standards significantly differ in the way estimate the value of likelihood and impact and how they combine these values to obtain the risk level. For example, some methodologies like CORAS [11] and the NIST 800-30 [17] standard require analysts to define a qualitative scale for likelihood and impact, assign a value to likelihood and impact and then use a risk evaluation matrix to combine the values of likelihood and impact into a risk level. These method to estimate risk is subjective because it strongly depends on the opinion and expertise of the analyst. It also do not allow a comparison of the results done by two different analysts.

Other methodologies instead define criteria to estimate likelihood and impact, assign a value to these criteria and then use multiplication and/or addition of the values to compute the overall risk level. Examples of these methodologies are Octave Allegro [4] and the OWASP Risk Rating Methodology [15]. Octave Allegro requires the analyst to evaluate a risk level based on the impact that an attack have on the victim organization. The impact is assessed in terms of areas of impact: reputation, financial, productivity, safety and health, and fines and legal penalties. Each area is ranked based on the impact that it has on the organization's business goals and the values assigned to the impact areas and their rank are multiplied to obtain the overall risk score.

To address imprecision, subjectivity and vagueness inherent in linguistic assessment of likelihood and impact, some works have adopted decision theory and fuzzy logic. For instance, de Gusmao et al. developed an approach to security risk analysis that combines decision theory and fuzzy logic [6]. Shameli-Sendi et al. consider the fuzzy MCDM problem to effectively perform information security risk analysis [16]. In particular, they proposed a fuzzy expert system to assess the risks of information systems by linking expert opinions with respect to specific criteria with linguistic variables.

2.2 Privacy Risk Assessment

The few existing methodologies for assessing privacy risks have some limitations. Some methodologies like the one proposed by the Data Protection Authorities in France, Germany, Spain and UK [5,9,1,13] do not provide specific criteria to evaluate the severity and the likelihood nor a formula to combine them.

Other methodologies provide criteria but they are specific to category of privacy threats. For instance, ENISA [8] has proposed a methodology to assess the severity of personal data breaches. The main criteria are *data processing context* (DPC), *ease of identification*(EI), and *circumstances of breach*(CB). The data processing context captures the type of breached data together with a number of factors linked to the context of processing. The ease of identification determine how easy it is to identify an individual in the breached data. The circumstances of breach includes the loss of security of breach data and the malicious intent of the attacker. The overall severity is then computed as the product of DPC and EI plus the value of CB.

The remaining methodologies provide criteria for likelihood and impact estimation, but they combine these values using approaches that do not reduce the subjectivity of the evaluation.

The OWASP Top 10 List of Privacy Risks for web applications [14] evaluates privacy risks as a product of the likelihood and impact. The likelihood is estimated based on the results of a survey where experts rated the frequency of the top 10 privacy vulnerability in web applications. The impact is evaluated from the perspective of the organisation and of the individual. The former is assessed in terms of reputation and financial loss, while the one on the individual is rated based on the social standing and reputation, financial well being and personal freedom. The overall impact is computed as the average of the values assigned to each criteria.

Similarly, Wagner and Boiten [18] propose a set of criteria to assess the likelihood and impact of privacy risks. Impact is rated based on the *scale* of the attack, the *sensitivity* of the breached data, the *expectation* of the individual, and the *harm* to the individuals affected by the attack. Instead, the likelihood is given by the *likelihood of attack* and the *likelihood of adverse effect*. Rather than providing a method to combine the values assigned to each of the criteria to evaluate impact and likelihood, they measure the different criteria separately and then combine them visually using a radar plot.

Threat Category	Privacy Property	Threat Instance
Linkability	Unilinkability	Guess someone uson a diet by linking his online search for recipes
Identifiability	Anonimity, Pseudoanonimity	Identify a user in a database
Non Repudiation	Plausible Deniability	Determine who express a vote in an online voting system
Detectability	Undetectability, Unobservability	Determine who is accessing a web page
Disclosure of Information	Confidentiality	Data breach
Unawareness	Awareness	Sharing pictures on Facebook with unintended audience
Non-Compliance	Compliance	Disclosing data to third party without user's consent

Table 1 LINDDUN Privacy Threats Taxonomy and Examples.

3 Preliminaries

3.1 LINDDUN Overview

LINDDUN [20] is a privacy threat modeling technique. LINDDUN acronym stands for the categories of privacy threats that the methodology helps to identify: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness, and Non-compliance. The threat categories in the taxonomy negate corresponding privacy properties: Unlinkability, Anonimity and Pseudoanonimity, Plausible Deniability, Undetectability, Confidentiality, Awareness and Compliance. Table 1 shows the LINDDUN privacy threat categories and corresponding privacy properties along appropriate examples.

LINDDUN analysis consists of six steps. The first three represent the problem space while the remaining three correspond to the solution space:

- Problem Space
  1. A Data Flow Diagram (DFD) of the system under analysis is created, which represents how information flow into the system, how they are processed and where they are stored;
  2. Each element in the DFD is mapped with a number of LINDDUN privacy threat categories;
  3. The privacy threat categories are refined in concrete threat scenarios.
- Solution Space
  1. Privacy threats are prioritized based on their risks;
  2. An appropriate mitigation strategy is selected to address the highest privacy risks;
  3. Specific privacy enhancing technologies (PETs) have to be selected to implement the selected strategy.

3.2 Fuzzy Set Theory

Opinions cannot always be expressed in a precise way, often they are vague and uncertain. In order to model these situations more precisely, the fuzzy set theory, was proposed in [21] by L.A. Zadeh.

Given a set X called the `discourse` and a subset $A \subseteq X$. A fuzzy set is a pair (A, μ_A) where μ_A is a membership function $\mu_A : A \to [0, 1]$. The value $\mu_A(x)$ characterizes the grade of membership of x in A.

3.3 Triangular Fuzzy Number

A fuzzy number is a convex fuzzy set of the real line R such that there exists a single $x_0 \in R$, called the mean value, where $\mu_A(x_0) = 1$, while $\mu_A(x)$ is piecewise continuous.

One of the most used fuzzy number types is the triangular fuzzy number. Its membership function has the shape of a triangle, as shown in Figure 1.

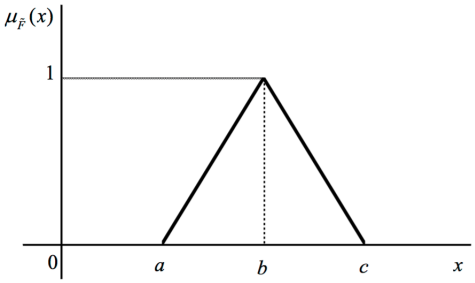

Fig. 1 Membership function of a triangular fuzzy number.

The membership function of the triangular fuzzy number $\tilde{F}$ is formalized as

$$\tilde{F} = \begin{cases} 0 & x < a \text{ and } x > c \\ \frac{x-a}{b-a} & a \le x \le b \\ \frac{c-x}{c-b} & b \le x \le c \\ 1 & x = b \end{cases}$$

where a, b, c of Figure 1 can be interpreted as the lower bound, the peak point and the upper bound of the fuzzy number, respectively. The triangular fuzzy number can be formally written as follows:

$$\tilde{F} = (a, b, c).$$

Given two triangular fuzzy numbers $\tilde{A} = (a, b, c)$ and $B = (\tilde{d}, e, f)$, four main operations can be expressed as follows:

[Addition] $\tilde{A} \oplus \tilde{B} = (a + d, b + e, c + f)$;
[Multiplication] $\tilde{A} \otimes \tilde{B} = (ad, be, cf)$;
[Multiplication by a real number k] $k \otimes \tilde{A} = (ka, kb, kc)$;

[Division] $\frac{\tilde{A}}{\tilde{B}} = (\frac{a}{d}, \frac{b}{e}, \frac{c}{f})$.

The signed distance of a triangular fuzzy number $\tilde{A}$ is defined as follows:

$$d(\tilde{A}) = \frac{1}{4}(a + 2b + c).$$

3.4 Fuzzy Multi-Criteria Decision Making Problem

A multi-criteria decision-making (MCDM) problem consists of determining the best option among several alternatives when multiple criteria can be utilized to rate the alternatives. Let $A_1, A_2, \ldots, A_m$ be possible alternatives and $C_1, C_2, \ldots, C_n$ be criteria against which alternative performance are measured. A MCDM problem can be expressed in matrix format (decision matrix) as

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

$$w = \begin{bmatrix} w_1 & w_2 & \ldots & w_n \end{bmatrix}$$

where x_{ij} is the rating of alternative A_i with respect to criterion C_j and w_j is the weight of criterion C_j. Fuzzy multi-criteria models are used to assess alternatives in situations where crisp data are inadequate. In such cases the ratings of alternatives and weights of the criteria in the problem can be evaluated using linguistic values represented by fuzzy numbers. A linguistic variable is a variable whose values are words or sentences in a natural or artificial language. These linguistic variables can be expressed in positive triangular fuzzy numbers. Specifically, Table 2 and Table 3 present linguistic variables and fuzzy numbers for, respectively, the weight of individual criteria and the ratings of alternatives.

Linguistic Variables	**Fuzzy Numbers**
Very Low (VL)	(0,0,0.1)
Low (L)	(0,0.1,0.3)
Medium Low (ML)	(0.1,0.3,0.5)
Medium (M)	(0.3,0.5,0.7)
Medium High (MH)	(0.5,0.7,0.9)
High (H)	0.7,0.9,1.0)
Very High (VH)	(0.9,1.0,1.0)

Table 2 Linguistic Variables and Fuzzy numbers for the weights of criteria.

In MCDM, normalization techniques usually map attributes (criteria) with different measurement units to a common scale in the interval $[0, 1]$ [3]. Each normalization method is divided in two formulas, one for benefit and another for cost criteria, to ensure that the final rating is logically correct, i.e. when it is a benefit criterion for high values it will correspond to high normalized values (maximization - benefit) and when it is a cost criterion high values will correspond to low normalized values (minimization - cost).

Let $\tilde{D}$ a decision matrix for a fuzzy MCDM, the linear scale transformation transforms matrix $\tilde{D}$ to a normalized fuzzy decision matrix

$$\tilde{R} = [\tilde{r}_{ij}]_{m \times n}$$

such that

$$\tilde{r}_{ij} = (\frac{a_{ij}}{c_j*}, \frac{b_{ij}}{c_j*}, \frac{c_{ij}}{c_j*})$$

if C_j is a benefit criterion where $c_j* = \max_i c_{ij}$, otherwise

Linguistic Variables	**Fuzzy Numbers**
Very Poor (VP)	(0,0,1)
Poor (P)	(0,1,3)
Medium Poor (MP)	(1,3,5)
Fair (F)	(3,5,7)
Medium Good (MG)	(5,7,9)
Good (G)	(7,9,10)
Very Good (VG)	(9,10,10)

Table 3 Linguistic Variables and Fuzzy numbers for the ratings of alternatives.

$$\tilde{r}_{ij} = (\frac{\bar{a}_j}{c_{ij}}, \frac{\bar{a}_{ij}}{b_{ij}}, \frac{\bar{a}_j}{a_{ij}})$$

if C_j is a cost criterion where $\bar{a}_j = \min_i a_{ij}$.

4 Proposed Methodology

In this section we first present the criteria for evaluating the likelihood and impact of privacy violations. The relevance of such criteria is assessed with respect to the *Cyber Equifax attack*, one of the largest recent security breaches carried out against one of the major credit reporting agencies [12]. Then, we utilize a fuzzy-based approach for assessing the level of risk of a privacy threat.

4.1 Evaluation Criteria

Likelihood. The likelihood of a privacy threat estimates the probability that an attacker will discover a vulnerability and will successfully exploit it. We evaluate the likelihood based on characteristics of the attacker and of the vulnerability being exploited and whether there are security controls in place [17]. The *motivation*, *capabilities* and *target* give an indication of whether the attacker will initiate the privacy threat or not. If conducting the privacy threat requires more capability than the attacker has, then the attacker most likely will not initiate the threat. Similarly, if an attacker does not expect to achieve its intended objectives by executing the attack, the attacker will not initiate the privacy threat. If an attacker is not targeting a specific asset in the system, the probability that he will start the attack is very low. If an attacker does not find a vulnerability or the vulnerability is not *easy to exploit* it will not start the attack. The Equifax company, for instance, is a natural target for hackers, given the kind of information that credit reporting agencies need to handle. Moreover, the vulnerability at the ground of the attack was easy to exploit and well-known to the attackers. In particular, the vulnerability was present in an open-source framework called Apache Struts that Equifax uses for its online disputes application. The Apache Software Foundation released information regarding the vulnerability, along with an update to fix the issue about two months before the attack took place. Equifax did not update its system leaving to hackers the opportunity of exploiting the vulnerability with little capabilities.

The *presence of security controls* such as encryption of personal data or the presence of intrusion detection systems or a logging mechanism could also prevent an attacker to conduct an attack. Apparently, Equifax security had monitoring techniques in place. Indeed, they noticed suspicious traffic related to its online disputes portal so that the company eventually took down the disputes application, but it was too late.Given the criteria specified, the likelihood of the Equifax attack should be moderate to moderate high. Therefore, our methodology would have correctly foreseen the attack as possible.

Impact. When considering the impact of a privacy threat, there are two kinds of impact: the impact of the organization holding the personal data and the impact of the individuals whose privacy has been violated. The impact for the organization acting as data controller can be quantified in terms of *financial damage*, *reputation damage*, *non-compliance* and the *scale* of the attack [14, 8]. The financial damage quantifies the costs incurred by the organization to fix the vulnerability being exploited, or for recovering from the attack. The reputation damage evaluates the loss of trust from customers. Non compliance instead quantifies violation of data protection regulations like GDPR and the cost of fines paid for not being compliant. The *scale* of the attack instead corresponds to number of individuals affected by the privacy threat. The first major impact for the Equifax attack which affected about 146 million individuals, was the loss of investor confidence. The share price fell by 34% within the first week of notification of the breach. The company also suffered a significant loss of revenue due to reduced activity. Furthermore, the way Equifax handled the reporting of the breach is a clear example of non-compliance with the GDPR. In order for Equifax to be GDPR compliant, it should have reported the breach to the ICO within 72 hours (as for Article 33 of the GDPR) as well as informed the data subjects without undue delay (as for Article 34 of the GDPR). Equifax waited five weeks which is a substantial delay. It is very likely that the Equifax data breach could have avoided if correct procedures had been in place.

The impact to the individual depends on the *type of breached data*, *ease of identification*, *loss of data confidentiality*, *loss of data integrity* and *loss of data availability* [8]. The type of data determines the severity of the attack: e.g if only the name of an individual is disclosed, the severity is lower than if the credit card information were disclosed. Ease of identification evaluates how easy is for the attacker to match the breached data with one or more individuals. Loss of confidentiality, integrity and availability estimates the technical impact of the attack on the individual. The Equifax attack did not result in a loss of availability but just in a loss of confidentiality and integrity because cyber crim-

inals gained access to personal information like names, addresses, dates of birth, credit score and social security numbers and this information could have been included in fraudulent credit rating and loan applications.

4.2 Fuzzy-based Privacy Risk Assessment

In this section we propose the use of fuzzy theory to estimate the likelihood and the impact of privacy threats in order to deal with the imprecision and vagueness inherent in linguistic assessment. In particular, we adapt the fuzzy multiple criteria decision-making approach, utilized for solving facility location selection problems in [2], to the problem of performing effective privacy risk assessments.

The proposed approach consists of three stages: 1) the rating stage; 2) the aggregation stage; and 3) the selection stage. In the rating stage, given m threats and n evaluation criteria, k decision-makers express their opinions (or weights) about the importance of each criterion in assessing the likelihood and the impact intensity of privacy threats as well as their ratings about the severity of each threat with respect to each specified criterion. In this stage, decision makers opinions, normally stated in fuzzy data form such as linguistic terms, are converted into triangular fuzzy numbers. In the aggregation stage, weights and ratings are aggregated and normalized in order to compute weighted fuzzy matrices with respect to both likelihood and impact criteria. In the selection state, the level of risk for threat is computed by using fuzzy values for likelihood and impact. Finally, after defazzification, threats can be prioritized according to their level of risk.

Next, we describe the details of the three aforementioned stages.

Rating Stage. This stage consists of four phases:

[Phase 1] Decision-making opinions are collected and linguistic weighting variables as well as linguistic rating variables are identified in order for decision-makers to assess criteria importance in estimating the likelihood and the impact of privacy threats.

[Phase 2] Utilize linguistic weighting variables (Table 2) to assess criteria importance.

[Phase 3] Utilize linguistic weighting variables (Table 3) to assess ratings performance of alternatives (i.e. threats) with respect to each criterion.

[Phase 4] Opinions collected in the previous two phases expressed in linguistic terms are converted in fuzzy numbers.

Aggregation Stage. This stage consists of seven phases:

[Phase 1] Compute aggregated fuzzy weights of individual criterion.
Specifically, let $\tilde{w_{jt}} = (a_{jt}, b_{jt}, c_{jt})$, where $j = 1, \ldots, n$ and $t = 1, \ldots, k$ be the weights associated to the criterion C_j by decision maker D_t, then the aggregate fuzzy weight for criterion C_j is computed as

$$\tilde{w_j} = (a_j, b_j, c_j) = \frac{1}{k}(\tilde{w_{j1}} \oplus \ldots \oplus \tilde{w_{jk}}).$$

Let $C_1, \ldots, C_{n_1}$ be criteria to assess likelihood and let $C_{n_1+1}, \ldots, C_n$ criteria to assess impact.

[Phase 2] Compute aggregated fuzzy ratings with respect of likelihood criteria for each threat. Specifically, the matrix $\tilde{L}$ of fuzzy ratings can be expressed as follows:

$$\tilde{L} = \begin{bmatrix} \tilde{x}_{11} & \tilde{x}_{12} & \ldots & \tilde{x}_{1n_1} \\ \tilde{x}_{21} & \tilde{x}_{22} & \ldots & \tilde{x}_{2n_1} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{x}_{m1} & \tilde{x}_{m2} & \ldots & \tilde{x}_{mn_1} \end{bmatrix}$$

where

$$\tilde{x_{ij}} = \frac{1}{k}(\tilde{x_{ij}}^1 \oplus \ldots \oplus \tilde{x_{ij}}^k)$$

is the aggregated fuzzy rating of alternative T_i with respect of criterion C_j where $\tilde{x_{ij}}^t$ is the rating by D_t of alternative T_i with respect of criterion C_j, for each $t = 1, \ldots, k$.

[Phase 3] Compute aggregated fuzzy ratings with respect to impact criteria for each threat. Specifically, for each $i = 1, \ldots, m$, $j = n_1 + 1, \ldots, n$, the matrix $\tilde{I}$ of fuzzy ratings can be expressed as follows:

$$\tilde{I} = \begin{bmatrix} \tilde{x}_{1n_1+1} & \tilde{x}_{1n_1+2} & \ldots & \tilde{x}_{1n} \\ \tilde{x}_{2n_1+1} & \tilde{x}_{2n_1+2} & \ldots & \tilde{x}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{x}_{mn_1+1} & \tilde{x}_{mn_1+2} & \ldots & \tilde{x}_{mn} \end{bmatrix}$$

where

$$\tilde{x_{ij}} = \frac{1}{k}(\tilde{x_{ij}}^1 \oplus \ldots \oplus \tilde{x_{ij}}^k)$$

is the aggregated fuzzy rating of alternative T_i with respect of criterion C_j where $\tilde{x_{ij}}^t$ is the rating by D_t of alternative T_i with respect of criterion C_j, for each $t = 1, \ldots, k$.

	Threat Category	**Threat Instance**
T1	Linkability	Infer a customer has a disease by linking his geolocation data with Point-of-Interest
T2	Information Disclosure	Exploit SQL Injection vulnerability to gain unauthorized access to database
T3	Non Compliance	Share geolocation data with a location-specific advertising company without user's consent

Table 4 Privacy Threats to Customer Database.

Likelihood Criteria	**DM1**	**DM2**	Aggregated Fuzzy Weight	Normalized Weight
C1: Attacker's Motivation	H	MH	(0.6,0.8,0.95)	0.21
C2: Attacker's Capabilities	H	H	(0.7,0.9,1.0)	0.23
C3: Attacker's Target	MH	M	(0.4,0.6,0.8)	0.16
C4: Vulnerability's Exploitability	MH	H	(0.6,0.8,0.95)	0.21
C5: Existing Security Controls	MH	MH	(0.5,0.7,0.9)	0.19
Data Controller's Impact Citeria	**DM1**	**DM2**	Fuzzy Weight	Normalized Weight
C6: Scale	H	H	(0.7,0.9,1.0)	0.15
C7: Financial Damage	H	VH	(0.8,0.95,1.0)	0.15
C8: Reputation Damage	MH	H	(0.6,0.8,0.95)	0.13
C9: Non-Compliance	H	H	(0.7,0.9,1.0)	0.15
Data Subject's Impact Criteria	**DM1**	**DM2**	Fuzzy Weight	Normalized Weight
C10: Type of Breached Data	M	H	(0.5,0.7,0.85)	0.11
C11: Ease of Identification	MH	H	(0.6,0.8,0.95)	0.13
C12: Loss of Confidentiality	H	H	(0.7,0.9,1.0)	0.15
C13: Loss of Integrity	ML	M	(0.2,0.4,0.6)	0.07
C14: Loss of Availability	M	M	(0.3,0.5,0.7)	0.08

Table 5 Importance Weight of Criteria.

[Phase 4] Defuzzify the fuzzy weights of the privacy criteria by using the signed distance. Specifically, for each $j = 1, \ldots, n$, the defuzzification of $\tilde{w_j} = (a_j, b_j, c_j)$ is computed as:

$$d(\tilde{w_j}) = \frac{1}{4}(a_j + 2b_j + c_j).$$

Moreover, for each $j = 1, \ldots, n$, the $j-th$ element w_j of the normalized weights vector $w = [w_1, w_2, \ldots, w_n]$ is computed as follows:

$$w_j = \frac{d(\tilde{w_j})}{\sum_{j=1}^{n} d(\tilde{w_j})}.$$

We denote $w_L = [w_1, \ldots, w_{n_1}]$ be the normalized vector of aggregated fuzzy weights with respect of the likelihood and $w_I = [w_{n_1+1}, \ldots, w_n]$ be the normalized vector of aggregated fuzzy weights with respect of impact.

[Phase 5] Apply linear normalization to both matrices $\tilde{L}$ and $\tilde{I}$ as shown in Section 3.3 to obtain normalized matrices $\tilde{L_N}$ and $\tilde{I_N}$.

[Phase 6] Compute the weights with respect of likelihood criteria by multiplying the matrix $\tilde{L}_N$ by the vector w_L^T which is the transposed vector of w_L.

[Phase 7] Compute the weights with respect of impact criteria by multiplying the matrix $\tilde{I}_N$ by the vector w_I^T which is the transposed vector of w_I.

Notice that the rating stage and the aggregate stage could be executed by different sets of experts. Moreover, being the criteria fixed, the weights associated to them during the rating stage could be used to perform more than one analysis.

Selection Stage. This stage consists of four phases:

[Phase 1] Compute the values of likelihood for each threat by adding all values related to each likelihood criterion.

Criteria	Threat	DM1	DM2
C1	T1	G	G
	T2	VG	VG
	T3	P	MP
C2	T1	VG	VG
	T2	VG	VG
	T3	F	MP
C3	T1	F	MG
	T2	VG	VG
	T3	F	P
C4	T1	P	MP
	T2	VG	VG
	T3	P	P
C5	T1	VP	P
	T2	G	VG
	T3	VP	VP
C6	T1	F	MG
	T2	VG	VG
	T3	F	MP
C7	T1	G	G
	T2	MG	G
	T3	VG	VG
C8	T1	P	P
	T2	VG	VG
	T3	G	G
C9	T1	G	G
	T2	G	MG
	T3	VG	VG
C10	T1	G	G
	T2	VG	VG
	T3	G	G
C11	T1	G	MG
	T2	VG	VG
	T3	F	MP
C12	T1	G	MG
	T2	VG	VG
	T3	P	MP
C13	T1	P	P
	T2	F	MP
	T3	VP	VP
C14	T1	VP	VP
	T2	F	F
	T3	P	VP

Table 6 Ratings of Customer's Database Threats Under All Criteria.

[Phase 2] Compute the values of impact for each threat by adding all values related to each impact criterion.

[Phase 3] Multiply the fuzzy values of likelihood and impact of each threat and obtain the deffuzified values by applying the signed distance method.

[Phase 4] Compare the results obtained to prioritize the threats according to their risks.

5 Case Study

In this section we illustrate the steps of our methodology for privacy risk assessment. We consider a realistic scenario where DriveSafe is an online car insurance company that offers pay as you go car insurance policies at competitive prices. In order to benefit from the pay as you go policy, customers have to install a smart device in their car that collects information about their driving. The smart device collects information like geolocation (GPS signal) and speed. This information is sent via satellite to the car insurance company's central servers where it is stored in a database along with other customer information such as its name and address and the credit card details used to pay the insurance premium. The customer information are not *pseudonymised* nor *encrypted* before being stored in the database. For the analysis we will focus on privacy threats targeting the database storing customer information. We have identified three main categories and instances of threats that are applicable to the database following the first three steps of the LINDDUN methodology introduced in Section 2. The threats are listed in Table 4. The company's owner hired two privacy analysts to assess possible privacy risks. Very recently a novel SQL injection vulnerability was reported. Thus, the two analysts, envisioning a concrete possibility of data breach, associate high weights to the likelihood criteria of capabilities and ease of exploiting with respect to threat $T2$. Similarly, the scale, the reputation damage as well as ease of identification and loss of confidentiality impact criteria weights for $T2$ are considered to be significant by both analysts. Indeed, since DriveSafe's assets include valuable information for attackers, it is likely that the vulnerability will be exploited if not patched, causing significant financial and reputation losses, as happened with the Equifax attack. The resulting data breach could also facilitate attackers on exploring other threats categories such as linkability. For instance, attackers can infer private and valuable information by linking costumer's geolocation data and their point of interest once such data has been licked. See threat $T1$ in Table 4 for a concrete example. For the reasons above, it is reasonable to expect that $T2$ is the threat with the highest level of risk.

In the following we denote with D_1 and D_2 the two analysts (decision makers). Their opinions will be collected in order to prioritize the identified threats. Then, the three stages described in section 4.2 will be followed at the extent of first characterizing the likelihood and the impact of each threat and, subsequently, computing the corresponding level of risk. In the following we illustrate the three stages in details:

	C1	C2	C3	C4	C5
T1	(7,9,10)	(9,10,10)	(4,6,8)	(0.5,2,4)	(0,0.5,2)
T2	(9,10,10)	(9,10,10)	(9,10,10)	(9,10,10)	(8, 9.5,10)
T3	(0.5,2,4)	(2,4,6)	(1.5,3,5)	(0,1,3)	(0,0,1)

Table 7 Aggregated ratings with respect of likelihood criteria.

	C6	C7	C8	C9	C10	C11	C12	C13	C14
T1	(4,6,8)	(7,9,10)	(0,1,3)	(7,9,10)	(7,9,10)	(6,8,9.5)	(6,8,9.5)	(0,1,3)	(0,0,1)
T2	(9,10,10)	(6,8,9.5)	(9,10,10)	(6,8,9.5)	(9,10,10)	(9,10,10)	(9,10,10)	(2,4,6)	(3,5,7)
T3	(2,4,6)	(9,10,10)	(7,9,10)	(9,10,10)	(7,9,10)	(2,4,6)	(0.5,2,4)	(0,0,1)	(0,0.5,2)

Table 8 Aggregated ratings with respect of impact criteria.

Rating Stage. This stage consists of four phases:

[Phase 1] Decision-making opinions are collected to assess criteria importance in estimating the likelihood and the impact of privacy threats.

[Phase 2] Importance of criteria are assessed by using linguistic weighting variables in Table 2 as shown in Table 5.

[Phase 3] Performance of alternatives (i.e. threats) with respect of each criterion is assessed utilizing linguistic weighting variables in Table 3 as shown in Table 6.

[Phase 4] Opinions expressed in linguistic terms are converted in fuzzy numbers according to Table 2 and Table 3.

Aggregation Stage. This stage consists of seven phases:

[Phase 1] Compute aggregated fuzzy weights of individual criterion.
Specifically, let $\tilde{w_{jt}} = (a_{jt}, b_{jt}, c_{jt})$, where $j = 1, \ldots, n$ and $t = 1, 2$ be the weights associated to the criterion C_j by decision maker D_t, then the aggregate fuzzy weight for criteria C_j is computed as

$$\tilde{w_j} = (a_j, b_j, c_j) = \frac{1}{2}(\tilde{w_{j1}} \oplus \tilde{w_{j2}})$$

as shown in Table 5.

[Phase 2] Compute the matrix of aggregated fuzzy ratings with respect of likelihood criteria as shown in Table 7.

[Phase 3] Compute the matrix of aggregated fuzzy ratings with respect of impact criteria as shown in Table 8.

[Phase 4] First defuzzify the fuzzy weights of the privacy criteria by using the signed distance and then compute the normalized values as shown in Table 5.

	T1	T2	T3
C1	(0.7,0.9,1)	(0.9,1,1)	(0.05,0.2,0.4)
C2	(0.9,1,1)	(0.9,1,1)	(0.2,0.4,0.6)
C3	(0.4,0.6,0.8)	(0.9,1,1)	(0.15,0.3,0.5)
C4	(0.05,0.2,0.4)	(0.9,1,1)	(0,0.1,0.3)
C5	(0,0.05,0.2)	(0.8,0.95,1)	(0,0,0.1)

Table 9 Normalized fuzzy matrix with respect of Likelihood criteria.

	T1	T2	T3
C6	(0.4,0.6,0.8)	(0.9,1,1)	(0.2,0.4,0.6)
C7	(0.7,0.9,1)	(0.6,0.8,0.95)	(0.9,1,1)
C8	(0,0.1,0.3)	(0.9,1,1)	(0.7,0.9,1)
C9	(0.7,0.9,1)	(0.6,0.8,0.95)	(0.9,1,1)
C10	(0.7,0.9,1)	(0.9,1,1)	(0.7,0.9,1)
C11	(0.6,0.8,0.95)	(0.9,1,1)	(0.2,0.4,0.6)
C12	(0.6,0.8,0.95)	(0.9,1,1)	(0.05,0.2,0.4)
C13	(0,0.16,0.5)	(0.3,0.6,1)	(0,0,0.16)
C14	(0,0,0.14)	(0.4,0.7,1)	(0,0.07,0.2)

Table 10 Normalized fuzzy matrix with respect of Impact criteria.

	T1	T2	T3
C1	(0.15,0.19,0.21)	(0.19,0.21,0.21)	(0.01,0.04,0.08)
C2	(0.20,0.23,0.23)	(0.20,0.23,0.23)	(0.04,0.09,0.13)
C3	(0.06,0.09,0.12)	(0.14,0.16,0.16)	(0.02,0.04,0.08)
C4	(0.01,0.04,0.08)	(0.18,0.21,0.21)	(0,0.02,0.06)
C5	(0,0,0.03)	(0.15,0.18,0.19)	(0,0,0.01)

Table 11 Weighted normalized matrix with respect of Likelihood criteria.

	T1	T2	T3
C6	(0.06,0.09,0.12)	(0.13,0.15,0.15)	(0.03,0.06 0.09)
C7	(0.10,0.13,0.15)	(0.09,0.12,0.14)	(0.13,0.15, 0.15)
C8	(0,0.01,0.03)	(0.11,0.13,0.13)	(0.09,0.11,0.13)
C9	(0.10,0.13,0.15)	(0.09,0.120.14)	(0.13,0.15,0.15)
C10	(0.07,0.09,0.11)	(0.09,0.11,0.11)	(0.07,0.09, 0.11)
C11	(0.07,0.10,0.12)	(0.11,0.13,0.13)	(0.02,0.05, 0.07)
C12	(0.09,0.12,0.14)	(0.13,0.15,0.15)	(0.007,0.03, 0.06)
C13	(0,0.01,0.03)	(0.02,0.04,0.07)	(0,0,0.01)
C14	(0,0,0.011)	(0.03,0.06,0.08)	(0,0.006,0.022)

Table 12 Weighted normalized matrix with respect of Impact criteria.

	Fuzzy Likelihood	Fuzzy Impact	Risk Level
T1	(0.42,0.56,0.69)	(0.5,0.7,0.8)	(0.2,0.4,0.6)
T2	(0.88,0.99,1)	(0.8,1,1)	(0.7,0.99,1)
T3	(0.08,0.2,0.38)	(0.47,0.64,0.97)	(0.03,0.12,0.36)

Table 13 Fuzzy likelihood values, fuzzy impact values, and fuzzy level of risk per threat.

[Phase 5] Linear normalization is applied to both the matrix of fuzzy ratings with respect of likelihood criteria and the matrix of fuzzy ratings with respect of impact criteria. The resulting matrices are shown in Table 9 and 10. Notice that all criteria in our example are benefit criteria.

[Phase 6] The normalized weighted matrix with respect of likelihood criteria is represented in Table 11.

[Phase 7] The normalized weighted matrix with respect of impact criteria is represented in Table 12.

Selection Stage. This stage consists of four phases:

[Phase 1] Compute the values of likelihood of each threat by adding all values related to each likelihood criterion. These values are shown in Table 13.

[Phase 2] Compute the values of impact of each threat by adding all values related to each impact criterion. These values are shown in Table 13.

[Phase 3] Multiply the fuzzy values of likelihood and impact of each threat to obtain their level of risk (see Table 13). Then compute deffuzified values by applying the signed distance method (see Table 13).

[Phase 4] Consider the results obtained to prioritize the threats. Our methodology shows that $T2$ and $T3$ are respectively the threats with the highest and lowest level of risk (see Table 14) confirming our original hypothesis.

	Risk Level	Defuzz. Value
T2	(0.7,0.99,1)	0.92
T1	(0.2,0.4,0.6)	0.4
T3	(0.03,0.12,0.36)	0.15

Table 14 Fuzzy value and defazzification value of the level of risk per threat.

6 Conclusions

A Data Protection Impact Assessment (DPIA) is a process that helps organization to identify, assess and minimize the data protection risks of their data processing activities. However, the existing DPIA methodologies do not provide an effective solution to assess and prioritize privacy risks because they rely upon an analyst to rate the impact and likelihood of the risks.

In this paper we have proposed a set of well-defined criteria that analysts can use to measure the likelihood and the impact of a privacy risk. Then, we adopt the fuzzy multi-criteria decision-making approach to systematically measure the severity of privacy risks while modeling the imprecision and vagueness inherent in linguistic assessment. Our realistic case study, inspired by the real scenario in which the Equifax attack took place, provides a proof of concept that our methodology is appropriate for prioritizing privacy risks. We leave as future work the investigation about different ways of evaluating the proposed methodology such as comparing the effectiveness of our approach with other multi-criteria decision making techniques such as analytic hierarchy process (AHP). We also plan to explore the use of multi-criteria decision making approaches to select alternative organizational and technical measures to address the highest privacy risks.

7 Compliance with Ethical Standards

Funding: There is no source of funding available for this research work.

Conflict of Interest: Authors declare that they have no conflict of interest.

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. AEPD: Guia Practica de Anlisis de riesgos en los tratamientos de datos personales sujetos al RGPD) (2017). https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf
2. Awasthi, A., Chauhan, S.S., Goyal, S.K.: A multi-criteria decision making approach for location planning for urban distribution centers under uncertainty. Mathematical and Computer Modelling **53**(1-2), 98–109 (2011)
3. Camarinha-Matos, L.M., Falcão, A.J., Vafaei, N., Najdi, S. (eds.): Technological Innovation for Cyber-Physical Systems - 7th IFIP WG 5.5/SOCOLNET Advanced Doctoral Conference on Computing, Electrical and Industrial Systems, DoCEIS 2016, Costa de Caparica, Portugal, April 11-13, 2016, Proceedings, *IFIP Advances in Information and Communication Technology*, vol. 470. Springer (2016)
4. Caralli, R., Stevens, J., Young, L., Wilson, W.: Introducing octave allegro: Improving the information security risk assessment process. Tech. rep. (2007)
5. CNIL: Privacy Impact Assessment Methodology (2018). https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf
6. De Gusmao A., Camara L., Silva M., Poleto T., Costa A.: Information security risk analysis model using fuzzy decision theory. International Journal of Information Management **36**, 25–34 (2016)
7. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requir. Eng. **16**(1), 3–32 (2011)
8. ENISA: Recommendations for a methodology of the assessment and severity of personal data breaches (2013). https://www.enisa.europa.eu/publications/dbn-severity
9. ICO: Data Protection Impact Assessment (DPIA)) (2017). https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/
10. Kahraman, C., Onar, S.Ç., Öztaysi, B.: Fuzzy multicriteria decision-making: A literature review. Int. J. Comput. Intell. Syst. **8**(4), 637–666 (2015). DOI 10.1080/18756891.2015.1046325. URL https://doi.org/10.1080/18756891.2015.1046325
11. Lund, M.S., Solhaug, B., Stlen, K.: Model-Driven Risk Analysis: The CORAS Approach. Springer Publishing Company, Incorporated (2010)
12. Moore, T.: On the harms arising from the equifax data breach of 2017. Int. J. Crit. Infrastruct. Prot. **19**(C), 47–48 (2017). DOI 10.1016/j.ijcip.2017.10.004. URL https://doi.org/10.1016/j.ijcip.2017.10.004
13. North Rhine-Westphalia State Commissioner for Data Protection and Freedom of Information: The Standard Data Protection Model(SDM) (2017). https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.*pdf*
14. OWASP: OWASP Top 10 Privacy Risks (2014). https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project
15. OWASP: OWASP Risk Rating Methodology (2018). https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
16. Shameli-Sendi A., Shajari M., Hassanabadi M., Jabbarifar M., Dagenais M.: Fuzzy multi-criteria decision making for information security risk assessment. Open Cybernetics and Systemics Journal **6**, 26–37 (2012)
17. Stoneburner, G., Goguen, A.Y., Feringa, A.: Sp 800-30. risk management guide for information technology systems. Tech. rep., Gaithersburg, MD, United States (2002)
18. Wagner, I., , Boiten, E.: Privacy risk assessment: From art to science, by metrics. pp. 225–241 (2018)
19. WP29: Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) (2017). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
20. Wuyts, K., Scandariato, R., Joosen, W.: Empirical evaluation of a privacy-focused threat modeling methodology. The Journal of Systems Software **96**, 122–138 (2014)
21. Zadeh, L.A.: Fuzzy sets. Information and Control **8**(3), 338–353 (1965)