TrustE-VC: Trustworthy Evaluation Framework for Industrial Connected Vehicles in the Cloud

Mohammad N. Aladwan, Feras M. Awaysheh, Sadi Alawadi, Mamoun Alazab, Tomás F. Pena and José C. Cabaleiro

Version: accepted article

TrustE-VC: Trustworthy Evaluation Framework for Industrial Connected Vehicles in the Cloud

Mohammad N. Aladwan, Feras M. Awaysheh, Mamoun Alazab, Sadi Alawadi, Tomás F. Pena, and José C. Cabaleiro.

Abstract—The integration between cloud computing and vehicular ad hoc networks (VANETs), namely, vehicular clouds (VCs), has become a significant research area. This integration was proposed to accelerate the adoption of intelligent transportation systems. The trustworthiness in VCs is expected to carry more computing capabilities that manage large-scale collected data. This trend requires a need for a security evaluation framework that ensures data privacy protection, integrity of information, and availability of resources. To the best of our knowledge, this is the first study that proposes a robust trustworthiness evaluation of vehicular cloud (TrustE-VC) for security criteria evaluation and selection. This paper proposes three-level security features in order to develop effectiveness and trustworthiness in VCs. To assess and evaluate these security features, our evaluation framework consists of three main interconnected components: (i) an aggregation of the security evaluation values of the security criteria for each level, (ii) a fuzzy multicriteria decision-making algorithm, and (iii) a simple additive weight associated with the importance-performance analysis and performance rate to visualize the framework findings. The evaluation results of the security criteria based on the average performance rate and global weight suggest that data residency, data privacy, and data ownership are the most pressing challenges in assessing data protection in a VC environment. Overall, this paper paves the way for a secure VC using an evaluation of effective security features and underscores directions and challenges facing the VC community. The paper sheds light on the importance of security by design, emphasizing multiple layers of security when implementing industrial VCs.

Index Terms—Industrial Connected Vehicles, Vehicular Clouds, Security Analysis, Decision making, Industrial Internet of Things, Security by Design

1 Introduction

The vast amount of data generated by the Internet of Things (IoT), especially VANETs (vehicular ad hoc networks), needs a scalable resource, which can be provided by cloud computing on a rental basis. Accordingly, the cloud has attracted the most significant interest in IoT-based applications [1], [2], particularly vehicular clouds (VCs) [3]. The transmitted data in such a realm should be located securely throughout the whole life cycle to guarantee high data privacy. Security is a crucial aspect of spreading the adoption of cloud capabilities among industrial connected vehicles (CVs) [4] and industrial cyber-physical systems [5], [6]. In this regard, security by design can mitigate many of these imposed challenges [7]. Without adequately addressing this concern, a VC would not gain the clients' trustworthiness and, hence, acceptance. This facility can be achieved by regularly evaluating the security components of the VC to put together an adequate plan of improvement. However, a dedicated work that evaluates the trustworthiness of this framework remains an open challenge.

When a cloud-based connected vehicle system is realized, significant security concerns should be considered [8], [9], [10]. Security features (criteria) are not equal, which means that they should not be governed and managed at the same level. It is essential to note the importance of creating a shared understanding of security-related criteria and be able to assign priorities based on each security criteria impact and potential for mitigation. These considerations include security by design of the system and utilization of underlying security technologies and services. This research captures security services used in industrial CVs that describe the VC security items and relationships among them. It also presents landscape techniques to define security gaps (distance from an ideal point of security) and best practices. This work aims at facilitating the realization of vehicles securely connected to cloud computing in an industrial environment. First, we analyze the security criteria of data analytics in VC computing and propose three-level security evaluation elements. Namely, Level 1 consists of 6 common security criteria (CSCs). Level 2 consist of 10 security control components (SCCs). Level 3 consist of 36 security control subcomponents (SCSs). Next, the framework uses the proposed security criteria as a measure to comprehensively evaluate and rank the security criteria using a multicriteria decision-making algorithm. Finally, the framework proposes to compare the evaluated criteria to an ideal level and report (visualize) the evaluation results in order to update the security by design.

Deploying a secure industrial IoT solution has only been recently proposed to provide security analysis and mitigate vulnerabilities at the design/modeling phase [7]. However, this proposal did not offer a practical solution for optimizing

This work was supported by the Ministry of Education, Culture, and Sport, Government of Spain (Grant Number TIN2016-76373-P), the Xunta de Galicia (accreditation 2016–2019, ED431G/08, and ED431C 2018/2019), and the European Union (European Regional Development Fund—ERDF).

M. N. Aladwan, F. M. Awaysheh, T. F. Pena, and J. C. Cabaleiro are with the Centro Singular de Investigación en Tecnoloxías Intelixentes (CiTIUS), University of Santiago de Compostela, Spain (e-mail: m.alseran@gmail.com; feras.awaysheh@usc.es; tf.pena@usc.es; jc.cabaleiro@usc.es)

S. Alawadi is with the department of Computer Science and Media Technology - Internet of Things and People (IOTAP) Research Center, Malmö University, Sweden (e-mail: sadi.alawadi@mau.se)

Mamoun A. Alazab is with the College of Engineering, IT and Environment, Charles Darwin University, Australia (e-mail:alazab.m@ieee.org.)

the design phase by evaluating the system security features as this study does. Additionally, this study copes with the previous limitation and aids in better security updates and patches at the runtime/simulation phase. The proposed methodological approach combines the use of criteria importance and performance rates for determining trust service attributes that a designer or policy maker should devote more attention to. It also labels which feature should be lower priority to keep the focus on the high-priority ones. Trustworthiness evaluation of vehicular cloud (TrustE-VC) offers a useful and practice-ready tool for designers and industrial CV practices to better evaluate and select industrial CV trust requirements.

The remainder of this paper is organized as follows. Section 2 provides the background of this article along with the underlying motivation. A discussion of the proposed framework (TrustE-VC) and its main components is presented in Section 3. Section 4 highlights the TrustE-VC framework outputs and results that need to be addressed within the next-generation industrial CV and IoV-cloud platforms. Related work is presented in Section 6. Finally, we conclude our paper in Section 7.

2 Background

The focus on significant requests for sensitive data allocated from various sources drives us to pay more attention to data security [11]. These confidential data can reside near the device (on the edge/fog side) or in the cloud. This implies that the data can be attacked during transmission or at their site. Data security and privacy are considered to be main barriers for full acceptance of the IoT paradigm [12]. Most security threats and extensive privacy issues stem from the lack of well-investigated security and privacy guidelines. However, these guidelines and security requirements (confidentiality, integrity, availability, privacy, audibility, accountability, and trustworthiness) will give the IoT stakeholders the vision to build secure IoT systems during the design phase, which aims to enhance IoT data security and privacy and prevent data scams [13].

2.1 Vehicle-to-Cloud Connection

VC technology relies on vehicles' onboard computing capabilities, storage, and sensing power and leverages cloud computing services. Cloud computing represents a practical model that supports the scalable deployment of management of large-scale collected data on the edge of the network with a cost-effective and sophisticated approach of storing and processing big datasets. In this context, the security of vehicle-to-cloud data exchange and communication is a first-class concern among industrial CV practitioners. Overall, Figure 1 illustrates the major layers associated with the industrial CV ecosystem, such as the connected vehicle layer, edge/fog support service layer, and cloud service delivery layer [14]. In such an architecture, the data life cycle is composed of several stages, with the data flowing from sensors and smart objects to the cloud. It begins with data generation (e.g., collected from vehicles and IoV infrastructure) by different objects, where connection security is required. The allocated data are then assembled (using compression and aggregation) and transferred to edge IT and the cloud. Following this, metadata are reserved, and the data are kept in the cloud storage within a data lake, which can be multitenant storage serving several applications.

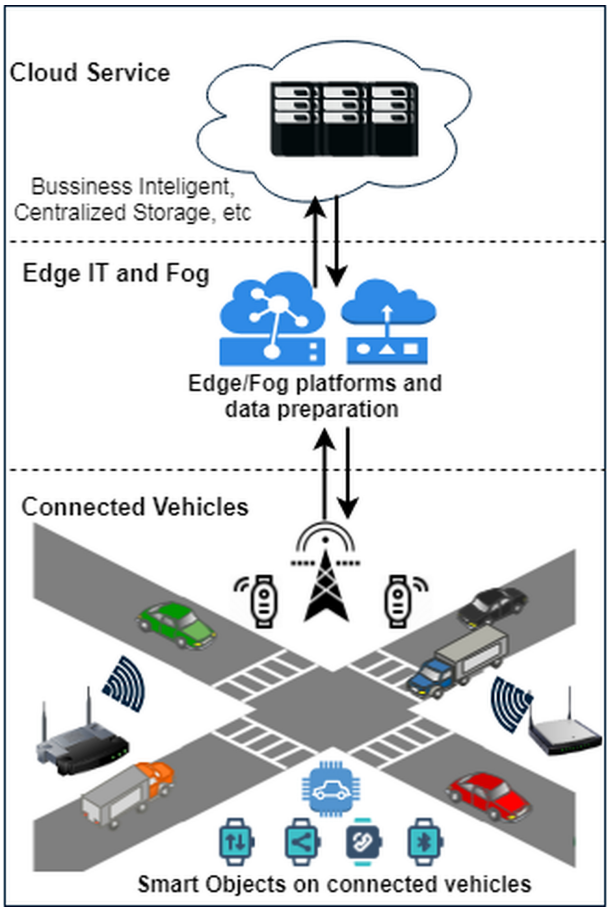


Fig. 1: Abstracted layers of connected vehicles with the cloud paradigm.

In the same context, the data life cycle flows among different VC service layers [15]. First, at the data generation point (very bottom) is the sensor mesh network, named *object and communication abstraction*, which comprises physical smart devices such as sensors [16]. This layer includes hardware and firmware that provide car–to–car and car–to–infrastructure (defined earlier as V2V and V2I) connectivity using different communication technologies such as Bluetooth and WiFi. Subsequently, with the vast number of IoV devices spawning data, the storage and computation of these data will take place on the cloud. Hence, different applications can harness it to make valuable decisions. It is worth mentioning that some applications utilize stream data processing on the edge nodes (also including fog deployments) such as traffic ahead or parking nearby. Finally, VC systems grant end users applications in an SaaS layer (e.g., machine learning and ITS). These applications, however, leverage the services and functionalities of the lower cloud service layer. Based on an analysis of these applications, users and administrators can remotely send commands to smart devices at the bottom layer. Supporting the architecture security involves several approaches, from

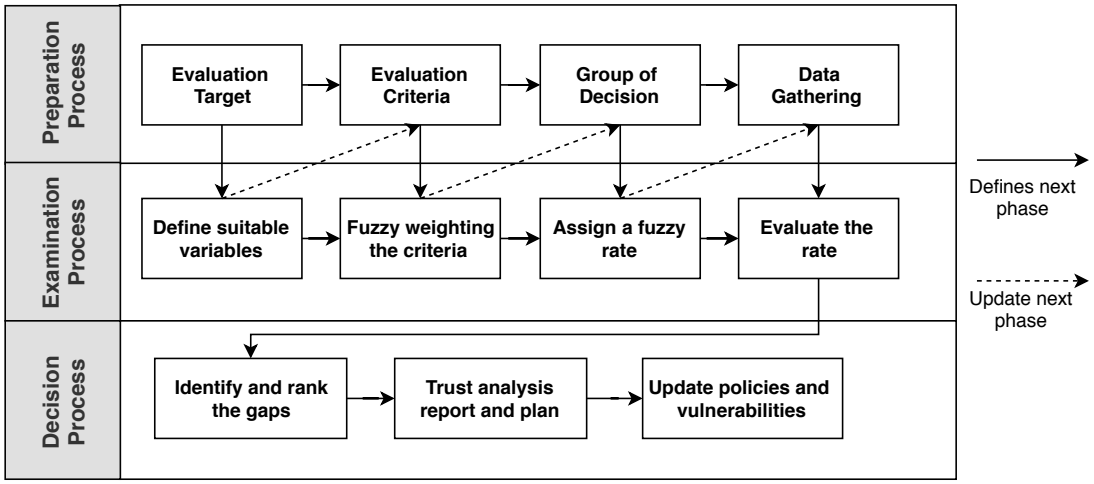


Fig. 2: Context-based pattern matching for a trust by design of TrustE-VC framework

physical and network security to edge and cloud platform security. It also includes framework and application security, security analytics (e.g., behavioral analysis, data flow analysis, Trojan detection, etc.) and continuous security testing — in addition to identification and access management, such as authentication and authorization.

2.2 The necessity of VC security evaluation

The Internet of Vehicles (IoV) in the cloud paradigm represents a responsibility transfer of data hosting, software control, and infrastructure management [17], [18]. IoV implementers are always seeking to secure their operational environments, as security is always a first concern. On the other hand, cloud providers improve their competitiveness in the cloud market by ensuring that appropriate security expectations for their services are met. Security engineering (planning, designing, and assessment) that minimizes the vulnerability surface and meets clients' security satisfaction is expected. However, it is challenging to meet these expectations unless they are based on the results of systematic gap analysis and assessment. This analysis could aid in evaluating the security level of every component individually as well as their integration. Evaluating the security level of a VC system enables the suggestion of an efficient and effective plan that maximizes the security and minimizes the level of risk to an acceptable level. Consequently, VC practitioners identify the unimproved gaps and have a clear sense of the system security level and how to address the challenges.

IoV-to-cloud security evaluation aids in shaping the security policy of the service provider as follows:

Achieve client satisfaction: Based on the security evaluation, the VC provider will provide adequate information regarding service enhancements to achieve the client's highest level of satisfaction. A security evaluation report will reduce the vulnerabilities among the system components by allowing the security designers to control undesirable behavior. Additionally, it will improve the security level and reduce the risk to the clients' satisfaction.

Improve VC services: A security evaluation can lead to a significant enhancement in the system security that sustains its adoption by the clients. It can also guide service providers to improve their service, in addition to determining and meeting the client's requirements. This information will assist VC providers in establishing a new service level that can meet IoV needs.

Gain competitive advantages: The intelligent industrial CV business is rapidly growing. A competitive and growing market share is vital for the industry. By providing a detailed report on the service security status by conducting a security evaluation, customers can be reassured regarding the security measures that maintain their data privacy and confidentiality. This report, in return, leads to competitive advantages. High rates on a security evaluation after classifying the standard security criteria improve the system reliability in the market. Therefore, industrial CV providers could use this information to convince potential customers.

3 VC Security Evaluation Framework

Defining the evaluation criteria is crucial to evaluating the performance parameters of the target system (i.e., VC). In this section, diagrammatic VC security levels are proposed in Table 1. These levels are used to assess the VC and then identify the unimproved gaps for further enhancements. In total, this study proposes 52 different evaluation metrics. Namely, six are in level 1, ten in level 2, and thirty-six in level 3. Level 1, namely, common security criteria (CSCs), are hierarchically divided into 10 security control components (SCCs) in level 2. Those SCCs are broken down into 3 specific security control subcomponent (SCS) techniques in level 3. The final aim of this table is to provide a unified benchmark (evaluation criteria) to evaluate the security of VC services within any proposed solution.

The TrustE-VC methodology contains a sequence of structured processes, which are described using well-defined activities (i.e., inputs and outputs). In Figure 2, we propose a matching methodology for instantiating trust requirements in a context pattern (structural descriptions) of the VCs. The main processes of this method include preparation, examination, and decision. The preparation stage starts with identifying the evaluation target (with suitable variables) and describing objects that are subject

TABLE 1: Diagrammatic Vehicular Cloud Security Level in Industrial Connected Vehicles

CSC	SCC	SCS
Physical and Environmental Protection (C1)	Infrastructure Security Design (C13)	-Physical access control rights and roles (C131) -Multiple barriers to physical access (C132) -Monitoring physical access (C133) -Lockable physical casings (C134) -Disaster and incident management (C135) -Mirroring and redundancy of the infrastructure (C136)
	Network Security Design (C11)	-Communication channels security (C111) -Network security design (C112) (segmentation and isolation). -Malicious insiders (C121) -Firmware security (C122)
	Smart Object, Sensor, and Actuator Security (C12)	
Logical Access Control (C2)	Authentication (C22)	-LDAP-based and Kerberos protocol (C221) -Third party approach (C222) -Dual-stage authentication (C223) (mesh network and edge) -Smart object access control rights and roles (C224)
	Authorization (C21)	-Identity access policies (C211) -Penetration testing (C212)
Communication Confidentiality (C3)	Wire Encryption (C31)	-Multiple-level encryption (C311) -Blockchain encryption (C312) -Transparent data encryption (C313) -End-to-end wire encryption(C314) -Identity-based encryption and attribute-based encryption(C315) -Data privacy (C316)
Communication Integrity (C4)	Communication Integrity (C41) (objects and edge/cloud computation)	-Data transmission protection (C411), e.g., SSL/TLS protocol -System vulnerabilities/exploitable bugs (C412) -Data and wire encryption (C413) -Hardware compatibility (C414) -Monitoring production environment (C415) -Scalability and compatibility(C416)
Data and Service Availability (C5)	Data Availability (C52) Service Availability (C51)	-Data replication (C521) -Failure history and recovery (C511) -Redundancy of disasters and incidents (C512)
Data Privacy and Governance (C6)	Data Privacy and Governance (C61)	-Behavioral analytics and monitoring (C611) -Managing service/operation log information and file (C612) -Tagging (data labeling for governance) and filtering (C613) -Automation of service (C614) -Compliance with legalization (C615) (data and software) - Compliance with SLA (C616).

to evaluation. Evaluation criteria point out the characteristics and constraint parameters of this target by weighting these criteria (optimal weight vector of the criteria). These evaluation criteria are further aggregated and associated with a group of decisions to obtain the collective trust weight and start the data gathering (of the available solution domain), which evaluates the rates of each criterion. This aggregation must be assigned a fuzzy rate of fuzzy best and worst values to be evaluated properly [19]. Based on the evaluation results, the correlation among the criteria weight and ideal point (the security gap) is scored and rated. In other words, evaluate the normalized fuzzy difference to evaluate the fuzzy index value. This score can be utilized to report particular pieces of information and prepare a mitigation plan that, eventually, updates any security breach or vulnerability by determining the rank of the trust criteria mode.

Our evaluation framework is composed of three main components to assist with the security gaps of a typical VC environment: (1) Aggregation of the evaluation values of the security levels, i.e., SCCs and SCSs in the decision-making method (group decision makers (GDMs)), is proposed. Evaluation of the security level of the industrial CV based on a singular perception framework (one DM) can return poor decisions [20]. Hence, to acquire a reasonable resolution, the use of GDMs is a suitable and relevant approach to knowledge synthesis and collection. In [20], the authors' results obtained from GDMs are more objective, as they combine different experiences and views. (2) Fuzzy set theory and fuzzy aggregation techniques are used to evaluate the security level of industrial CV criteria according to the GDMs as a fuzzy multicriteria decision-making (MCDM) approach. (3) Simple additive VIKOR associated with the performance analysis and performance rate is used to visualize the framework findings, as proposed in [21].

3.1 Multicriteria Group Decision Making

To evaluate security solutions in a VC system using several components, we have to assess all of its criteria. Usually, any computing system cannot function well with all evaluation criteria, and hence, the investigator or security analyst has to map the trade-off among them. This is especially relevant within large-scale architectures as in a typical industrial CV. Evaluating and selecting the best security criteria tuning is the primary goal of our framework. Herein, we propose a multidecision algorithm that feeds the fuzzy ranking model of our proposed evaluation framework.

Next, we review some concepts regarding realization of the preliminaries of the criterion space, fuzzy set theory, and the decision making approach, which combined represent the basic principle of our proposed framework.

1) Representing the criterion space:

$$\max i; \quad \text{subject to} \quad i \in I \tag{1}$$

where i is the vector of **Y** criteria and I is the feasible set, $I \subseteq GY$. If G is defined explicitly (a set of choices), the result is called a multiple-criteria (MC) analysis. If I is defined implicitly (by a set of constraints), the result named an MC process.

2) Representing the fuzzy sets:
To present the main concepts of fuzzy sets that link elements to define their membership to a function, which is usually [0,1], the membership degree is generally a figure (special fuzzy set), where χ & pick rate on the real line, and $\tilde{q}((\chi))$ is a continuous mapping of U to the closed rate in the interval [0,1] as follows:

$$\tilde{q} = (\chi, \bar{q}(\chi)), \chi \in U \tag{2}$$

3) Representing the decision making:

The decision-making process matches criteria to a set of potential decisions accessible to the security designers and analytics. The criteria weight are the values of the security evaluation. Hence, investigators set identical security metrics in the decision model based on the specified security criteria. For example, when designing and implementing a VC solution, the implementer chooses the design parameters (security criteria). Each of these influences the security measures that evaluate the system components. Mathematically, an evaluation framework can be described as shown below:

$$\begin{aligned} &\max i = f(e) = f(e_1, \ldots, e_n) \\ &\text{subject to}, e \rightarrow E; \text{ as follows:} \\ &i \in I = f(e) : e \in E, E \subseteq I^n \end{aligned} \tag{3}$$

where E is the feasible set, and e is the decision variable vector of size n. A well-developed specific case is achieved when E is a polyhedron defined by linear inequalities and qualities. Different definitions are fundamental in **TrustE-VC**; these are closely linked to the nondominance and efficiency defined based on both space and variable representations.

Definition 1: if there exists $e^* \in E$, then $e^* \in E$ is not dominated when $e \geq e^*$ and $e \neq e^*$.

Definition 2: $e^* \in E$ is efficient if there does not exist another $e \in E$ such that $f(e) \geq f(e*)$ and $f(e) \neq f(e*)$. A key factor for a successful **evaluation framework** is a good representation of the decision situation by a problem domain.

Definition 3: if there does not exist another $i \in I$ where $i > I^*$, then we can say that $i^* \rightarrow I$ is weakly nondominated.

Definition 4: if there does not exist another $e \in E$ such that $f(e) > f(e^*)$, then $e^* \rightarrow E$ is weakly efficient as well, including all nondominated and some other particular points.

These unique points appear in practice, which makes them vital. Moreover, it is essential to distinguish them from nondominated points. To illustrate this case, consider that we maximized a particular objective, i.e., security criteria. Doing so may return a weakly nondominated point that is dominated. The dominated points of the weakly nondominated set are located either on vertical or horizontal planes (hyperplanes) in the criterion space.

Ideal point: shows the highest (the best for the maximization weight) of each criteria and compares favorable to an unfeasible decision.

Nadir point: shows the lowest (the worst for the maximization weight) of each criteria among the evaluation set. The ideal point and the nadir point are useful in the **evaluation process** to obtain the "quality" of the range of solutions.

Algorithm 1 illustrates our evaluation framework approach. Furthermore, it can indeed be realized by a GDM model that feeds the fuzzy ranking model of our proposed framework. Mathematically, problems corresponding to the above arguments can be represented as the following formal definitions:

By defining the most suitable ϕ^* and the worst $\widehat{\phi}$ values of all values of all test criteria, $i = 1, 2, \ldots, n$, $\phi^* = \max(\phi_j, j = 1, \ldots, J)$ and $\widehat{\phi} = \min(\phi_j, j = 1, \ldots, J)$

Algorithm 1: Multidecision approach for weighting security criteria in the VC framework

Require: Criterion functions $f(y)_i$
Determine best ϕ_i^* and worst $\widehat{\phi}_i$ values $\forall \quad f(y)_i$;
if i^{th} *function represents a benefit* **then**
  $\phi^* = \max(\phi_j)$, $\widehat{\phi} = \min(\phi_j)$
else
  $\phi^* = \min(\phi_j)$, $\widehat{\phi} = \max(\phi_j)$
end
Compute both values S_j and R_j.
Calculate the comprehensive sorting index I_j
Rank the fuzzy values R, S and I in ascending order.
Select the $\min(I_j)$ that represent the best ranked; the alternative $A^{(1)}$ is proposed as a compromise solution.
if $C1$ *is Acceptable advantage* **then**
  $I(A^{(2)}) – I(A^{(1)}) \geq \frac{1}{m-1}$, where $A^{(2)}$ is the alternative with the second position in the ranking list by I.
end
if $C2$ *is Acceptable stability in decision making* **then**
  The alternative $A^{(1)}$ must also be the best ranked by T or/and S.
end

if the i^{th} function is a benefit, whereas $\phi^* = \min(\phi_j, j = 1, \ldots, J)$ and $\widehat{\phi} = \max(\phi_j, j = 1, \ldots, J)$ if the i^{th} function is a cost.

Here, $S^* = \min(S_j), j = 1, \ldots, J, \widehat{S} = \max(S_j, j = 1, \ldots, J), R^* = \min(R_j), j = 1, \ldots, J$, and $\widehat{R} = \max(S_j, j = 1, \ldots, J)$. Eq. 5 is used to compute the group utility S_j, which is used to normalize the distance, and Eq. 4 is used to calculate the individual regret R_j in order to normalize the Chebyshev distance.

$$T_j = \sum_{i=1}^{n} w_i \left(\frac{\phi^* - \phi_j}{\phi^* - \widehat{\phi}}\right) \tag{4}$$

$$S_j = \max\left[w_i \left(\frac{\phi^* - \phi_j}{\phi^* - \widehat{\phi}}\right)\right] \tag{5}$$

Then, the comprehensive sorting index I_j is computed using the following equation:

$$I_j = v\left(\frac{S_j - T^*}{\widehat{T} - T^*}\right) + (1 - v)\left(\frac{S_j - S^*}{\widehat{S} - S^*}\right) \tag{6}$$

where $j = 1, 2, \ldots J$, $R^* = \min(R_j)$, $\widehat{R} = \max(R_j)$, $S^* = \min(S_j)$ and $\widehat{S} = \max(S_j)$.

is introduced as a weight for the strategy of maximum group utility, whereas $1 - v$ is the weight of the individual regret. A compromise between these strategies could be reached by setting $v = 0.5$, and here, v is modified as $\frac{(n+1)}{2n}$ (from $v + 0.5\frac{(n-1)}{n} = 1$) since the criterion (1 of n) related to R is also included in S.

3.2 Fuzzy Set Theory Modeling

Due to the subjectivity of the anonymous values of the security criteria, the evaluation of the security level of industrial CV is imprecise and arguably vague. This imprecision issue requires novel decision-making approaches that address the subjective evaluations. Fuzzy set theory has been proposed as a pioneering solution, which aids in different areas [22]. In this study, we employed this theory to express and manage ambiguity in decision making. The linguistic variables in the fuzzy theory (e.g., very high, very low, low, and high) can afford a powerful connection tool—by assigning a numerical variable within a binary set (0,1). These linguistic variables effectively model the vagueness or fuzziness inherent in decision-making problems [20].

In this research, we utilized the fuzzy triangular numbers [23] that describe linguistic variables connected with a membership degree of 0 or 1. This criteria enables modeling of fuzzy operations with both convenience and simplicity. A triangular fuzzy number is a fuzzy number represented by three points (K_1^L, K_2^M, K_3^H), where $(k_1 < k_2 < k_3)$.

According to [23], in fuzzy triangular numbers, any membership functions of fuzzy number A can be defined as follows:

$$\left\{\begin{array}{cc} 0, & x < K_1^L \\ x - \frac{K_1^L}{K_2^M} - K_1^L, & K_1^L \leq x \leq K_2^M \\ K_3^L - \frac{x}{K_3^M} - K_2^L, & K_2^L \leq x \leq K_3^M \\ 0, & x \leq K_3^H \end{array}\right\}$$

A fuzzy multicriteria selection approach for analyzing the performance of industrial CV communications to the cloud was implemented by employing intuitionistic fuzzy numbers. In the proposed model, linguistic terms are used to rate the alternatives via criteria weighting and their corresponding fuzzy numbers.

3.3 Adaptive evaluation approach

To handle the problem of portfolio selection and aggregation of decisions, the SAW approach is proposed and the method in [24], [25] is used. Due to its simplicity and ability to identify unimproved gaps of alternatives, SAW has become the most popular decision-making (DM) approach. According to [20], [24] SAW is considered to be straightforward and can easily handle DM queries, motivated by its linear additive function, which can individually represent DM decisions. An empirical study [26] applied SAW and found superiority in both performance and simplicity. The essential principle of SAW is to calculate and categorize the weighted sum of the performance degrees for every criterion group.

The following equation describes this process:

$$A = \sum_{i=1}^{u} x_y x_{ij}, \quad j = 1, 2, \ldots, u-1, q = 1, 2, \ldots, v-1 \quad (7)$$

For identifying evaluation criteria to achieve the ideal level of any tested standard, a multiattribute model called importance-performance analysis (IPA) was reported [27]. It is composed of a dimension matrix, namely, "Importance" and "Performance", to explain evaluation criteria graphically. IPA has been utilized for analysis in different studies to allocate unimproved gaps between various services. The use of IPA aims to describe the security criteria associated with each industrial CV component. The IPA map is beneficial for deciding how best to allocate unimproved gaps between an actual industrial CV system and an ideal point depending on the evaluation criteria. In this study, we use the "performance rate" (PR) represented by the x-axis instead of "performance", while "global weight" (GW) constitutes the y-axis instead of "importance."

The GW is used to demonstrate the importance of the criteria sample and examine the reliability in Figure 3. Hence, the GW represents the importance and performance realization to improve the system reliability. The weights range from 0 to 1 according to the following equation:

$$W = W_x \in (W_1, W_2, \ldots, W_n) \quad (8)$$

$$BestPR = \left[(K-3-K_1) + (K-2-K_1)\right] / 3 + K_1, \forall i \quad (9)$$

$$GW = \frac{W}{\sum_{i=1}^{W_x} W_n,}, n = 1, 2, \ldots, n_i \quad (10)$$

4 Analysis and Results

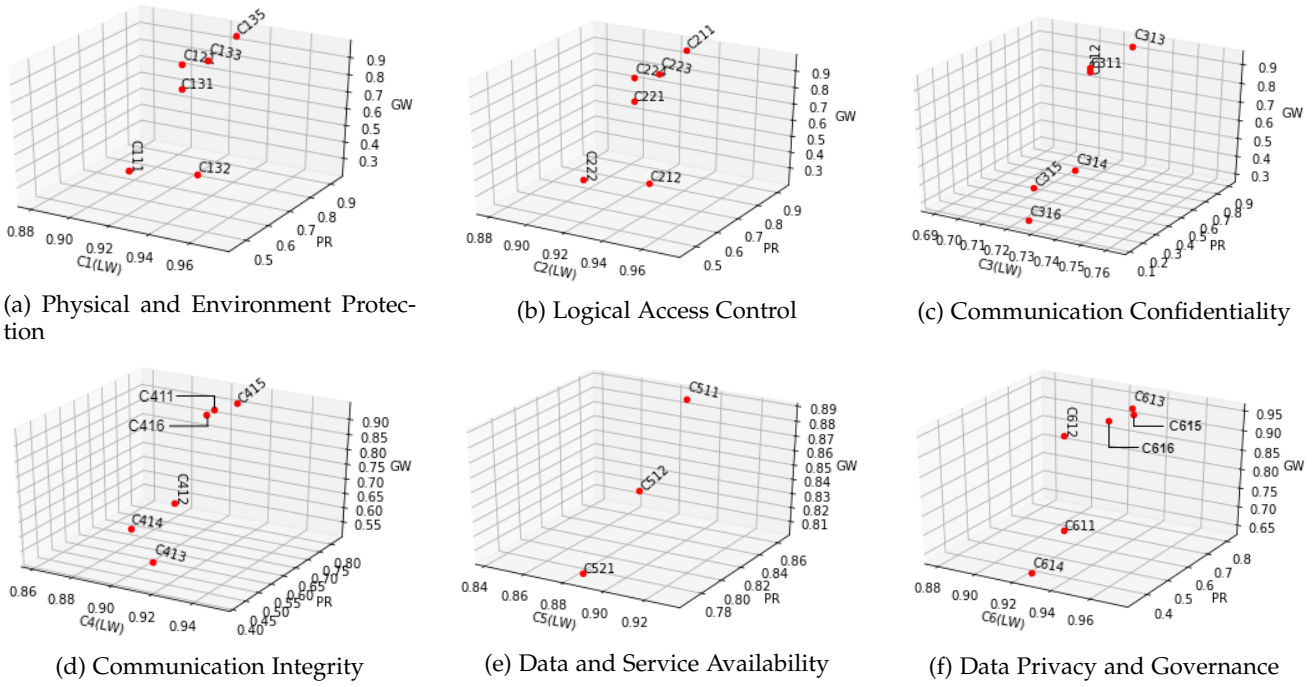
The proliferation of IoT devices had led to the generation of a considerable amount of heterogeneous data. The allocated data have to be kept in appropriate storage (e.g., the cloud), which is remotely accessible for processing. Consequently, these data can be used to learn a new pattern of behavior using a machine learning algorithm that embeds the intelligence into any system. With this growing trend, new security issues have arisen. Tremendous security criteria have been proposed to cope with these issues. However, our results demonstrate that all security criteria are not equal, which means that such criteria should not be governed and managed at the same level. Our novel framework TrustE-VC provides a trust measure of these different security criteria. It may be utilized to classify the importance of each criterion based on its distance from an ideal security point of the system.

Based on the results presented in Table 2, the average performance rate (APR) of TrustE-VC and the ideal point for each SCC are converted to crisp values by applying Eqs. 8 and 9, respectively, which identify the best PR among the set. The GWs related to all of these values are converted to fuzzy numbers using Eq. 10. Next, the main APRs are mapped against their GWs to graphically present a map depicting the SCC that is most in need of improvement (see Table 2). It can be observed that TrustE-VC achieved poor results in terms of authorization (C_{22}) and encryption (C_{31}). Thus, TrustE-VC should pay more attention to and find the best strategy to improve these criteria. Moreover, the GW and APR datasets in Table 2, with overall averages of 0.799 and 0.478, respectfully, were assigned to form an IPA analysis for the VC. This aims at defining the linkage of both the x- and y-axes for each IPA map.

Sensitive data should be located and transmitted securely throughout the whole life cycle to guarantee high data privacy of such a deployment architecture, for instance, integrating the IoT paradigm with the cloud for storage, processing, and data security purposes [28]. For example,

TABLE 2: Highlighted TrustE-VC findings for the SCCs and SCSs.

SCC Criteria	GW	APR (CV)	SCS Evaluation	
			Lowest PR	Highest PR
Infrastructure Design_C_{13}	0.820	0.556	$C_{111(0.580,0.886)}$	$C_{113(0.926,0.946)}$
Network Security_C_{11}	0.800	0.426	$C_{121(0.506,0.820}$	$C_{122(0.853,0.886}$
Object Security_C_{12}	0.840	0.648	$C_{132(0.605,0.811}$	$C_{131(0.820,0.926)}$
Authentication_C_{22}	0.875	0.485	$C_{212(0.459,0.506)}$	$C_{213(0.800,0.886)}$
Authorization_C_{21}	**0.600**	**0.416**	$C_{222(0.760,0.240)}$	$C_{221(0.926,0.946)}$
Wire Encryption_C_{31}	**0.604**	**0.343**	$C_{316(0.126,0.300)}$	$C_{313(0.906,0926)}$
Integrity_C_{41}	0.820	0.420	$C_{414(0.420,0.686)}$	$C_{415(0.820,0.906)}$
Data Availability_C_{52}	0.784	0.560	$C_{521(0.766,0.806)}$	—
Service Availability_C_{51}	0.755	0.546	$C_{511(0.820,0.840)}$	$C_{512(0.866,0.886)}$
Privacy & Governance_C_{61}	0.738	0.369	$C_{614(0.346,0.646)}$	$C_{613(0.811,0.926)}$
Overall Average	**0.799**	**0.478**	—	—



(a) Physical and Environment Protection

(b) Logical Access Control

(c) Communication Confidentiality

(d) Communication Integrity

(e) Data and Service Availability

(f) Data Privacy and Governance

Fig. 3: A fuzzy weight-variance 3D plot diagram for each CSC and SCC in TrustE-VC.

encryption researchers have traditionally responded by focusing on multiple CSCs, such as transparent data encryption, end-to-end wire encryption, and data masking and tokenization. TrustE-VC can provide a blockchain of thing encryption services as a supplementary service to clients. Such an approach could let the client choose from the recommended encryption software and techniques within different layers. Moreover, TrustE-VC needs to raise the encryption level to include most elements existing at the TrustE-VC cloud level. Multiple level encryption, blockchain encryption, transparent data encryption, identity-based encryption, attribute-based encryption, and wire encryption migration are all encryption routines to improve this SCC.

In contrast, C_{11}, C_{51}, C_{13}, and C_{52} were the SCCs that obtained the most significant attention from TrustE-VC. These four criteria were estimated as satisfactory in meeting customer needs, as they had the most leading APR rates. This analysis leads TrustE-VC to a significant realization that these criteria should be retained from the VC customer points of view. This assessment should help in attracting new VC customers and increasing business shares.

Table 2 shows that TrustE-VC has high-performance rates in most SCCs except for C_{22} and C_{31}, as they are far from the ideal point. Depending on these conclusions, recommendations are expected to enhance the unimproved gaps of TrustE-VC for these lower SCCs through various strategies. For instance, a strategy could be considered to improve the privacy with an appropriate access control level to include most components in the industrial CV system. Fault tolerance and recovery mechanisms, to operate appropriately under an incident or a failure, are other examples, to name a few. Only four out of six SCCs have a high APR for TrustE-VC, namely, data (C_{11} and C_{13}) and access control (C_{51} and C_{52}), in that they perform fairly against the ideal point. The remaining APRs of the SCCs are lower than the target point (ideal), in which each SCA criteria performs poorly against the ideal point. A primary assumption would be that these SCCs need an updated strategy (including installation of new hardware and tools) to be improved. Additionally, the table shows the highest and lowest value of each

SCS criteria, except for data availability C_{52} which contains one SCS: replication C_{521}. Different SCCs within TrustE-VC need additional refinement to achieve the target level. These SCCs have a lower APR than the other SCCs, which does not imply that all SCCs have to be urgently improved. In other words, it is necessary to identify the SCCs that need improvement action and those SCSs under each SCC that need further refinement. An IPA diagram for TrustE-VC is illustrated in Figure 3 to achieve the above objectives. In this 3D plot of the framework findings, each CSC represents the x-axis. Meanwhile, the PR and GW of each SCS represent the y-axis and z-axis, respectively. To represent the fuzzy weight variance, Cn = (CSC (Cn), PR (Cn), GW (Cn)), and the final IPA(Cn) $= \sum CSC + PR(Cn) * GW(Cn)$.

5 Discussion

Standardizing the industrial IoT is an essential measure to widely accept and support its technology [29]. However, the standardization process of the trust methods faces several challenges, among which is the lack of an evaluation approach of these standards and solutions. A study that aims at evaluating the trust of current industrial IoT solutions with a focus on the security criteria selection is indispensable. Along this line, this study proposes a methodological approach to comprehensively assess a leading application in this realm, i.e., industrial CV.

This research contributes to the deployment of the industrial VC security body of knowledge by first examining in detail the building blocks of the industrial VC trust architecture. Second, a rigorous and robust evaluation framework based on evaluation theory is presented, which guides VC service providers to identify security gaps. Finally, we highlight some open challenges and recommendations for both service providers and customers for a comprehensive discussion toward achieving the vision of providing trustworthy IoV-cloud secure services.

The proposed approach combines the use of criteria importance and performance rates for determining those trust service attributes to which a designer or policy maker should devote more attention. It also labels which feature should be a lower priority to keep the focus on the high-priority ones. First, the proposed approach uses the three-level security evaluation elements as a classification tree to analyze all the security elements in an industrial CV environment. Next, a multicriteria decision-making algorithm is applied for comprehensively weighing these criteria. Together, they offer a useful and practice-ready tool for designers and industrial CV practitioners to better evaluate and select industrial CV trust requirements.

5.1 Security by Design

Security by design is a development approach that ensures that security is considered from the start of system deployment, and not as an additional late phase, to operate and maintain the trustworthiness of industry 4.0 technologies [7]. Due to its inherently remote operations, resource cotenancy, distributed management, and administrative control, ensuring the privacy of IoT-based workloads while outsourcing computation is crucial. Industrial CV clients do not have direct control over the systems that utilize their data because of the cloud's black-box nature. In this context, modeling and optimization of IoT feature selection is an emerging trend [30].

To this end, our study addresses an emerging research gap of optimizing the security features of an implemented industrial VC solution by evaluating and ranking these features for optimal selection in the design phase.

Based on our test observation, the most pressing challenges in assessing IoT data protection before a move to the cloud are as follows:

- Data residency: This refers to the physical geographic location where the data stored in the cloud reside. When deploying a cloud-based IoV system, the physical location of the data is no longer known or fully trusted. Data residency also includes data flow channels, data stream processing, and edge data input/output.
- Data privacy: This describes the ability to limit data sharing in industrial CV systems, including with third parties, through an organization or individuals. Maintaining an appropriate data privacy level can be achieved by exploring various technologies and tools, including encryption. Other solutions include modifying policies and legislation to prevent unauthorized access or use of data. Defining the legal ownership, responsibilities, and privileges of data between the owner and data custodian can alleviate privacy threats.
- Data ownership: Defining data ownership is a serious concern within IoV-to-cloud data processing. When a client transfers his or her data to the cloud, the primary processor of that data is then not the physical owner, but the provider. Consequently, a new threat parameter is raised regarding trust for that provider. The client cannot be sure how the cloud system manipulates his or her data or whether the processing complies with his or her demands.

5.2 Future trends

In this paper, we address one of the leading open issues regarding industrial CV adoption. Namely, we evaluate the security criteria during the design phase of a cloud-based IoT application. We present a rigorous and robust evaluation model called TrustE-VC. The proposed framework formalizes and generalizes the main ideas proposed in the literature for empirical evaluation and selection of security criteria. TrustE-VC's main contribution is to help VC platforms identify the standard security criteria and provide security gap analysis according to a novel multi-criteria decision-making evaluation theory for supporting industrial CV systems as a commodity service in the cloud. Diagrammatic security levels, a novel evaluation theory, and a fuzzy ranking approach based on additive weight and CV security analysis comprise the critical framework components.

Future studies can focus on the following aspects. First, it would be interesting to employ TrustE-VC on other VC implementations (frameworks) to capture qualitative risk

evaluation information in a highly complex decision environment. In particular, the approach could be implemented with industrial CV providers to compare and evaluate the results of those providers to identify the most trustworthy providers in today's market. Second, utilization of new MCDM utility approaches, such as SWARA (step-wise weight assessment ratio analysis) and WASPAS (weighted aggregated sum product assessment) [31], can be applied to extend TrustE-VC to cope with other scenarios and trust analyses. Finally, the proposed TrustE-VC can be readily applied to extend the 52 security and trust criteria this study investigates. In fact, due to the wide trust area to evaluate, this study focused on the threats associated with industrial IoV-to-cloud security threats. Hence, it is worthwhile to conduct broader research that focuses on other trust criteria, such as privacy, governance, auditability, compliance, availability, and competence. The extension of these trust evaluation criteria should involve as much as possible the criteria that influence the trust of a suitable industrial CV solution. Finally, integration of this evaluation framework with the edges of the vehicular network modes [32], e.g., vehicle-to-vehicle and vehicle-to-infrastructure communication, is also considered a possible research trend.

6 Related Work

The security of IoV deployment architectures and VC service security have always been a concern and, hence, are a research trend. A large body of research aims to address this concern in the literature with various insights [8], [9], [12], [33], [34], [35]. Recently, Gupta et al. [36] proposed an authorization framework relevant to IoV and vehicular clouds; they discussed the need for access control within such a sensitive environment. They extended their work with the CV-ABACG [37] model, a formalized dynamic group, and attribute-based access control for a smart car ecosystem. In [17], the integration of cloud computing and fog computing for securing the data storage in IIoT deployment architectures was proposed. Meanwhile, realization of service-oriented models to securely access the underlying resources of cloud manufacturing based on IoT technologies was attempted in [38].

A recent study by Yang Lu and Li Da Xu indicated that the security quality of service-based design has the potential, as a leading research trend, to protect the IoT network [39]. This vital aspect was further investigated to enable security analysis and mitigation of security threats [7]. A risk assessment for wired networks using attack graphs was studied in [40]. Security analysis of IoT systems based on the generic behavior by formalizing the interactions among various IoT things and capturing IoT-specific threat classifications was reported [41]. However, all previous studies did not aim to evaluate the industrial IoT framework trust or provide a ranking and selection approach among the security features. For this, TrustE-VC aims at addressing this research gap and copes with the modern evaluation and selection methodology.

Kayes, A. S. M. et al. proposed a context-sensitive access control that supports control decisions when there are dynamic changes to the context [42] and context-aware access control using fuzzy logic [43]. Meanwhile, in [44] the context-aware access control policies at the runtime is specified, and a pluggable single-sign-on authentication module is suggested in [45]. While addressing the trust challenges of the ITS using cutting edge, big data frameworks was discussed in [46] with a multi-tier VC architecture. The work in [47] proposed a machine learning algorithm for relay attack detection in the VC.

On the other hand, securing a vehicular network using a fuzzy trust model based on experience and plausibility to ensure the reliability of vehicle communications was reported [33]. While many evaluation models of cloud computing have been proposed in the literature [21], [48], [49], they do not yet provide practical analysis for security designers of cloud-based IoT and VC systems. Aiming at improving the intelligent transportation system, Bui and Jung [50] used a dynamic decision-making approach for CVs. However, evaluating multiple conflicting criteria in decision making has not been a subject of intensive studies in the literature. This advanced analytic method aids in better decision making to choose prioritized security improvement actions and, hence, ensure the trustworthiness of the industrial CV environment. In this paper, we address this main open issue by proposing a novel evaluation approach.

7 Conclusion

A large body of research aims to address the security concern posed by the data transmission of connected vehicles with various insights. They do not yet provide practical analysis for security by design of cloud-based IoT and VC systems. Ensuring sustainable security integration of industrial CVs in the cloud environment with systematical security evaluation and selection has been limited in this context. This study intends to investigate a VC evaluation to offer assurances of the functional security properties of VC deployment architectures. The proposed TrustE-VC framework aims to express imprecise trust evaluation information to facilitate multiple-criteria decision analysis within industrial CV environments.

This framework provides a theoretical contribution based on the evaluation theory outlined by (1) categorizing a diagrammatic security taxonomy for security evaluation criteria in industrial CV clouds, (2) promoting a GDM ranking technique for better security criteria selection, and (3) introducing a fuzzy evaluation and ranking technique to evaluate and classify the unimproved security vulnerabilities in IoV-to-cloud deployment architectures. It also contributes to leveraging fuzzy sets and fuzzy IPA to accurately use the DM responses to prioritize the CSCs, SCCs, and SCS to achieve a better coverage for enhancing unimproved security vulnerabilities in current and future industrial CV environments. TrustE-VC aids in better decision making to choose prioritized security improvement actions and, hence, ensure the trustworthiness of the VC environment. Overall, the use of TrustE-VC as a basis to develop VC applications has proven the robustness and reliability of such a framework. As future work, the usage of the proposed methodology and framework will be considered to evaluate other IoT-applications and cyber-physical systems in the industrial IoT with larger-scale security features.

REFERENCES

[1] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," *Future generation computer systems*, vol. 56, pp. 684–700, 2016.

[2] E.-K. Lee, M. Gerla, G. Pau, U. Lee, and J.-H. Lim, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular fogs," *International Journal of Distributed Sensor Networks*, vol. 12, no. 9, p. 1550147716665500, 2016.

[3] J. Pillmann, B. Sliwa, J. Schmutzler, C. Ide, and C. Wietfeld, "Car-to-cloud communication traffic analysis based on the common vehicle information model," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, IEEE, 2017.

[4] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, 2016.

[5] H. Tao, M. Z. A. Bhuiyan, M. A. Rahman, T. Wang, J. Wu, S. Q. Salih, Y. Li, and T. Hayajneh, "Trustdata: Trustworthy and secured data collection for event detection in industrial cyber-physical system," *IEEE Transactions on Industrial Informatics*, 2019.

[6] F. Farivar, M. S. Haghighi, A. Jolfaei, and M. Alazab, "Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber physical systems and industrial iot," *IEEE transactions on industrial informatics*, 2019.

[7] H. Mouratidis and V. Diamantopoulou, "A security analysis method for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4093–4100, 2018.

[8] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted v2x communication," *Vehicular Communications*, vol. 12, pp. 50–65, 2018.

[9] I. García-Magariño, S. Sendra, R. Lacuesta, and J. Lloret, "Security in vehicles with iot by prioritization rules, vehicle certificates and trust management," *IEEE Internet of Things Journal*, 2018.

[10] T. Wang, M. Z. A. Bhuiyan, G. Wang, L. Qi, J. Wu, and T. Hayajneh, "Preserving balance between privacy and data integrity in edge-assisted internet of things," *IEEE Internet of Things Journal*, 2019.

[11] M. Ahvanooey, Q. LI, X. Zhu, M. Alazab, and J. Zhang, "Anitw: A novel intelligent text watermarking technique for forensic identification of spurious information on social media," *Computers & Security*, 2019.

[12] M. Tang, M. Alazab, and Y. Luo, "Big data for cybersecurity: vulnerability disclosure trends and dependencies," *IEEE Transactions on Big Data*, 2017.

[13] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[14] M. Aladwan, F. Awaysheh, J. Cabaleiro, T. Pena, H. Alabool, and M. Alazab, "Common security criteria for vehicular clouds and internet of vehicles evaluation and selection," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications*, pp. 814–820, IEEE, 2019.

[15] J. E. Siegel, D. C. Erb, and S. E. Sarma, "A survey of the connected vehicle landscape—architectures, enabling technologies, applications, and development areas," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2391–2406, 2017.

[16] H. Peng, L. Liang, X. Shen, and G. Y. Li, "Vehicular communications: A network layer perspective," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1064–1078, 2018.

[17] J.-S. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, "Secure data storage and searching for industrial iot by integrating fog computing and cloud computing," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4519–4528, 2018.

[18] L. Zhu, F. R. Yu, Y. Wang, B. Ning, and T. Tang, "Big data analytics in intelligent transportation systems: A survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 1, pp. 383–398, 2018.

[19] Z.-p. Tian, J.-q. Wang, and H.-y. Zhang, "An integrated approach for failure mode and effects analysis based on fuzzy best-worst, relative entropy, and vikor methods," *Applied Soft Computing*, vol. 72, pp. 636–646, 2018.

[20] G.-H. Tzeng and J.-J. Huang, *Multiple attribute decision making: methods and applications*. Chapman and Hall/CRC, 2011.

[21] H. M. Alabool and A. K. B. Mahmood, "A novel evaluation framework for improving trust level of infrastructure as a service," *Cluster Computing*, vol. 19, no. 1, pp. 389–410, 2016.

[22] L. A. Zadeh, "Fuzzy sets," *Information and control*, vol. 8, no. 3, pp. 338–353, 1965.

[23] G. J. Klir and B. Yuan, "Fuzzy sets and fuzzy logic: theory and applications," *Upper Saddle River*, p. 563, 1995.

[24] C. W. Churchman and R. L. Ackoff, "An approximate measure of value," *Journal of the Operations Research Society of America*, vol. 2, no. 2, pp. 172–187, 1954.

[25] K. R. MacCrimmon, "Decisionmaking among multiple-attribute alternatives: a survey and consolidated approach," tech. rep., RAND CORP SANTA MONICA CA, 1968.

[26] S. H. Zanakis, A. Solomon, N. Wishart, and S. Dublish, "Multi-attribute decision making: a simulation comparison of select methods," *European journal of operational research*, vol. 107, no. 3, pp. 507–529, 1998.

[27] J. A. Martilla and J. C. James, "Importance-performance analysis," *Journal of marketing*, vol. 41, no. 1, pp. 77–79, 1977.

[28] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of iot and cloud computing," *Future Generation Computer Systems*, vol. 78, pp. 964–975, 2018.

[29] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[30] A. Ahmad, M. Khan, A. Paul, S. Din, M. M. Rathore, G. Jeon, and G. S. Choi, "Toward modeling and optimization of features selection in big data based social internet of things," *Future Generation Computer Systems*, vol. 82, pp. 715–726, 2018.

[31] A. Mardani, M. Nilashi, N. Zakuan, N. Loganathan, S. Soheilirad, M. Z. M. Saman, and O. Ibrahim, "A systematic review and meta-analysis of swara and waspas methods: Theory and applications with recent fuzzy developments," *Applied Soft Computing*, vol. 57, pp. 265–292, 2017.

[32] Y. Feng, B. Hu, H. Hao, Y. Gao, Z. Li, and J. Tan, "Design of distributed cyber–physical systems for connected and automated vehicles with implementing methodologies," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4200–4211, 2018.

[33] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales, M. K. Khan, and S. Goudarzi, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619–15629, 2017.

[34] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Communications Magazine*, vol. 55, no. 6, pp. 146–152, 2017.

[35] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "A systematic review of data protection and privacy preservation schemes for smart grid communications," *Sustainable cities and society*, vol. 38, pp. 806–835, 2018.

[36] M. Gupta and R. Sandhu, "Authorization framework for secure cloud assisted connected cars and vehicular internet of things," in *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, pp. 193–204, ACM, 2018.

[37] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Dynamic groups and attribute-based access control for next-generation smart cars," in *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*, pp. 61–72, ACM, 2019.

[38] F. Tao, Y. Zuo, L. Da Xu, and L. Zhang, "Iot-based intelligent perception and access of manufacturing resource toward cloud manufacturing," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1547–1557, 2014.

[39] Y. Lu and L. Da Xu, "Internet of things (iot) cybersecurity research: a review of current research topics," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103–2115, 2018.

[40] A. Sen and S. Madria, "Risk assessment in a sensor cloud framework using attack graphs," *IEEE Transactions on Services Computing*, vol. 10, no. 6, pp. 942–955, 2016.

[41] M. Mohsin, Z. Anwar, G. Husari, E. Al-Shaer, and M. A. Rahman, "Iotsat: A formal framework for security analysis of the internet of things (iot)," in *2016 IEEE Conference on Communications and Network Security (CNS)*, pp. 180–188, IEEE, 2016.

[42] A. Kayes, J. Han, W. Rahayu, T. Dillon, M. S. Islam, and A. Colman, "A policy model and framework for context-aware access control to information resources," *The Computer Journal*, vol. 62, no. 5, pp. 670–705, 2018.

[43] A. Kayes, W. Rahayu, T. Dillon, E. Chang, and J. Han, "Context-aware access control with imprecise context characterization for cloud-based data resources," *Future Generation Computer Systems*, vol. 93, pp. 237–255, 2019.

[44] A. Kayes, W. Rahayu, and T. Dillon, "An ontology-based approach to dynamic contextual role for pervasive access control," in *2018*

IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), pp. 601–608, IEEE, 2018.

[45] F. M. Awaysheh, J. C. Cabaleiro, T. F. Pena, and M. Alazab, "A pluggable authentication module for big data federation architecture," in *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*, pp. 223–225, ACM, 2019.

[46] F. Awaysheh, J. C. Cabaleiro, T. F. Pena, and M. Alazab, "Big data security frameworks meet the intelligent transportation systems trust challenges," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 807–813, IEEE, 2019.

[47] U. Ahmad, H. Song, A. Bilal, M. Alazab, and A. Jolfaei, "Securing smart vehicles from relay attacks using machine learning," *The Journal of Supercomputing*, pp. 1–18, 2019.

[48] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," *Future Generation Computer Systems*, vol. 29, no. 4, pp. 1012–1023, 2013.

[49] A. Shameli-Sendi, M. Shajari, M. Hassanabadi, M. Jabbarifar, and M. Dagenais, "Fuzzy multi-criteria decision-making for information security risk assessment," *The Open Cybernetics & Systemics Journal*, vol. 6, no. 1, 2012.

[50] K.-H. N. Bui and J. J. Jung, "Aco-based dynamic decision making for connected vehicles in iot system," *IEEE Transactions on Industrial Informatics*, 2019.

Mohammad N. Aladwan obtained his BSc Software Engineering degree from Al Balqa 'Applied University in 2005 and a MSc Degree in Computer Networks and Security at Central Queensland University (Australia) in 2010. Currently, he is a Ph.D. Student at the University of Santiago de Compostela-CiTIUS. His main research interests include security in cloud environments and middleware for Cloud and Big Data

Feras M. Awaysheh holds a PhD. in Big Data and Cloud Computing from the University of Santiago de Compostela, Spain. He obtained a BSc. Software Engineering degree from Al Balqa 'Applied University in 2008 and MSc. Degree from New York Institute of Technology (NYIT) With Honor in 2010, majoring in Information, Computer, and Network Security. Currently, he is a researcher at the CiTIUS research center and a visiting fellow at the University of Edinburgh, UK. His main research interest includes large-scale distributed systems and Big Data analytics in general. Besides, developing and running software reliably in production for resource allocation (on-premises and cloud-based clusters), and middlewares for load-balancing and security solutions in HPC, Cloud, IoT, and Big Data deployment architectures.

Sadi Alawadi holds a Ph.D. in Computer science /AI with honor, 2018, from Santiago de Compostela University - Spain. And a Master degree in Softcomputing and intelligence system, 2012, from Granada University - Spain. Currently, he is working at Malmö University - Sweden at IOTAP research center. His main research lines include IOT systems, IoT middleware, End-User Development in the IOT, Machine learning, Deep learning, federated learning, transfer learning, Smart cities, and their related systems, Bigdata, Real-time analysis, Dimensionality reduction, and data visualization Context Awareness, and Blockchain.

Mamoun Alazab is an Associate Professor at the College of Engineering, IT and Environment at Charles Darwin University, Australia. He received his PhD degree in Computer Science from the Federation University of Australia, School of Science, Information Technology and Engineering. He is a cyber security researcher and practitioner with industry and academic experience. Alazab's research is multidisciplinary that focuses on cyber security and digital forensics of computer systems with a focus on cybercrime detection and prevention including cyber terrorism and cyber warfare. He has more than 150 research papers. He delivered many invited and keynote speeches, 24 events in 2019 alone. He convened and chaired more than 50 conferences and workshops. He works closely with government and industry on many projects, including Northern Territory (NT) Department of Information and Corporate Services, IBM, Trend Micro, the Australian Federal Police (AFP), the Australian Communications and Media Authority (ACMA), Westpac, United Nations Office on Drugs and Crime (UNODC), and the Attorney General's Department. He is a Senior Member of the IEEE. He is the Founding chair of the IEEE Northern Territory (NT) Subsection.

Tomás F. Pena got his Ph.D. in Physics in 1994 in the University of Santiago de Compostela (Spain). From 1994, he is an associate professor in the Department of Electronics and Computer Science of the University of Santiago de Compostela. From 2010, he is a member of the Research Center in Intelligent Technologies (CiTIUS) of this University. His main research lines include the high performance computing in general, the architecture of parallel systems, the development of parallel algorithms for clusters and supercomputers, the optimization of the performance in irregular codes and with sparse matrices, the prediction, and improvement of the performance of parallel applications in general, the development of applications and middleware for Grid and Cloud, and the use of Big Data technologies for scientific and NLP applications. He is IEEE senior member and associate editor of IEEE Trans. on Computers and IEEE Access.

Jose C. Cabaleiro got his Ph.D. in Physics n the University of Santiago de Compostela (Spain). From 1994 he is an associate professor in the area of Computer Architecture in the Department of Electronics and Computing in the University of Santiago de Compostela. His main lines of interest include the architecture of parallel systems, the development of parallel algorithms for irregular problems and with sparse matrices, prediction, and improvement of the performance of parallel applications, optimization of the memory hierarchy in irregular problems and development of applications and middleware for Grid and Cloud.