Computer Standards & Interfaces 81 (2022) 103596

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Toward pre-standardization of reputation-based trust models beyond 5G

José María Jorquera Valero [a,*], Pedro Miguel Sánchez Sánchez [a], Manuel Gil Pérez [a], Alberto Huertas Celdrán [b], Gregorio Martínez Pérez [a]

[a] Department of Information and Communications Engineering, University of Murcia, 30100 Murcia, Spain
[b] Communication Systems Group (CSG) at the Department of Informatics (IfI), University of Zurich UZH, 8050 Zürich, Switzerland

ARTICLE INFO

Keywords:
Trust and reputation model
Trust standardization
Requirements
KPIs
Trustworthiness relationships
Beyond 5G

ABSTRACT

In the last years, the number of connections in mobile telecommunication networks has increased rampantly, and in consequence, the number and type of relationships among entities. Should such interactions are to be profitable, entities will need to rely on each other. Hence, mobile telecommunication networks demand trust and reputation models that allow developing feasible communications in 5G and beyond networks, through which a group of entities can establish chains of services between cross-operators/domains, with security and trustworthiness. One of the key obstacles to achieving generalized connectivity beyond 5G networks is the lack of automatized, efficient, and scalable models for establishing security and trust. In this vein, this article proposes a pre-standardization approach for reputation-based trust models beyond 5G. To this end, we have realized a thorough review of the literature to match trust standardization approaches. An abstract set of requirements and key performance indicators has been extracted, and some pre-standardization recommendations proposed to fulfill essential conditions of future networks and to cover the lack of common trust and reputation models beyond 5G.

1. Introduction

With the proliferation of the fifth generation of mobile networks (5G), new technologies, approaches, entities, and communications rise to evolve and cover certain shortages from previous generations [1]. 5G also expects to support a multi-tenant business model [2] in which users may rent or buy service, resource, and infrastructure capabilities across multiple domains to cover feasible peak workloads and fulfill their Key Performance Indicators (KPIs). Therefore, the configuration of reliable cross-domain/operator service chains plays a pivotal role to guarantee the expected Quality of Services (QoS) as well as avoiding risky connections that may compromise data integrity in 5G-enabled scenarios. Despite the fact that trust is not contemplated as an innovative paradigm, since it began to be considered around 2000 [3], it is expected to be used in a wide variety of 5G scenarios such as cloud environments [4], IoT [5], and network slicing [6], among others. Thence, trust is one of the technologies that await to support 5G and beyond networks into a new era of more secure and reliable communications.

Trust can be defined as the assessable confidence and/or belief that illustrates recorded value from previous experiences and the expected value for future interactions. The trust concept may also encompass security aspects such as integrity, access control, and confidentiality, as well as privacy aspects such as disclosure, secrecy, and isolation (see Fig. 1). Nevertheless, security and privacy aspects are mainly centered on entity's identity while trust deals with entity's behavior.

Traditionally, trust has been usually handled through models that allow establishing reliable relationships among different stakeholders involved in the communication. In the same way, prior trust models were mainly focused on end users and peer-to-peer connections [7]. Nevertheless, trust, as well as other technologies that last over time, needs to be adapted to the new trends and requirements of telecommunication networks. One of the changes compared to conventional trust models is the entity on which the model is applied. Nowadays, not only end users are considered as an entity on which to calculate a trust score before establishing a communication, but also service consumers, resource consumers, software suppliers, network service providers, and network resource providers [8]. Therefore, trustworthy end-to-end chains should be contemplated so as to prognosticate the trust of all involved entities from the origin to the end.

Likewise, trust needs to progress toward new approaches that have

* Corresponding author.
E-mail addresses: pedromiguel.sanchez@um.es (P.M. Sánchez Sánchez), mgilperez@um.es (M. Gil Pérez), huertas@ifi.uzh.ch (A. Huertas Celdrán), gregorio@um.es (G. Martínez Pérez).

https://doi.org/10.1016/j.csi.2021.103596
Received 31 March 2021; Received in revised form 23 September 2021; Accepted 30 October 2021
Available online 2 November 2021

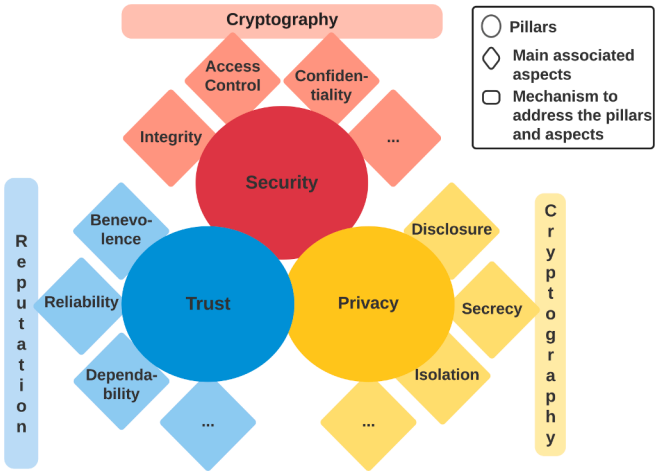

Fig. 1. Different view on trust.

not been considered previously such as zero-touch [9] and zero trust [10], among others. In the case of zero-touch, trust models should empower an end-to-end automatization of network and service management through high-level policies, rules, machine learning, and artificial intelligence algorithms. Regarding the zero trust approach, this entails the evasion of implicit trust to any entity in an intra- or inter-domain scenario. Accordingly, beyond 5G networks boost again trust model investigations to adapt them to the new properties of such networks. Hence, prior trust models must evolve towards novel models that consider beyond 5G network trends and challenges such as end-to-end trustworthiness solutions, process automation, and circumventing the default trust.

To the best of our knowledge, there are no guidelines or standards that induct a set of recommendations to follow in order to develop a trust and reputation model in beyond 5G networks. This absence stands in the way of disseminating trust and reputation models as an abstract mechanism, which could be applied regardless of the final deployment scenario. In the same manner, the lack of an abstract model beyond 5G also makes difficult its utilization as an enabler to guarantee secure and trustworthy connections. In this regard, the article carries out a comprehensive analysis of previous guidelines, standardizations, and roadmaps for trust models to look at conventional properties and features. Moreover, the article at hand provides a pre-standardization approach for trust and reputation models beyond 5G. To cope with these challenges, the main contributions of this article are as follows.

- An in-depth research on previous standardization proposals of trust and reputation models is conducted, as none was found at present to guide us in the development of a reputation-based trust model beyond 5G. At the same time, related work is analyzed and contrasted to perceive similarities between prior trust models and future ones. As well, it is achievable to detect new trends and shortages.
- Different sets of requirements and KPIs are identified from both previous trust model standardizations (i.e., pre-5G) and 5G/Beyond 5G (B5G) trust models. By means of such requirements and KPIs, specific needs to be met for a reputation-based trust model beyond 5G are recapped.
- A description of an abstract trust and reputation model beyond 5G is introduced. The description contains the four essential modules that make up such a model, in addition to several recommendations that may be contemplated as part of a pre-standardization approach.

The remainder of the article is structured as follows. Section 2 describes a literature review of works related to standardization approaches, as well as research projects and regulatory organizations working on trust and reputation models beyond 5G. Section 3 illustrates the progress of requirements and KPIs from the main solutions found in the state-of-the-art review. Section 4 gives our design recommendations for trust and reputation models beyond 5G, as well as drawing four abstract modules of such model. Finally, Section 5 expounds some conclusions as well as open perspectives for future work.

2. Analysis of trust model standardization proposals

Prior to contributing to a reputation-based trust model standardization approach, a broad understanding of the literature is required. This process enables recognizing features and components of long-term trust models, KPIs fulfilled, entities involved, etc. Thus, we are going to carry out thorough research on (pre-)standardization papers (Section 2.1), prevalent research projects (Section 2.2), and regulatory organizations that had worked or are still working on reputation-based trust model standardization and towards beyond 5G trust models (Section 2.3). Our intention consists in identifying properties, features, and components that trust models have contemplated for ages, as well as sighting their evolution. So as to ease an overview of all drafted proposals, two comparative tables (see Table 1 and Table 2) are depicted at the end of Section 2.3, where the complete list of properties, features, and components of each research paper, research project, and regulatory organization can be observed. In this way, the illustrated properties, features, and components state principal aspects among trust model standardization proposals from long-term to nowadays. Nevertheless, the following subsections do not intend to explain how the properties, features, and components of each proposal have been addressed owing to the fact that there is not a general and unique method for each one.

2.1. Research papers related to trust and reputation model standardization

Since early2000′s, trust models and its standardization have been a research field addressed by numerous authors. Despite trust and reputation models have been contemplated and designed in several areas such as ubiquitous environments [11], cloud environments [12], IoT [13], ad-hoc networks [14], and 4G and 5G networks [6], among others, only a few proposals submitted a comprehensive trust model. In this sense, a suitable trust and reputation model must contemplate many characteristics such as direct and indirect trust, reputation scores, historical trust, degradation of time, the validation of a third-party recommendation (user's credibility), user's satisfaction, time windows, resilience to common attacks, rewards, and punishments, just to name but a few, along with a selective number of requirements and KPIs.

Even though not many papers were found in the literature review under keywords such as standardization, pre-standardization, roadmap, or general trust model topics, we introduce from its beginnings to today the most representative efforts related to the previously keywords in different computer science areas. In 2004, a first standardization attempt was showcased by Trček [15]. The author presented a trust management standardization proposal that considered the essence of trust, which means that he researched all trust factors that should be considered for developing a trust model, regardless of cognitive principles. This research was mainly focused on a review of the trust field and the presentation of a trust taxonomy. For that, the author identified a list of relevant and basic trust factors. Among them, it should be pointed out the irrationality, forgetting factor (i.e., past interactions have lower relevance), and trust differentiation. In addition, Trček defined a set of properties for his trust model standardization proposal such as utilization of discrete values that can lead to diffuse decision making, context-dependence, reflexivity, asymmetry, non-transitive, and dynamic trust relationships, being some of them considered in the current trust models (see Table 1). It is worthwhile to briefly describe the meaning of important properties such as the context-dependence, which is aware of entities and their interactions, application environments, and other context factors, and the non-transitive, that refers to the

Table 1
Common properties of trust model standardizations.

		State-of-the-art research papers											*Research projects*				*Regulatory organizations*						
		[15]	[16]	[17]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[27]	[28]	[33]	[34]	[35]	[36]	[38]	[39]	[40]	[42]	[41]	[10]	Ours
	Year (20xx)	04	10	12	12	12	14	14	15	16	17	20	20	18	19	19	19	17	18	18	18	20	20	21
PROPERTIES	**Dynamicity**	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?	✓	✓	✓	?	✓	✓	✓
	Context-dependence	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Infinitesimal		✓	✓	✓		✓	✓	✓			✓	✓	?	?	?	?	✓		✓	?	✓		✓
	Integrity	✓	✓	✓				✓	✓		✓		✓	?	?	?	?	✓		✓	✓		✓	✓
	Benevolence		✓								✓		✓	?	?	?	?	✓		✓	?			
	Identity		✓	✓				✓	✓				✓	?	?	?	?		✓	✓	✓	✓	✓	✓
	Asymmetry	✓	✓	✓		✓	✓			✓		✓	✓	?	?	?	?	✓	✓		?			✓
	Privacy-preserving		✓				✓		✓				✓	?	?	?	?			✓	✓	✓	✓	✓
	Non-transitive	✓	✓			✓	✓	✓	✓			✓	✓	?	?	?	?	✓	✓	✓	?	?	✓	✓

?: Information is not currently available.

mathematical property: if A trusts B and B trusts C, then A does not trust C by default. Perhaps due to the early definition of this standard proposal, the author did not figure out other relevant aspects such as user's satisfaction, reputation, and credibility, or even what components or modules ought to have a standard trust model. As it can be observed in Table 2, aspects such as direct/indirect trust or components of trust models began to be contemplated in subsequent publications.

Years later, other standardization proposals emerged like Gómez Mármol and Martínez Pérez [16] and Bøegh and Yuan [17]. Gómez Mármol and Martínez Pérez realized another effort to pinpoint a trust pre-standardization, in this case of trust and reputation models for distributed and heterogeneous systems [16]. Six years later since Trček [15], the authors detected an absence of standardization efforts for trustworthiness models [16]. Nevertheless, in contrast to Trček [15], the number of trust and reputation model investigations had increased and therefore identifying a common set of properties, trust components, or processes might be easier. In consequence, Gómez Mármol and Martínez Pérez reviewed trust and reputation models in distributed systems, obtaining general processes and characteristics. Thus, this thorough research was the basis of their recommendations for pre-standardization. Among the most relevant recommendations, it can be highlighted the set of model components (gathering information, scoring & ranking, entity selection, transaction, and reward & punish); information sources weighting; privacy-preserving via pseudonyms or unique identifiers generated cryptographically; degradation of time in transactions; accuracy vs consumption/performance; and treatment of newcomers and reputation abusers. Even though it is a 2010 proposal, it is one of the most exhaustive identified in the literature given the multitude of properties considered. Nonetheless, Gómez Mármol and Martínez Pérez followed a distributed approach but it did not consider cross-domain and multi-stakeholder contexts that are trends in networks beyond 5G, as well, they did not contemplate abstract requirements and KPIs to be applied in their trust model. Therefore, our proposed reputation-based trust model not only considers pivotal 5G cross-domain and multi-stakeholder scenarios, but also incorporates new techniques and approaches to adapt the properties, features, and components of trust models to new requirements.

In the case of Bøegh and Yuan [17], the authors analyzed the main differences between trust and trustworthiness, as well as they introduced a service behavior trustworthiness management scheme which was forwarded to the Sub Committee ISO/IEC JTC1/SC7 [18]. They defined trust as a subjective value that depends on the risk propensity of the trustor, the action, and the trustworthiness (it changes over time). Among the most pivotal requirements established by the authors, we can note trustworthiness management visibility, awareness of real identities, auditability, impartiality, and objectivity. In addition, the authors also provided a list of components that were needed in their schema, being some of them common for other trust models, such as a formal language for specifying service behavior, a method for assessing the ability of the service provider, a monitoring capability, a method for assessing service behavior, and another one for determining the service trustworthiness. In short, this approach was more focused on a service behavior trustworthiness model so not all components can be extrapolated to a general trust model.

Despite they are not considered as proposals for standardization, there are some solutions in the literature that help future authors to carry out trust model standardization. In the case of Vinkovits [19], the author realized an investigation of how users, who did not have a trust model concept understanding previously, comprehend trust in distributed systems and what were initial requirements that all trust management model must accomplish. Among the set of requirements identified, a great number are shared with the Gómez Mármol and Martínez Pérez's pre-standardization proposal [16]. The author identified three main model components: gathering information, scoring & ranking, and entity selection. Regarding the information gathering model, Vinkovits outlined the use of quality parameters in direct and indirect trust,

Table 2
Common features and components (COMPs) of trust model standardizations.

		State-of-the-art research papers											*Research projects*				*Regulatory organizations*						Ours
		[15]	[16]	[17]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[27]	[28]	[33]	[34]	[35]	[36]	[38]	[39]	[40]	[42]	[41]	[10]	
	Year (20xx)	04	10	12	12	12	14	14	15	16	17	20	20	18	19	19	19	17	18	18	18	20	20	21
FEATURES	**Direct trust**	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	?	✓	✓	✓
	Indirect trust		✓	✓	✓	✓	✓	✓	✓	✓			✓	?	?	?	?	✓		✓	?		✓	✓
	Weighting		✓		✓	✓	✓	✓	✓					?	?	?	?	✓		✓	?		✓	✓
	Reward & punishment		✓				✓	✓		✓			✓	?	?	?	?				?	✓		✓
	Forgetting factor	✓	✓	✓	✓									?	?	?	?				?		✓	✓
	Satisfaction		✓								✓			?	?	?	?	✓			?			✓
	Credibility								✓		✓			?	?	?	?	✓			?			✓
	Subjectivity problem		✓				✓							?	?	?	?	✓			?			✓
	Resilience attacks		✓				✓							?	?	?	?	✓		✓	?	✓	✓	
COMPs	**Information gathering**		✓	✓	✓	✓	✓						✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Trust calculation		✓	✓	✓	✓	✓						✓	✓	✓	✓	✓	✓	✓	✓	?	✓	✓	✓
	Trust storage		✓				✓						✓	?	?	✓	?	✓		✓	?		✓	✓
	Decision-making		✓	✓	✓	✓	✓						✓	?	✓	✓	?	✓		✓	?	✓	✓	✓
	Reward & punish		✓			✓								?	?	?	?				?			✓

?: Information is not currently available.

reliability rate establishment, transaction history considering time, etc. With regard to reliability rate, the author contemplated this parameter to avoid bias votes and to apply recommendations to the trust computation process that were similar to recommender preferences. In the case of scoring & ranking, it should be noted the quantified trust, parameter weightings, and computation of average rating. By means of this component, the author intended to generate a trust score calculated in a transparent way. Finally, regarding entity selection, it was established criteria for the service selection based on trust score. However, this proposal did not contemplate some crucial properties that Gómez Mármol and Martínez Pérez did such as user satisfaction, user identification, and user credibility [16], among others.

As it can be observed in Table 1, prior to 2012 there was a lack of trust model approaches, since Trček [15] and Gómez Mármol and Martínez Pérez [16] were the only standardization approaches identified to date. In this vein, Abassi and El Fatmi identified such trust model shortage and carried out an investigation to cover it [20]. In particular, they considered trust as a concept related to security and which allowed increasing it. Besides, they identified multiple trust and reputation model properties such as permanence, non-transitive, reflexivity, context-dependence, scalability, and asymmetry, which were incorporated in their trust management model. Through the trust management model, they endeavored to unify and standardize trust to the most communication environments and needs. The trust life cycling modeling was mainly made up of three components: trust establishment, trust update, and trust revocation. In terms of trust to establish a given relationship between parties, the trust level for this fact can be computed through Equation (1).

$$Trust(T, t, a, o, [c], [recd]) \rightarrow level \tag{1}$$

where T is the trustor; t denotes the trustee; a is the action related to the trust request; o corresponds to the object of the recommendation; c (optional) are the possible constraints; and *recd* (optional) indicates a given feasible recommendation.

In order to tackle the previous components, they also thought about using discrete values to assign trust levels (considering three intervals: distrust, no information, trust) and using recommender's weighting parameters. Even though the authors took into account several key properties and components, this approach, to the best of our knowledge, could have been improved since they did not talk about the information gathering component (common trust dimensions and features), user's credibility issue, or degradation of time in transactions.

Two years after the proposal published in 2012 by Abassi and El Fatmi [20], Costagliola et al. worked on a pre-standardization model that facilitated the way to future researchers by means of their trust, reputation, and recommendation (TRR) meta model [21]. Whilst this research was focused on an e-commerce field, they introduced some general concepts that can be applied independently of the field of a trust model. In this sense, their TRR meta model was able to identify fundamental concepts, features, and modules. First, they recommended identifying all possible entities involved in the trust and reputation model to associate features such as longevity, privacy, anonymity, and initial values for modeling newcomers. Next, the TRR model should contain an information gathering component to specify active and passive mechanisms and to check the information authenticity. Then, the information storing component contemplated features such as non-repudiation, aging, and data aggregation. They also considered fairly access to shared information. Finally, their trust and reputation model considered recommendation systems, decision-making processes, incentive mechanisms, and malicious attacks resilience. As illustrated in Table 1 and in Table 2, this approach shared fundamental ideas such as dynamism, asymmetry, privacy-preserving, and non-transitive with other previous investigations like Trček [15] and Gómez Mármol and Martínez Pérez [16], and even it contemplated identical components/modules for gathering and managing trust information with

Gómez Mármol and Martínez Pérez [16], Bøegh and Yuan [17], and Vinkovits [19]. Therefore, we can observe how over the years the proposed trust standardization models tend to converge toward common principles, although there are still some discrepancies between them such as the consideration of user credibility and a satisfaction factor. As the main handicap of this approach, it can be outlined the absence of crucial features such as user's satisfaction and recommender's credibility. These properties are essential in trust and reputation models to ensure a trustworthy and accurate system.

Another interesting research centered on reputation models is tackled by Vavilis et al. [22]. They presented a reference model for reputation that contained both a set of needed requirements and reputation system features. In the case of requirements, they were divided into three subgroups: the formulation dimension, the fair treatment of newcomers, and the integrity of reputation values, being some of them previously identified by Gómez Mármol and Martínez Pérez [16]. In parallel, and considering these requirements, Vavilis et al. generated a table with some of the main properties that reputation systems should consider to be abstract [22]. Among them, we can highlight absolute reputation values, (un)certainty, timestamp, interaction context, trust dissemination, scope similarity, and the range of user behavior (trust vs mistrust). In addition, they introduced some tips to meet these challenges.

Despite it is not considered as a pre-standardization investigation, Kanwal et al. detected a lack of standardization and interoperability in cloud computing area, and they generated a taxonomy for trust models [23]. With the aid of their model, they attempted to gather the functional and non-functional requirements to present a general taxonomy that allowed evaluating and establishing trust. To this end, they classified all kinds of trust models available in cloud computing (agreement-, certificates-, feedback-, domains-, and subjective-based models), and then, they introduced two or three functional features for each one. The authors considered a common set of features for different models, being derived from key concepts such as security, performance, control, and deployment. Although some functional and non-functional features are contemplated in previous (pre-) standardizations researches (e.g., credibility, dynamic trust, transaction history, or subjectivity, among others), this approach is far from being a beginning of standardization as it overlooked other crucial elements (see Table 1 and Table 2). In particular, the authors did not consider attack mitigation nor features and general components that any trust model in the cloud or other environments must contain. Besides, some functional features assigned to a specific kind of trust model could be taken into consideration by more than one.

Similarly, Joshi and Mishra also detected a need for trust standardization in mobile ad hoc networks [24]. They carried out a roadmap toward trust management and privacy-preservation. In particular, the authors gathered the main aspects of trust management and trust establishment across mobile networks to generate a trust algorithm that guides the outperformance to the mobile scenario. Their proposal computed trust as a conjunction of node cooperation index, reliability index, trust factor, and the disjunction of selfish index. However, since this research was not focused on trust models but a trust algorithm from trust model characteristics, it did not contemplate other relevant properties such as context-dependence, forgetting factor, or privacy-preserving, among others.

Although it can be considered indirectly related to trust standardization models, Viardot carried out an analysis of trust standardization to drive the acceptance of technology innovations [25]. Despite the paper was not focused on trust models, the author considered three important characteristics related to trust like credibility, integrity, and benevolence, and as such properties influence the acceptance of technology innovations, and therefore in standardization. When it comes to benevolence, it is understood as the trustor's kindness perception in the trustee's efforts without rewards [26]. Although the relevance of these characteristics has a different consequence depending on the innovation and standardization cycle, the author highlighted the need to fulfill them to guarantee a minimum basis of trustworthiness in any standard. In this sense, he emphasized that trust standardization will be probably continued by benevolence standardization. Thus, there are certain risks associated with the lack of benevolence of an innovation provider such as the definition of measurement criteria or interpretation of trust, as being benevolent has different connotations in different parts of the world.

Even though there is not a large spectrum of papers that address the trust and reputation standardization issue, there are still researchers who are concerned about the lack of standardization. One of them is Jelenc [27] who detected a massive increase in entities that utilized trust to establish and share information in 5G networks. In this regard, he also observed an absence of standards that enable us to share such information. Thus, the author proposed a general framework to make an easier trust information exchange through the definition of a message structure and an appropriate protocol. Despite this research is more focused on technical details rather than theoretical aspects, it is another contribution toward trust unification. At the same time, it also intends to speed up the information exchange once the trust and reputation model is determined. Due to the fact that this approach was presented from a technological point of view, Table 1 and, more specifically, Table 2 depict this research as the most underrepresented one regarding properties, features, and components.

Finally, Ylianttila et al. provided a white paper with the most relevant research challenges and recommendations to follow for trust, security, and privacy beyond 5G networks such as the upcoming 6G era [28]. Regarding trust, the authors encouraged its use as a mechanism to ensure secure information exchange with third parties and to protect communicated data from being accessed by unauthorized parties. One of the main recommendations to be taken into account to enable trust network deployment is to assign a global and unique identifier/locator for each device, which was also described by Gómez Mármol and Martínez Pérez [16]. In particular, the authors proposed stable IDs to allow a proper gathering of trust and reputation information, as well as identifying bad or unusual devices' behaviors [28]. Another recommendation, as well as a challenge, is to empower the deployment of a trust management model as a centralized, distributed, or hybrid approach according to use case requirements. Finally, since given benchmarks try to direct the readers toward the generation of trust models as abstract as possible, the authors suggested a set of model components that consists of gathering, processing, storing, distributing stakeholders' evidence, as well as making decisions. This should also withstand common trust and reputation attacks.

Notwithstanding that there is not a standardization proposal [29], a new investigation, centered on 6G initiatives, is currently considering trust as a primordial element in their approaches. Ramezanpour et al. argued the indispensable requirement of integrating zero trust principles into 6G [29]. In this vein, the authors designed an intelligent zero trust architecture (i-ZTA) for untrusted networks which contemplated properties such as dynamicity, context-dependence, and integrity, among others. Furthermore, i-ZTA intended to ensure both data sharing and communications from 5G core to tactical edge networks.

2.2. Research projects toward trust models beyond 5G

Given the massive increase in the number of devices, together with the growth of activities and available connections between devices that interact on the Internet, this entails a rise of possible security risks and threats. The generation of trust models is an engaging field that allows establishing cross-domain network connections reliably, avoiding possible connections that endanger the integrity of user data or compromise the security of service providers and end users. Thence, the trust and reputation model beyond 5G is a topic not widely covered and under the spotlight of some European research projects. In particular, the EU Research and Innovation programme called H2020 [30], in

which both European and US researchers, enterprises, and institutions may work together [31], has financed multiple kinds of researches to cover the current lack of trust standardization. Nonetheless, most of them are in early stages, and consequently, certain information about trust model properties, features, or components is not yet available. In this regard, Table 1 and Table 2 represent the common properties of trust model standardizations found in literature and discussed above.

In terms of potential US research funding sources, we identified a recent National Science Foundation's program that supports research and innovation initiatives via open calls. In particular, the Secure and Trustworthy Cyberspace (SaTC) program endeavors to boost small and medium projects that cope with cybersecurity and privacy risks in society [32]. Among the principal research topics of interest, the National Science Foundation emphasizes the use of techniques for building trust in cyberspace such as leveraging trust frameworks and models in cloud computing environments, considering zero trust architectures, and exemplifying trust via transparency and accountability metrics. Nonetheless, there is not currently a list of proposals accepted, and consequently, the final areas to be addressed by the SaTC calls are not available. It is worth noting that the authors of the present article conducted a review in other US foundations with academic disciplines in computer science such as the Advanced Scientific Computing Research (ASCR), the US. Department of Defense (DoD), and the James S. McDonnell Foundation (JSMF). However, no research projects were found working on 5G trust models. Similarly, China research funding sources such as the 973 Program and the Torch Program were consulted, however, no projects addressing the issue of trust models in 5G were found.

Among the funded H2020-EU projects, 5G-ENSURE started an abstract trust modeling for 5G networks [33]. In this approach, trust is understood as a decision to accept (or not) risks arising from threats. The authors carried out the deployment of an asset-centric tool (named Trust Builder) that identifies threats that may compromise a stakeholder based on links established by assets. For threats identification, they used a set of ontologies to represent primary and secondary (they are propagated through the system) security threats associated with assets and different use cases. After that, a set of security measures (controls) is supplied to prevent them and establish which is responsible for each control. Global trust among stakeholders is determined from a list of primary and secondary threats that generate the increase or loss of trust, and therefore the establishment of a network connection between them. But, from our standpoint, this trust model is mainly centered on risk determination and mitigation, but it does not consider a set of common characteristics that other trust and reputation models have; for instance, indirect recommendations, forgetting factor, or even the definition of trust components or modules.

Another H2020-EU project is Cyber-Trust that deals with cyber-intelligent threat information gathering to cover some IoT security challenges [34]. Although the focus of this project is related to the detection and mitigation of risks, vulnerabilities, and threats, also contemplating Trust Management Systems (TMS) benefits. To this effect, they make use of a trust system management that has a central role in the Cyber-Trust platform since it is responsible for calculating both trust and risk levels. Then, these scores are used to trigger actions that redefine current communication rules and serve as a link to peer-level trust management systems for exchanging trust assessments. As this project is underway, there is not much information that is currently available. So, we are aware of the TMS contains a gathering information component/module that collects information from a vulnerability database, network architecture, and asset repository, among other sources. As well, the TMS calculates overall trust and risk scores and stores them in a database, and finally, it decides to accept or reject requests for the Cyber-Trust system modules. In short, the available information at this moment does not provide technical details but verifies that the system complies with the basic modules of information collection, computing, storage, and dissemination. We hope that next reports provide more technical details to compare synergies between trust models beyond 5G and the trust (pre)-standardization approaches.

Given the relevance of trust and reputation models in 5G telecommunication networks, not only 5G-ENSURE, Cyber-Trust, and SaTC consider the trust factor in their proposals. INSPIRE-5Gplus is another H2020-EU project that envisages trust management as an essential property [35]. Notably, INSPIRE-5Gplus aims to develop a trustworthiness end-to-end smart network and service security management framework across multi-domains. Even though INSPIRE-5Gplus is in an early stage, it is possible to identify that a trust manager mechanism will be developed to gather trust and reputation information from Secure Service Level Agreements, among other dimensions. This information acquired from multiple monitored 5G entities will be measured and assessed through multiple trust levels. After that, it will be shared with end users in 5G virtualized networks and security management entities in a safe and trustable way. INSPIRE-5Gplus will also consider the main components that trust model (pre-)standardization proposed years ago.

Finally, another ongoing European research project is MonB5G [36], which is focused on distributed management of network slices. Despite the project is not centered on trust models or trust management approaches, it considers trust-based mechanisms as a method capable of efficiently assisting in the security of network slice management. For this reason, MonB5G attempts to carry out a deliverable where trust models and trust management approaches will be addressed. Nonetheless, and as the previous projects Cyber-Trust [34] and INSPIRE-5Gplus [35], it is also in an early stage, and hence, we are not able to know technical information regarding trust model or trust management approaches that they will utilize. Nonetheless, it is imperative to highlight another research project beyond 5G [37] contemplating trust model as a mechanism to help increase the security level of various environments that make up 5G networks. 5GZORRO aims to design a security and trust framework integrated with 5G service management platforms, by following zero trust principles in distributed multi-stakeholder environments [37]. It is worth noting that our reputation-based trust model, being presented in this article, is inspired by the 5GZORRO trust objectives.

2.3. Trust model standardization from regulatory organizations

Regulatory bodies, together with investigation groups and projects, are interested in trust concept unification to homogenize trust enforcement both in industry and in the research field. In this regard, there are more and more proposals recorded with the aim of standardizing trust models or even providing trust architectures that consider the most pivotal fundamentals. Table 1 and Table 2 compare the main properties, features, and components took into account by them.

Among regulatory bodies involved, we can stand out the International Telecommunication Union (ITU), particularly a subgroup dedicated to providing recommendations named ITU-T. This regulatory body has multiple documents related to trust considerations such as ITU-T Y.3052 [38], Y.3053 [39], and Y.3054 [40].

In the case of the ITU-T Y.3052, it is concentrated on trust provisioning in ICT infrastructures and services. Nevertheless, trust is addressed as previous trust model standardizations. ITU-T Y.3052 tackled paramount features and introduced the main modules/components to develop a trust framework. About features, ITU-T Y.3052 contemplated two main sources, direct trust and indirect trust. It is worth pointing out that the trust concept may also cover security and privacy aspects, which broaden trust boundaries as well as contributing to generate a more complete trust model (see Fig. 1). Finally, this recommendation document took into account a set of processes for trust-provisioning (data collection, management, analysis information, dissemination, and trust information lifecycle management), which coincides with standardization proposals such as Gómez Mármol and Martínez Pérez [16], Costagliola et al. [21], and Ylianttila et al. [28]. The data collection, management, analysis information, and

dissemination are mapped with the information gathering component, and the trust information lifecycle management covers the trust calculation, storage, and decision-making components (see similarities between Table 1 and Table 2). Two principal absences were identified in this document. Trust provisioning was only applied to end users (ICT context) so trustworthy end-to-end relationships were not guaranteed, and on the other hand, requirements and KPIs beyond 5G networks were not taken into account because this approach was proposed considering the needs of 2017 networks.

In the case of the ITU-T Y.3053 [39], it was a trustworthy networking conceptual model that included features and requirements of identification, trust evaluation, and trustworthy communication. In the manner of Gómez Mármol and Martínez Pérez [16], Bøegh and Yuan [17], Costagliola et al. [21], and Ylianttila et al. [28], it was also in favour of using IDs to identify network elements and build trust relationships. It should note that ITU-T Y.3053 boosted a trust-centric network domain, in consequence, some high-level or functional requirements could not be applied. Among them, we can emphasize the trustworthy communication links based on trust level properties, the trust information lifecycle management support, and the domain policies settlement. Last, but not least, the ITU-T Y.3054 contemplated the use of trust as a feasible mechanism to dwindle risks in media server [40]. In this sense, the ITU-T Y.3054 presented a group of trust requirements that trust-based media services should support. These were divided into the main trust model components: trust data collection, trust analysis, trust application, and trust management. Among the most relevant requirements, we can identify the pre-processing of collected data, trust quantification (i.e., a real number), ID management, applying analyzed trust to content, multiple trust evaluation methods, and so on. In the end, the ITU-T group was the pioneer in identifying a small set of requirements associated with trust and reputation models. Nonetheless, ITU-T Y.3054 did not contemplate other paramount properties of trust and reputation models such as recommendation's credibility, user's satisfaction, or forgetting factor, which guarantee an accurate and trustworthy model.

Similarly, the ITU-T X.5Gsec-t group is developing a security framework based on trust relationship for a 5G ecosystem [41]. Despite the initiative is at an early stage, it is possible to pinpoint multiple key ideas under its framework. The main goals are to (i) recognize stakeholders involved in a 5G ecosystem for detecting usual threats, along with assigning their security responsibilities, and to (ii) determine security borders among stakeholders as well as establishing a security and trustworthiness relationship. Currently, among the most relevant trust factors, the proposal introduces reputation, ability to execute contracts, promise-broken punishment, and independence. In this vein, trust level is also influenced by the importance of assets, geographic scope, and severity that will allow obtaining different trust levels divided into low, medium, and high trust. As stated above, it is still a draft that needs to mature in future iterations, so there are unknown notions such as the expansion of the current trusted properties, the techniques used to determine trust level, how the trust level will be penalized through promise-broken punishment mechanisms, and so on.

The International Organization for Standardization (ISO) is also another regulatory institution that is interested in the use of trust as an enabler to enhance information technology. Specifically, through ISO/IEC TR 23186:2018 it is endeavored to increase security and trust levels of multi-sourced data processing in cloud computing [42]. The ISO developed a framework of trust for the handling of multi-sourced data that covered data use obligations and controls, data provenance records, quality and integrity, chain of custody, immutable proof of compliance, security, and privacy. Even though the previous document is classified as a non-open source of information, its purpose is mostly focused on identifying trust elements that guarantee reliable data processing. Thus, the ISO considered properties such as chain of custody, immutable proof of compliance, quality and integrity of data provenance, and so on. Nevertheless, no trust features, modules, and phases have been recognized among the main themes of the document.

Another regulatory body is the National Institute of Standards and Technology (NIST), which recently presented a Zero Trust Architecture (ZTA) [10]. This technical report mainly introduced basic concepts and logical components that any architecture must contain for fulfilling a zero trust approach. Regarding basic concepts and meaning of zero trust, this approach considered multiple properties that previous trust model (pre-) standardizations, both research papers and research projects, had in mind. One of the most relevant properties is the continuous analysis and evaluation of assets and subjects trust, which was previously introduced as dynamic trust in Trček [15], Gómez Mármol and Martínez Pérez [16], Costagliola et al. [21], and Kanwal et al. [23]. Besides, the ZTA ought to be applied to end-to-end relationships using an access control mechanism to determine who (or which entity) owns the necessary permits. Another property shared with previous proposals was the forgetting factor [15], [16], [17], and [19] in the sense that two requests for the same resources, after a while, will need a new establishment of trust. In addition, the ZTA also contemplated new or missing features such as avoiding implicit trust, i.e., mistrust of resources or entities within the same organization, time limited to resources together with access control and policies, and non-transitive [21], in the vein of two requests to two resources (at the same time and provider) require two trust evaluations. Even though the ZTA proposal was centered on zero trust in the business security environment, many considerations and characteristics can be introduced to other environments. Similarly, other considerations may be applied to the ZTA approach in order to cover some missing points such as subjectivity problem (avoid misinterpreting of a personalized trust evaluation), user's satisfaction, recommender's credibility, or how to quantify the trust score.

To conclude, Table 1 and Table 2, which are related to subsections 2.1, 2.2, and 2.3, summarize the main characteristics collected from trust and reputation model standardization proposals. It can be appreciated how the last years have grown the number of papers, projects, and regulatory organizations interested in such topic. From the properties point of view (see Table 1), it can be esteemed as the dynamicity, context-dependence, and the use of infinitesimal values (i.e., continuous [43] or discrete [44] quantitative values) underline a clear trend over the years. Nonetheless, there are other properties such as entity identity (identification, authentication, and authorization) and privacy-preserving that have gained more bearing in recent years, even though there were previous ground-breaking approaches which took into account ([16], [17], [22], [23]).

In the second place, Table 2 also highlights interpretation and design movements of trust and reputation models in multiple environments. Not only features such as direct and indirect trust were identified as a basis of all trust and reputation models over the years, but also the consideration of essential components or modules that make up such models. In fact, the last one (the Reward & Punish component) was underrepresented from 2014 to 2020. It might be associated with the settlement of general actions under those components, and therefore, they did not focus their researches on the adaptation or improvement of the components but the identification of features and properties. Afterward and due to the emergence of novel decentralized technologies along with 5G networks, researchers and regulatory organizations have newly considered the investigation and adaptation of trust model components as a theme to be treated in order to adjust outdated trust models to new requirements and characteristics beyond 5G scenarios. Similarly, other features such as resilience attacks were also contemplated to cover previous absences.

To the best of our knowledge, multiple trust standardization models were proposed over the years, nevertheless, no pre-standardization trust and reputation model has been found that contemplates a set of abstract requirements and KPIs beyond 5G as a basis for their generation. By means of investigation tackled in Section 2, it was possible to identify multiple sets of requirements and KPIs. Thus, Section 3 gathers pre-5G and new 5G/B5G requirements and KPIs for suitable trust and reputation models. In the same way, the notions learned through this section

boost to propose our recommendations to assemble abstract trust and reputation models aligned with the 5G ecosystem. As it can be appreciated in Table 1 and Table 2, our model endeavors to cover some absences identified in the literature such as considering user's satisfaction, recommender's credibility, forgetting factor, or privacy-preserving. At the same time, the reputation-based trust model proposed in this manuscript overcomes feasible security threats like the duplication of identities by not contemplating a mechanism to identify the users involved in the trust model (see identity property in Table 1). Similarly, our model also considers a reward and punish mechanism (see components in Table 2) to encourage honest users' behavior as well as to provide truthful recommendations. More information on the challenges addressed and the considered techniques are detailed in Section 4.

3. Requirements and KPIs progression from pre-5G to beyond 5G

Notwithstanding that the trust model concept is familiarized for ages, these are constantly being iterated, adjusted to current needs and environments, and improved. It is for this reason that although such models continue to have a multitude of similarities such as properties, features, or even modules that make them up, in contrast, the requirements and KPIs have varied over time. Standardly, the requirements are understood as a set of specific needs that a trust model must meet to communicate with other entities. On the other hand, KPI means a kind of metrics that allow identifying through the deployment of the requirements, if minimum performance measures are met. One of the reasons why requirements and KPIs evolve is due to their close relationship to the technologies, the development environments, trust model scope, and so on. In this sense, requirements and KPIs are concepts to be examined in trust models, and consequently, this section pinpoints the key requirements and KPIs from previous trust model standardizations, how these standardizations satisfied them, and how requirements and KPIs are evolved toward 5G trust models.

Table 3
Requirements of pre-5G trust model standardizations.

ID	Requirement	Refs.
Pre5G-R1-H	Trustworthiness model should be public	[17]
Pre5G-R2-H	Trust models should have a layered architecture	[16,19]
Pre5G-R3-H	Generating fundamental concepts (ontology)	[21]
Pre5G-R4-H	Equal access to data should be a basis for information gathering	[17,21]
Pre5G-R5-F	Entities should have a real, known, and privacy-preserving identifier	[16,17]
Pre5G-R6-F	Auditing of actions related to trust models should be available	[17]
Pre5G-R7-F	Trust evaluation should be based on objective evidence and not biased	[16,17]
Pre5G-R8-F	Active and passive information gathering mechanisms	[16,17,19–24,28]
Pre5G-R9-F	Trust models should be able to discriminate incorrect ratings	[22]
Pre5G-R10-F	Trust models should be evaluated using a sufficient amount of information	[22]
Pre5G-R11-F	Entities should not be able to supply or compute its own trust score	[22]
Pre5G-R12-F	Newcomers should not gain advantage and be penalized	[16,22]
Pre5G-R13-F	Trust models ought to identify and mitigate common trust attacks	[16,17,21]
Pre5G-R14-F	Trust models should not introduce a high bandwidth and energy consumption overload	[16]
Pre5G-R15-F	Trust assessments should be classified by levels, ranges, or any other representative measure	[15–17,19–23,27,28]
Pre5G-R16-F	Trust values should be saved for future evaluations	[16,21]

Pre5G: Requirement prior to 5G.

Even though previous trust model standardization proposals were focused on a multitude of areas and environments, this section also recaps a set of abstract requirements and KPIs which might be applied in most scenarios. In addition, summary tables with the most relevant requirements (see Table 3, Table 4, and Table 5) and KPIs (see Table 6 and Table 7), from previous standardizations and future trust models beyond 5G, are located at the end of each subsection. Note that the requirements are divided into two main sorts, high-level (H) and functional (F), representing abstract properties that trust models ought to consider and depicting technical characteristics of configuration or deployment, respectively.

3.1. Pre-5G trust model requirements

Before introducing the set of high-level and functional requirements, it is required to mention the nomenclature to be employed. In particular, pre-5G trust model requirements are going to be expressed as *Pre5G-Rx-H* or *Pre5G-Rx-F*, where *Rx* is the number associated with the requirement; *H* means high-level; and *F* stands functional. It should be pointed that the number of requirements in Table 3, Table 4, and Table 5 is based on the least forcing thread of storyline.

In the case of Gómez Mármol and Martínez Pérez [16], they introduced multiple transcendental requirements. First and foremost, they presented a high-level trust model architecture (Pre5G-R2-H) and considered entity identification (Pre5G-R5-F) to prevent a malignant entity (Pre5G-R13-F) from exiting and entering system without being penalized, or even with a higher trust score in the event that it was

Table 4
Requirements for 5G and beyond 5G trust models.

ID	Requirement	Refs.
(B)5G-R1-H	Trust as a distributed service	[35,37]
(B)5G-R2-H	Trustworthiness relationships should be established end-to-end	[10,33,35,37]
(B)5G-R3-H	Trust communications should be intra- and inter-domain	[10,35,37]
(B)5G-R4-H	Trust models should be compatible with zero-touch network and service management	[35,37]
(B)5G-R5-H	Zero trust is an essential approach for trust models	[10,37]
(B)5G-R6-H	Zero trust should contemplate policies based on dynamic risks	[10]
(B)5G-R7-H	Trust models should be efficient and scalable	[10,33–37]
(B)5G-R8-H	Trust assessments should have a maximum time slot and consider task sensitivity	[10,37]
(B)5G-R9-H	Trust computation should be evaluated before providing access over resources	[10,33–37]
(B)5G-R10-F	Trust establishment processes should provide an automatic renegotiation when an entity is joining or leaving a trust link	[37]
(B)5G-R11-F	Information gathering should be a continuous process	[10,37]
(B)5G-R12-F	Pre-processing of collected data is necessary	[40]
(B)5G-R13-F	Trust information lifecycle management should be made up of planning, creation, allocation, modification, and deletion	[34,37,39]
(B)5G-R14-F	Interfaces for exchanging trust information is required	[37,40]
(B)5G-R15-F	Trust models should take into account domain policies	[35,37,39]
(B)5G-R16-F	Trust models should not rely on their default domain entities	[10,37]
(B)5G-R17-F	Trust models should make a decision on routing paths of incoming/outcoming packets according to trust levels and domain management policies	[33–35,37,39]
(B)5G-R18-F	Privacy-preserving for user data should be guaranteed	[10,33–37,40]

(B)5G: 5G and beyond 5G requirement.

Table 5
Requirements for 5G and beyond 5G trust models previously considered.

ID	Requirement	Refs.	Prior Reqs.
(B)5G-R19-F	Trust models can also cover security and privacy aspects	[10, 33–38]	Pre5G-R5-F, Pre5G-R13-F
(B)5G-R20-F	Entities' trust model should be managed by identifiers and locators	[10,37, 39]	Pre5G-R5-F
(B)5G-R21-F	Information gathering should be carried out from multiple sources	[37,40]	Pre5G-R8-F, Pre5G-R10-F
(B)5G-R22-F	Trust values should be quantized	[33–37, 39]	Pre5G-R15-F
(B)5G-R23-F	Trust values should be stored to keep the track over time	[37,39]	Pre5G-R16-F
(B)5G-R24-F	Trust levels should be validated after trust evaluation process	[39]	Pre5G-R6-F
(B)5G-R25-F	Trust models should consider IDs and locators for access and delivery control	[10,37, 39,40]	Pre5G-R5-F
(B)5G-R26-F	A newcomer should possess a regulated initial trust	[37,40]	Pre5G-R12-F
(B)5G-R27-F	Trust models should withstand and detect common attacks	[37]	Pre5G-R9-F, Pre5G-R13-F

(B)5G: 5G and beyond 5G requirement.

considered a newcomer (Pre5G-R12-F). This pre-standardization approach not only contemplated direct trust experience but also recommendations or opinions (Pre5G-R8-F). At the same time, they took into account the overload (Pre5G-R14-F) that trust models may generate over the systems. In this vein, it is essential that trust models cut down on bandwidth and energy consumption as much as possible, otherwise, it can be a drawback when introduced into environments as Wireless Sensor Networks, among others. Finally, Trček [15] and Gómez Mármol and Martínez Pérez [16] declared that trust evaluations need to be quantized (Pre5G-R15-F) and they should be stored to have a basis for future relationships with the same entities (Pre5G-R16-F) [16].

In the case of previous trust model requirements, by means of Bøegh and Yuan [17], we can identify an initial set of requirements that trustworthiness management systems had. The trust models should present a public schema (Pre5G-R1-H) to enable other entities to reproduce the same steps. In this regard, the trust model introduced transparency in allowing other authors to iterate on the model if certain shortcomings are detected. Via public schemas, it was also possible to audit some actions regarding trust models (Pre5G-R6-F), in the sense of checking misconduct and likely finding out conventional trust attacks. With regard to misbehavior checking, it was established the need for uniquely identifying all entities participating in trust models (Pre5G-R5-F). Through these identifiers, it would be possible to carry out several actions such as registration, identification, authentication, and authorization (Pre5G-R4-H) of all parties involved, and even to tackle well-known trust attacks such as the Sybil attack (Pre5G-R13-F). Lastly and like Gómez Mármol and Martínez Pérez [16], Bøegh and Yuan also declared another basic requirement, the use of objective evidences (capability and performance) which allows making and getting more trustworthy assessments (Pre5G-R7-F) [17].

Through Vinkovits' research [19], it can be recognized requirement of employing a clear and layered trust architecture (Pre5G-R2-H) that facilitated the division of a trust model into submodules or components, thus allowing the main tasks of the model to be identified more quickly. In order to converge toward a shared ontology of trust models, Costagliola et al. proposed to generate fundamental concepts (ontology) for reusing metrics and parts of trust models (Pre5G-R3-H) [21]. In this way, the author also introduced requisites regarding the mechanism for obtaining as many trust features (active or passive) as possible (Pre5G-R8-F) and controlling the access to the same information by entities involved (Pre5G-R4-H). Additionally, their pre-standardization approach also looked at resilience to common attacks (Pre5G-R13-F) such as ballot stuffing, Sybil attack, whitewash, etc.

In the Vavilis et al.'s work [22], the authors elicited the main requirements for reputation systems together with features needed to fulfill. Among the most relevant ones were the discrimination of incorrect ratings (Pre5G-R9-F) to increase accuracy system, as well as considering multiple dimensions (Pre5G-R8-F) to assess another entity with a minimum amount of trust information (Pre5G-R10-F). In addition, a newcomer entity should not gain advantages nor be penalized (Pre5G-R12-F), as well as entities should not be able to modify or calculate their own trust values (Pre5G-R11-F). Thus, considering the previous requirements described by Vavilis et al. [22], our trustworthiness model will endeavor to avoid a set of malicious practices that could lead to a lack of precision in the measures and the arrival of attacks. With a view to solving the previous requirements, the authors introduced some features in their model such as determining trustworthy users along with characterizing their behavior (Pre5G-R9-F), considering additional trust information if needed (Pre5G-R10-F), protecting trust values against unauthorized manipulation (Pre5G-R11-F), and determination of default values carefully (Pre5G-R12-F).

3.2. 5G/B5G Trust model requirements

As above-mentioned, the trust field continues to progress constantly, and in fact, in recent years with the arrival of 5G new needs have emerged which should now be covered. The end-to-end trustworthiness chains, the automation of processes driven by novel zero-touch approaches, and the circumvention of default trust are just some aspects that 5G/B5G trust models should address. These new aspects are the reason why trust models need to be adapted to new technologies, services, stakeholders, and environments that appear from 5G enablers. In this sense, and after realizing in-depth research in current trust model papers, investigation projects, and regulatory bodies, Table 4 underlines the most relevant requirements that were not considered by previous proposals and they play a pivotal role to fulfill the 5G/B5G needs. In this case of 5G/B5G trust model requirements, Table 4 follows the nomenclature *(B)5G-Rx-H* or *(B)5G-Rx-F*, where *(B)5G* stands 5G and beyond 5G; *Rx* is the number associated with the requirement; *H* means high-level; and *F* stands functional.

Among the new requirements that should be contemplated in refreshing 5G trust models, we can highlight novel end-to-end trust relationships ((B)5G-R2-H) since previous proposals mostly supplied trustworthiness to specific network segments. Another eye-catching characteristic is related to a trend of decentralized trust models ((B)5G-R1-H) as well as the elimination of a central trustor entity. The arrival of distributed ledger technologies (DLTs) has introduced improvements such as multi-domain interconnection ((B)5G-R3-H), data immutability, security by cryptography, privacy-preserving ((B)5G-R18-F), and shared data among peers ((B)5G-R14-F). In concert with DLTs and distributed environments, future trust models ought to incorporate intra- and inter-domain policies ((B)5G-R15-F) that allow adjusting current decisions to dynamic risks ((B)5G-R6-H), task sensitivity ((B)5G-R8-H), previous interactions, trust scores ((B)5G-R17-F), and so on. An initiative powered by the NIST [10], and also considered in trust models beyond 5G, it is the absence of trust ((B)5G-R5-H, (B)5G-R16-F) between entities in the same domain, between entities with previous relationships, or between entities before requesting access to a service or resource ((B)5G-R9-H). In order to fulfill the zero trust requirement, trust models may make use of access control mechanisms ((B)5G-R9-H) that enable identification, authentication, and authorization of all entities involved in trust processes.

In the end, trust models beyond 5G will facilitate automated,

Table 6
KPIs of pre-5G trust model standardizations.

KPI	Definition	Refs.	Related Reqs.
Pre5G-KPI 1	Trust models will detect malicious collusion generated by Sybil attacks	[16, 21]	Pre5G-R13-F
Pre5G-KPI 2	Trust models will not be mathematical models but deployment models	[19]	Pre5G-R6-F, Pre5G-R10-F, Pre5G-R15-F, Pre5G-R16-F
Pre5G-KPI 3	Trust models will provide QoS transparency	[23]	Pre5G-R6-F, Pre5G-R7-F, Pre5G-R16-F

Pre5G: KPI prior to 5G.

efficient, and scalable processes ((B)5G-R7-H), that will empower trust information lifecycle management ((B)5G-R13-F) taking into account general requirements. Thus, trust processes such as data pre-processing ((B)5G-R12-F), information gathering ((B)5G-R11-F), and trust establishment ((B)5G-R10-F) need to be automatized as far as possible to comply with innovative zero-touch approaches ((B)5G-R4-H). In this vein, it is hoped the set of abstract requirements identified in Table 4 (together with Table 5) afford generating an abstract trust model which boosts its subsequent application within the wide variety of scenarios envisaged in 5G.

After eliciting the most relevant requirements from previous trust model standardization documents on the state-of-the-art (see Table 3), and what new requirements have been incorporated (see Table 4), the next step is to determine what previous requirements continue to be taken into account in the beyond 5G trust models (see Table 5). Regarding Table 3, many requirements are considered fundamentals, and therefore, they are indirectly propagated toward news trust models. This is the case of Pre5G-R1-H, Pre5G-R2-H, and Pre5G-R4-H that contribute to the creation of a fair trust model. Nonetheless, these requirements are now considered common principles to all trust models beyond 5G, hence they are not introduced as novel requirements, but they are an intrinsic part of the trust models.

About previous fundamental requirements, we also have transitive requirements which are still contemplated in 5G trust models. These requirements address similar objectives, but they are partially rewritten from functionalities and characteristics of current technologies and deployment environments. By means of these requirements, 5G and B5G trust models not only preserve a common basis with other previous standardizations but also allow enforcement with previous scenarios and networks. In order to stand out these transitive requirements, Table 5 groups the most essential ones. In the case of previous requirements about data privacy-preserving (Pre5G-R5-F) and user protection (Pre5G-R13-F), the requirements (B)5G-R19-F, (B)5G-R20-F, and (B)5G-R25-F intend to cover the main objectives, however, the current technologies working on privacy-preserving and user protection areas have evolved. In this sense, trust models beyond 5G could utilize new approaches such as decentralized identity management [45] that supports a distributed trust model. Similarly, other matches can be detected in requirements Pre5G-R6-F regarding trust model auditing and Pre5G-R12-F about inappropriate default value for newcomers. They are subsequently tackled in 5G trust models via (B)5G-R24-F (trust levels verification) and (B)5G-R26-F (regulated initial trust value), respectively. Finally, there are also previous requisites such as information acquisition from several dimensions and sources (Pre5G-R8-F, Pre5G-R10-F), utilization of ranges or levels to express trust scores (Pre5G-R15-F), storage of previous relationships and evidence (Pre5G-R16-F), and responding to potential attacks (Pre5G-R9-F, Pre5G-R13-F), that must continue to be dealt even though information sources ((B)5G-R21-F) quantified trust measures ((B)5G-R22-F), the technologies to keep the track over the time ((B)5G-R23-F), or kinds of attacks ((B)5G-R27-F) have progressed over the years.

After introducing the requirements expected for 5G and beyond 5G trust models, it can be observed that only 9 of identified 27 requirements were covered by former trust model proposal standardizations (see Fig. 2). This is due to the fact the 9 orange hexagons allude to transitive requirements from prior 5G trust models to 5G and B5G trust models. In other words, requirements previously defined before 5G and partially rewritten to be compatible with the current technologies and deployments scenarios. Conversely, the 18 green circles depict novel requirements for 5G and B5G trust models, and because of that, they could not be considered by previous trust approaches and are not linked to previous standardization proposals in Fig. 2. In this vein, it would be advisable to promote new proposals for trust model standardizations that cover the requirements not considered by the current ones. To deal with it, we submit a set of recommendations for reputation-based trust models beyond 5G in Section 4.

3.3. Pre-5G trust model KPIs

Indirectly related to requirements, another measure, which has recently been used at an organizational level, is the KPIs. As mentioned above, these are a sort of quantifiable measurements normally utilized to measure our performance to fulfill positive results. Nevertheless, the KPI concept began to be recently utilized as earlier performance evaluations were not as necessary as they are now. Besides, KPIs tend to be more focused on projects both in the business field and in important RIA-type research (Research and Innovation Actions).

Since the identified European projects are centered on the generation of 5G/B5G technology standards, a subset of KPIs has been perceived through requirements to be met by associated trust models. In this sense,

Table 7
KPIs of 5G and beyond 5G trust models.

KPI	Definition	Refs.	Related Reqs.
(B)5G-KPI 1	Trust models have to automatize trust establishment processes by overcoming a minimum user satisfaction factor	[10,37]	(B)5G-R4-H, (B)5G-R5-H, (B)5G-R7-H, (B)5G-R10-F
(B)5G-KPI 2	Cross-domain trust establishment has to involve more than two stakeholders and establish an end-to-end relationship with the lowest connection attempts per domain	[37]	(B)5G-R1-H, (B)5G-R2-H, (B)5G-R3-H, (B)5G-R4-H, (B)5G-R5-H
(B)5G-KPI 3	Trust information gathering process will acquire data from multiple dimensions/sources	[35–37, 40]	Pre5G-R8-F, Pre5G-R10-F, (B)5G-R11-F, (B)5G-R14-F, (B)5G-R21-F
(B)5G-KPI 4	Trust models will enable its automatic renegotiation with previous entities converging in the lowest algorithm iterations	[37]	(B)5G-R5-H, (B)5G-R7-H, (B)5G-R10-F, (B)5G-R13-F
(B)5G-KPI 5	Trust models will identify and mitigate as many common trustworthiness attacks as possible	[37]	Pre5G-R9-F, Pre5G-R13-F, (B)5G-R19-F, (B)5G-R27-F
(B)5G-KPI 6	Trust models have to bear distributed, shared, cryptographically secure, and immutable technologies	[35–37]	Pre5G-R16-F, (B)5G-R1-H, (B)5G-R3-H, (B)5G-R14-F, (B)5G-R19-F, (B)5G-R23-F
(B)5G-KPI 7	Entities involved in trust models have to possess unique, global, and privacy-preserving identifiers that can be requested in real-time and independently of geographical area	[37]	Pre5G-R5-F, (B)5G-R1-H, (B)5G-R18-F, (B)5G-R20-F
(B)5G-KPI 8	All external trust APIs are expounded via open and public specifications	[37]	Pre5G-R1-H, Pre5G-R8-F, (B)5G-R14-F

(B)5G: 5G and beyond 5G KPI.

Table 6 depicts KPIs regarding trust model standardization papers from Section 2.1 and Table 7 contemplates 5G/B5G KPIs. These KPIs represent three general aspects, but nowadays there are still papers based on trust models that do not comply with them [46,47]. In short, they cover points such as avoiding Sybil attacks (Pre-5G-KPI 1), checking that ideas, equations, and measurements allow satisfying minimum requirements (Pre-5G-KPI 2), and helping other users to reproduce proposed trust models through their features (Pre-5G-KPI 3). Mainly, these KPIs were addressed through an attack detection and mitigation system (Pre-5G-KPI 1), determining use cases where models could be replicated (Pre-5G-KPI 2), and considering non-subjective characteristics that allow honesty of the results of a trust model to be verified as QoS (Pre-5G-KPI 3). As well, Table 6 also contains a column to represent an association between requirements and KPIs (from Table 3), in the sense of how certain requirements will be measured to demonstrate their performance.

3.4. 5G/B5G Trust model KPIs

Regarding trust models' KPIs in 5G/B5G networks, a set of technical indicators have been recognized from the 5GZORRO, INSPIRE-5Gplus, and MonB5G projects, as well as from the ITU-T and NIST organizations. In particular, these KPIs are aimed at the appropriate measurement of the above requirements from Table 4 and Table 5.

In the light of the fact that the authors of this article are involved in the 5GZORRO project daily, together with previous experience from other RIA projects, it was conceivable to discover a subset of realistic KPIs related to trust models beyond a 5G ecosystem. To the best of our knowledge, these KPIs are an abstract basis for trust models, however, some measurements could be slightly adapted to other use cases; for example, the maximum number of connections or algorithm iterations. 5GZORRO expects to improve the current trust model status in 5G networks, thence it contemplates novel technologies, mechanisms, and different use cases where KPIs should be evaluated [48]. Thus, from our point of view along with the ITU-T [40] and the NIST [10] documents, which are leading entities in the development and evolution of technologies, an initial set of KPIs has been obtained (see Table 7). Note that these KPIs do not establish a maximum or minimum number in terms of interactions, attempts, dimensions, and attacks since these values should be finally calculated depending on technologies, characteristics, deployment scenarios.

Among essential KPIs, we have identified a need to introduce an automatization or zero-touch approach into trust models to facilitate and encourage their use while presenting new features of trustworthiness models. Thus, a system could measure the fulfillment of this characteristic from a satisfaction value that involved users would generate based on their own policies, rules, and preferences ((B)5G-KPI 1). There are also KPIs that attempt to check a reasonable performance in end-to-end trust establishment ((B)5G-KPI 2) and to ensure that trust models have enough information sources for avoiding erroneous ratings ((B)5G-KPI 3). Another novel KPI is regarding the measurement of automatic trust relationships renegotiation, which is a trendy approach and needs to guarantee a minimum output based on the required algorithm iterations ((B)5G-KPI 4). Similar to Pre-5G-KPI 1, (B)5G-KPI 5 endeavors to ensure that trust models are resistant not only to the Sybil attack but also to other well-known attacks such as on-off or behavior attacks, among others. On another hand, new indicators like (B)5G-KPI 6 and (B)5G-KPI 7 try to look over whether trust models comply with secure, privacy-preserving, and immutable approaches in real-time, and independently their geographical location. Last but not least, (B)5G-KPI 8 boosts a transparent and open trust model through the divulgation of external APIs used.

After analyzing the requirements and KPIs, both previous approaches and new ones, we can conclude that current trust models have multiple similarities from the previous ones such as some modules or components, properties, and features. Nonetheless, a key effort ought to be

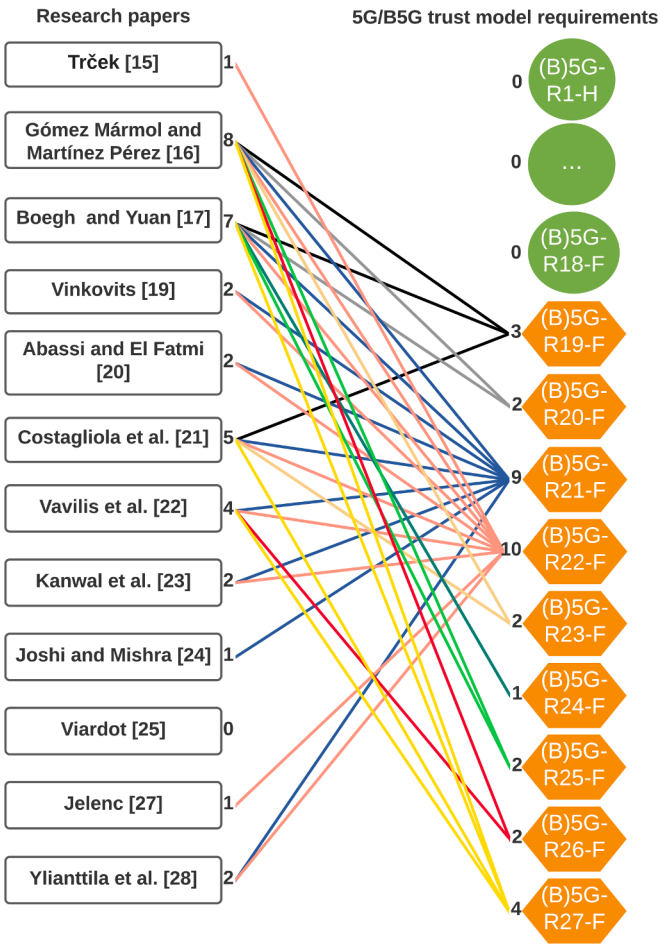

Fig. 2. Matching of previous trust model standardizations and requirements for 5G/B5G trust models.

covered under the adaptation of requirements and KPIs (see orange hexagons in Fig. 3), which have evolved over years to adjust technologies and needs of new era telecommunication networks. As it can be appreciated in Fig. 3, there is still a huge work to include and cover the new requirements and KPIs expected beyond 5G (see green circles), which are also described in Table 4 and Table 7. Lastly, it should be underlined that requirements and KPIs depicted in Fig. 3 are not in any particular order, but it intends to maximize their visibility and for clarity's sake

4. Recommendations for suitable trust and reputation models beyond 5G

Once the current 5G and beyond 5G requirements and KPIs have been identified, this section introduces a set of recommendations so as to design a reputation-based trust model that meets such requirements and KPIs. Thereupon, these recommendations represent the design principles to be followed by high-level trust and reputation models. In addition, the recommendations also propose cutting-edge technologies and approaches that may be contemplated to cover requirements and design universal trust models.

5G networks have a distributed nature that is motivated by the emergence of new technologies and greater interconnection capacity between parties involved. First and foremost, the distributed paradigm is taking advantage of essential 5G characteristics such as speed upgrades, low latency, enhanced capacity, increased bandwidth, availability, and coverage, which enable distributed computing and data processing without compromising user's QoS [49]. In the second place,

the growth of entities able to produce and propagate information has similarly been boosted with the 5G arrival. As a result, intra- and inter-domain connections have been enriched at the same time that a wide amount of information sources and data may help to improve trust model performance. Thereby, trust models should evolve toward new network approaches, technologies, and entity requirements.

In order to incorporate trust as a distributed service, a feasible approach is the incorporation of DLTs into the lifecycle of trust and reputation models [47,50]. In particular, these technologies could be profitable in the information gathering component since they would facilitate data acquisition from multiple sources whereas ensuring data immutability, integrity, and decentralization (integrity property). Furthermore, distributed ledgers may be utilized as an alternative to third trusted parties, which verified the trust in the services and stakeholders [51]. Now, DLTs supply alternatives through their multiples consensus mechanisms, in which a consensus is achieved among all parties in a system [28]. In the same way, the incorporation of these technologies boosts more secure and privacy-preserving trust model approaches. Hence, DLTs also ensure data privacy-preserving through their encryption mechanism so that unauthorized persons cannot retrieve sensitive information. Regardless of the blockchain-type to use, these encourage robust solutions of trust models due to the fact that an entity is able to acquire not only a lot of information but also different kinds of information sources about a specific target, thereby generating a wide dataset.

As aforementioned, trust models should be applied to both intra- and inter-domain communications, and therefore, these ought to contemplate a novel principle named zero trust [10]. By means of a zero trust approach, all models must compute an entity's score regardless of whether it is in a given trusted domain or another, whether it calculated a former trust relationship with that device or entity, or whether it is performing other different workloads with that same entity. Considering conventional trust models did not contemplate this property, which has been encouraged by the current large attack surface [52], it might be addressed through providing a set of policies and rules based on dynamic intra- and inter-domain risks [10]. At the same time, trust models should also preserve their essence, in the sense of not losing efficiency and scalability while introducing advances such as automation through machine learning [53] and deep learning [54] techniques, also known as zero-touch approaches.

After suggesting a subset of initial recommendations that trust and reputation models beyond 5G should tackle independently of the components or modules that make them up (see Fig. 4), the main recommendations of each module will be described below. Note that these modules and recommendations are inferred from the analysis of the state-of-the-art in Section 2 as well as the compliance with the requirements reported in Table 4 and Table 5 and the KPIs described in Table 7.

First and foremost, we propose a high-level reputation-based trust model considering the most universal modules contemplated by other trust approaches, which will be presented one by one together with their objectives, key functionalities, and features (see Fig. 5). In this vein, our reputation-based trust model allows its adaptation and integration in any 5G ecosystem, owing to its abstract layer descriptions.

4.1. The information gathering module

In the standard way, the first module of a trust and reputation model carries out data recollection. The *Information Gathering* should not be contemplated as a one-time process, which only gets information before establishing a relationship, but as a *dynamic* process that must continue because trust varies over time. In this regard, a trust and reputation model should define mechanisms such as predictors, triggers, and rules that enable the detection of irregularities in the data collected, trust threat predictions, and changes in trust relationships, among others (context-dependence property). Afterward, these events lead to the recalculation or the cessation of trust level. The detection of tampered trust values could be managed as a step within *data pre-processing*, through several techniques as perceptron detection [55] or consensus protocols after adding information to a blockchain [56]. Nonetheless, it is also true that the greater the number of reliable sources from which to obtain information, the greater the probability and easiness of detecting changes in the data. Hence, it is paramount that the information gathering process is carried out from multiple information sources and entities. Another widespread pre-processing step, and partially related to data manipulation, is the detection of common trust threats such as Sybil attack [57], collusion attack [58], bad-mouthing attack [59], subjectivity problem [60], etc. These threats may directly affect trust and

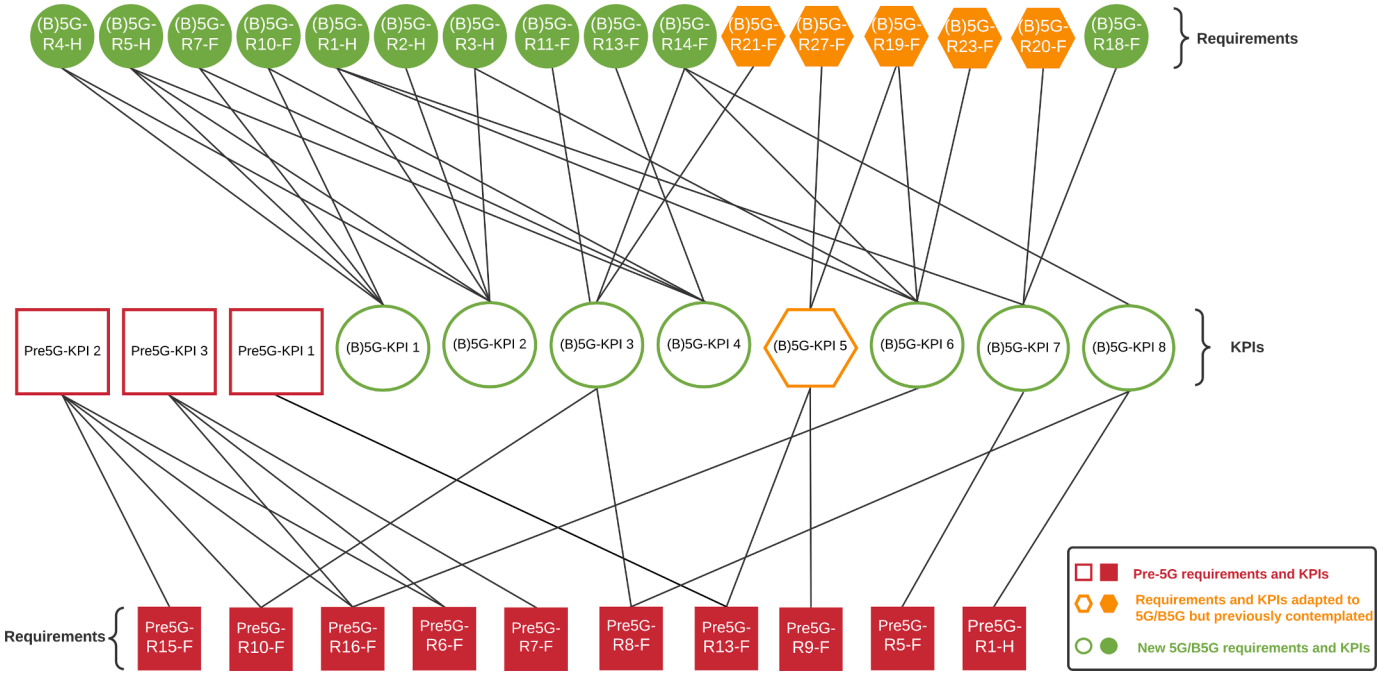

Fig. 3. Requirements and KPIs clustering in pre-5G, 5G, and beyond 5G.

reputation models' performance so they should be had in mind and addressed through the recommendation feedback mechanism and a threshold mechanism of credibility recommendation [61].

Furthermore, these initial data *recollection* steps ought to contemplate automatization themselves since a novel requirement beyond 5G network is the *zero-touch* approach [10], which is linked to end-to-end establishments. Due to current trust and reputation models should be able to generate cross-domains and end-to-end establishments, more than two stakeholders could be involved in the final trust score computation. Thereupon, multiple events such as proactive Service Level Agreement (SLA) renegotiation [62] or security incidents among involved parties [6] can occur suddenly, and in consequence, they may imply a trust automatic renegotiation when an entity is joining or leaving a trust link. Similarly, Smart Contracts (SCs) could provide a self-contained trust network by automatically triggering trust network functions based on previous trust relationships [28]. Therefore, our trust and reputation model should tackle the necessary calculations associated with possible entities entering or leaving the trusted link automatically. At the same time, this process should guarantee a minimum user's satisfaction and minimize the impact on the end user (satisfaction feature). For instance, after a trigger event identification, a subset of feasible intermediate nodes could be contemplated to cover the absence of a node that could leave the trusted link [63].

In the end, after performing these steps related to the *Information Gathering* module, our trust and reputation model processes the information in two ways. In the first place, *direct trust* contains information acquired by means of previous interactions with a particular stakeholder. Conventionally, *direct trust* has a greater weighting in obtaining a final trust and reputation score. Nevertheless, the weighting should be determined based on use case properties. In the second place, *indirect trust* includes information received from third parties (also known as recommenders). The *indirect trust* is calculated when a recommender, not directly involved in the current trust computation, supplies information about a trustee involved in the trust computation.

4.2. The trust computation module

Once data gathering is carried out successfully, the next module is the *Trust Computation* where calculation and decision-making processes would be handled. Before determining an entity's trust score, other considerations should be thought as newcomer treatment without information or how the trust level will be depicted.

On the one hand, a trust and reputation model might likely face a scenario where it cannot acquire information from trustees (newcomers) through the available collection mechanisms. In that case, a trust model ought to allow the newcomer participation in the system, and therefore, an initial trust score should be determined. To cope with it, a trust and reputation model may consider a stereotyping approach that affords for a tentative trust evaluation about *newcomers* through previous experiences with known entities [64]. Nevertheless, this situation implies critical decisions that should be considered [16]. First, newcomers should not possess more privileges than malicious entities detected by any trust and reputation model, avoiding that the last ones can create new identities to acquire more opportunities. Secondly, newcomers should also have the opportunity to be selected as trustworthiness nodes. Finally, the newcomer's trust score should increase little by little to avoid reaching a high trust score and then carrying out misbehaviors for a long time. Therefore, all these decisions should be taken into account when developing the trusted computing module.

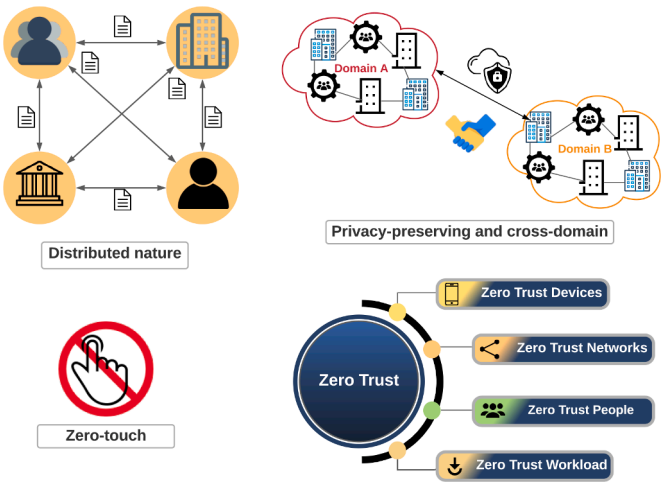

Fig. 4. Initial recommendations for trust and reputation models beyond 5G.

Apart from these starting considerations, a trust and reputation model should palliate other pivotal factors linked to trust computation such as degradation of time (also known as forgetting factor), user's evaluation credibility, or trust dimension weighting, among others. These factors are considered traditional trust concerns, and therefore, there are several solutions that could be applied. However, they should not be dismissed from our model. Regarding the forgetting factor, multiple solutions may be leveraged as providing more weight to recent evaluations [65], or considering more elaborated techniques as an adaptive forgetting factor using the Gompertz function [66]. The latter permits to adapt each forgetfulness factor with the trustee's honesty, as well as mitigates on-off attacks. In the case of user's credibility, his/her subjective opinion could be checked through the divergence between user's rating and cloud's current performance, by comparing the predefined SLAs and the monitoring values [67] (credibility feature). Last, the trust dimension weighting is usually tackled by giving higher relevance to own opinions (direct trust) instead of recommendations (indirect trust) [63].

On the other hand, how trust score would be *quantized* and represented is another key point (infinitesimal property). Up until now, there is not an agreement on standard terms of quantifying trust cross-domains [28]. Consequently, there are multiple ways to express a final trust score. From our standpoint, the utilization of continuous quantitative values (thresholds) associated with the definition of trust levels may be one of the most appropriate ways. By means of this approach, it would be feasible to establish a subset of generic intra- and inter-domain trust levels (employing labels), even though threshold values vary depending on intra-domain policies, rules, interests, priorities, etc. Then, through recommendations (values plus labels or only labels), a trustor could more easily interpret external recommendations. Therefore, considering trust level labels as a measure to be shared when a trustee provides recommendations to a trustor, the subjectivity problem from indirect trust could be partially avoided in our trust and reputation model (subjectivity problem feature). It is worth mentioning that a trust score of trustor on a trustee cannot be indirectly applied in the other side of a relationship (asymmetry property). Similarly, an entity must avoid implicit trust on another one as two entities A and C may trust an entity B, however, entity A does not trust entity C by default and vice versa (transitivity property). Last but not least, the decision-making process would carry out the corresponding actions taking into account the previously predicted trust score. In this sense, internal policies, rules, or other mechanisms will establish the criteria to be followed.

4.3. The trust storage module

Considering trust deterioration and as a basis of trust and reputation models, trust score is continuously being updated since external events might appear and have a direct influence on entities enrolled. In consequence, all information collected during the *trust model lifecycle* (i.e., features, events, policies, rules, trust scores, user's reputations, and so on) needs to be stored not only to enhance future predictions but also to help meliorate the overall system through recommendations. Multiple

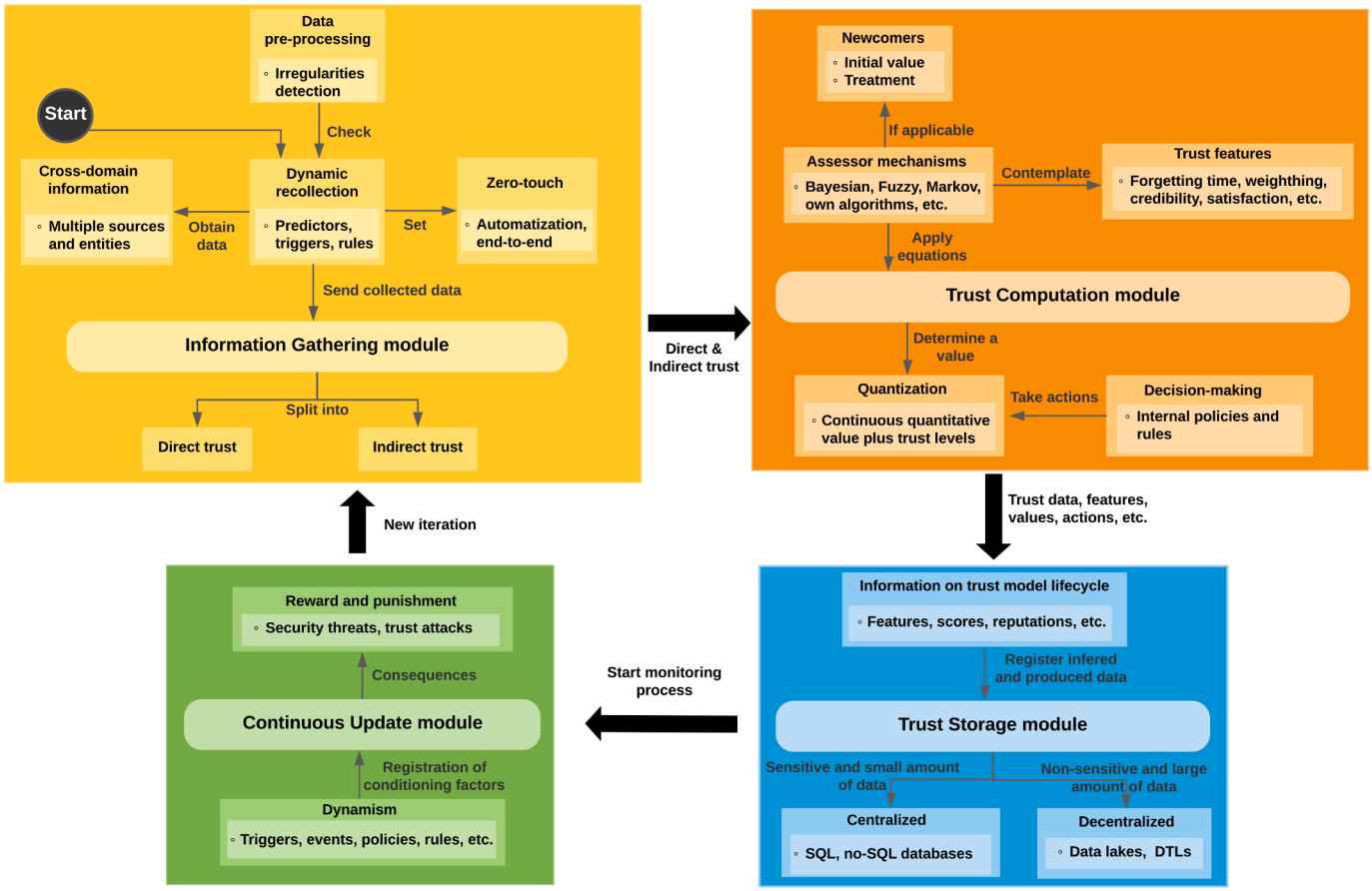

Fig. 5. Overview of trust and reputation model modules.

options may be considered for data storage, however, they are normally linked to the amount of data that is handled in the system and environment properties.

The *Trust Storage* module solutions could range from cloud storage as data lakes [68], which have a high raw data storage capacity and is usually used for tasks such as reporting, visualization, advanced analytics, and artificial intelligence, to conventional databases based on SQL and no-SQL approaches [69]. In fact, in cases where data related to trust relationships are not too heavy, and therefore do not trigger performance problems, they could be stored on a distributed ledger [70]. Thus, this on-chain storage enables a long-term reputation reflecting the trustworthiness of parties involved in the system, whereas characteristics such as information decentralization or immutable storage are also covered. In addition, a centralized database can be utilized as a local repository where only stakeholders of a domain may register private data with respect to recent trust interactions, internal policies, and rules that they cannot share with other parties. On the contrary, non-sensitive information, which may be partially/totally shared with other stakeholders, can be stored on decentralized approaches such as Data Lakes and DLTs.

4.4. The continuous update module

In spite of traditional and novel trust and reputation models present a sort of different characteristics and requirements as aforementioned (see Table 3 and Table 4), they also share similarities to achieve efficient systems (see Table 5). In addition to that, and considering requirements beyond 5G ecosystem, novel trust and reputation models ought to reckon scalability, and above all, automatization as development foundations. The latter is partially addressed by the *Continuous Update* module, in particular, through triggers and events. Earlier identification of triggers and events along with a suitable configuration themselves may help us react to possible attacks [71] and preserve an up-to-date trust and reputation model. For that reason, it is advisable that trust and reputation models possess a *dynamic* updating mechanism that allows identifying triggers from security threats, SLA violations, service execution failures, change policy relationships, or even active time of trust relationships.

Through these events, a model can automatize and adapt to the effects occurring in real time by recalculating trust scores. Such events are often associated with an increment or decrease of the final trust score, and sometimes, they are contemplated as part of *reward and punishment* processes [72]. Thence, should negative events appear in a trust relationship, the trust and reputation model will be penalized by decreasing its trust score. In the case of no events, the trust model might reward the trustee's reputation. In the end, *reward and punishment* algorithms encourage entities to reflect trust changes of the interaction nodes more objectively. In the work presented by Niu et al. [6], the use of reward and punishment mechanisms was focused on increasing trust level of Virtual Network Functions (VNFs) when the network slice running time increased without security incidents, and decreasing when the security threats or failure problems were detected. The rate of decline was determined by factors such as the level of security threats or the severity of the problem. Another approach was addressed by Kong et al. [73], who introduced these mechanisms to detect swaying attacks and build a more secure environment through simulating active and benign nodes to participate in the interaction. In the end, *reward and punishment* mechanisms spur trust and reputation models to be more secure and to be updated almost in real time.

Even though some introduced recommendations may palliate conventional trust and reputation attacks, our model does not currently provide a resilience mechanism to the wide range of possible attacks.

From our standpoint, the identification and mitigation of likely trust attacks are steps following the validation of a trust and reputation model, rather than design steps. Therefore, they are consequences of design decisions of a particular trust and reputation model. Notwithstanding, the authors will analyze previous proposals, such as Gómez Mármol and Martínez Pérez [16], ITU-T Y.3052 [38], ITU-T Y.3054 [40], ITU-T X.5Gsec-t [41], and ZTA [10], where resilience mechanisms were able to withstand Sybil attacks, bad-mouthing, on-off attacks, collusion attacks, etc. By means of such analysis, we will not only recognize a sort of traditional trust attacks, but also discover multiple techniques to be leveraged. After that, we will evaluate the resilience of their trust and reputation model, as well as readjust previous techniques of trust attack mitigation to beyond 5G scenario properties, if required.

Lastly, despite not being part of modules illustrated in the proposed trust and reputation model, we want to introduce some advantages of considering identity management together with trust and reputation models. Ordinarily, trust and reputation models interacted with users of their own domain, where would be easier to identify them, or other domains, where would be necessary a greater effort to identify and verify their identities. However, few trust and reputation models considered or associated an identity management component between the steps of their lifecycle. We honestly deem that the absence of identity management mechanisms is principally correlated with centralized approaches to identity management. In this case, Certificate Authorities (CAs) portray an essential role to give truthfulness of the certificates they issue. Nonetheless, this process is complicated when we are in a cross-domain scenario with multiple CAs, different types of certificates, certificate revocation lists, etc[74].

Because 5G networks expect to raise and facilitate cross-domain relationships among service/resource providers and service/resource consumers, new decentralized technologies have also appeared to tackle the aforementioned problems. In particular, one of the most avant-garde approaches is the decentralized identifiers (DIDs) defined by the World Wide Web Consortium [45]. DIDs are a unique, stable, and global identifier that enables its use in any type of entity (humans and machines), service, technology, and organization (identity property). In addition, they are resolvable with high availability and cryptographically verifiable, as well as linked to DLTs. In consequence, this mechanism may be utilized to manage entities involved in the trust and reputation model, to associate unique identifiers independently of their origin, and to provide access control over services and resources [75]. What is more, they also provide an extra trust and security level since they can be used for protecting communicated data being accessed by unauthorized parties [76], enabling a proper collection of trust and reputation information [38,39,77], and recognizing malicious devices.

In spite of identity is not a topic addressed by all trust and reputation models, some solutions do take into account identifiers to make easier the identification of general trust attacks like Sybil attacks [78]. In short, we consider worth that a trust and reputation model beyond 5G will consider a novel identity management mechanism as an external component but also associated with some trust and reputation model's activities, or even as one of the modules that would make up the overall trust and reputation model architecture.

In the end, the proposed trust and reputation model envisages covering the principal requirements and KPIs recognized in Section 3. At the same time, the presented trust and reputation model is as abstract as possible so that it may be tuned to different use cases and scenarios with little effort. Hence, the above recommendations are the earliest effort toward a feasible standardization of trust models in 5G and B5G networks.

5. Conclusion

Despite the fact that trust models are not a disruptive technology, their application in 5G ecosystems involves the contemplation, adjustment, and discarding of previous ideas raised in other standard trust models. The article at hand has analyzed the most prominent trust and reputation model standardization approaches in the research field so as to identify conventional characteristics and limitations compared to other proposals. At the same time, we have also studied newfangled research projects and regulatory organizations working on 5G and beyond 5G scenarios to recognize up-to-date trends as well as the principal changes involved.

Considering the previous investigations as a trustworthy basis, we have also provided multiple sets of requirements and KPIs that depict a progression from their beginnings (around 2000) to the present. Such requirements and KPIs have been set out from a generic point of view to allow for their application in a large number of scenarios and to enable feedback with previous proposals.

In addition, a pre-standardization approach for trust and reputation models beyond 5G has also been suggested. By means of the advice given, we have evolved the previous trust and reputation model standardization approaches to an abstract one that complies with paramount requirements and KPIs of beyond 5G networks. Additionally, this innovative approach enables its use in a multitude of scenarios thanks to its level of abstraction. Thus, we have presented four modules that allow accomplishing key actions associated with trust and reputation models, at the same time as fulfilling the aforementioned requirements and KPIs through the utilization of novel technologies and methods.

As future work, we will design and integrate a trust and reputation model for beyond 5G networks that achieves not only the abstract modules and steps described in this article but also the essential requirements and KPIs that will be standard foundations in future networks. Besides, we will build up an information model from the entities and characteristics of the reputation-based trust model so as to propose a subset of common characteristics that may be linked to a trust instance regardless of its enforcement environment. Additionally, we will cater for a set of generic interfaces to communicate the proposed trust and reputation model modules as well as interacting with the trust model itself. Last but not least, we will also research some viable trust attacks that our model may undergo, as well as infer resilience mechanisms and techniques.

CRediT authorship contribution statement

José María Jorquera Valero: Conceptualization, Methodology, Formal analysis, Investigation, Resources, Writing – original draft, Writing – review & editing, Visualization. **Pedro Miguel Sánchez Sánchez:** Conceptualization, Validation, Investigation, Visualization. **Manuel Gil Pérez:** Conceptualization, Validation, Formal analysis, Writing – review & editing, Visualization, Supervision. **Alberto Huertas Celdrán:** Conceptualization, Validation, Visualization, Supervision. **Gregorio Martínez Pérez:** Conceptualization, Validation, Writing – review & editing, Visualization, Supervision, Project administration.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work has been supported by the European Commission through 5GZORRO project (grant no. 871533) part of the 5G PPP in Horizon 2020. The paper solely reflects the views of the authors. EC is not responsible for the contents of this paper or any use made thereof. Authors thank the 5GZORRO Consortium for useful insights to this work.

References

[1] B. Bangerter, S. Talwar, R. Arefi, K. Stewart, Networks and devices for the 5G era, IEEE Commun. Mag. 52 (2) (2014) 90–96.

[2] Q. Wang, J. Alcaraz-Calero, M.B. Weiss, A. Gavras, P.M. Neves, R. Cale, G. Bernini, G. Carrozzo, N. Ciulli, G. Celozzi, et al., Slicenet: End-to-end cognitive network slicing and slice management framework in virtualised multi-domain, multi-tenant 5g networks. 2018 IEEE international symposium on broadband multimedia systems and broadcasting (BMSB), IEEE, 2018, pp. 1–5.

[3] A. Abdul-Rahman, S. Hailes, A distributed trust model. 1997 Workshop on New Security Paradigms, 1998, pp. 48–60.

[4] E.G. AbdAllah, M. Zulkernine, Y.X. Gu, C. Liem, TRUST-CAP: A trust model for cloud-based applications. 41st Annual Computer Software and Applications Conference, 2017, pp. 584–589.

[5] A.A. Adewuyi, H. Cheng, Q. Shi, J. Cao, A. MacDermott, X. Wang, CTRUST: A dynamic trust model for collaborative applications in the internet of things, IEEE Internet Things J. 6 (3) (2019) 5432–5445.

[6] B. Niu, W. You, H. Tang, X. Wang, 5G network slice security trust degree calculation model. 3rd IEEE International Conference on Computer and Communications, 2017, pp. 1150–1157.

[7] F. Gómez Mármol, G. Martínez Pérez, A.F. Gómez Skarmeta, TACS, A trust model for P2P networks, Wireless Personal Communications 51 (1) (2009) 153–164.

[8] C.J. Mitchell, Who needs trust for 5G?, arXiv preprint arXiv:2005.00862(2020).

[9] C. Benzaid, T. Taleb, AI-Driven zero touch network and service management in 5G and beyond: challenges and research directions, IEEE Netw 34 (2) (2020) 186–194.

[10] V.A. Stafford, Zero trust architecture, NIST Special Publication 800 (2020) 207.

[11] N.A. Mhetre, A.V. Deshpande, P.N. Mahalle, Trust management model based on fuzzy approach for ubiquitous computing, International Journal of Ambient Computing and Intelligence 7 (2) (2016) 33–46.

[12] P.S. Challagidad, V.S. Reshmi, M.N. Birje, Reputation based trust model in cloud computing, Internet Things Cloud Computing 5 (5-1) (2017) 5–12.

[13] S.Y. Hashemi, F.S. Aliee, Dynamic and comprehensive trust model for IoT and its integration into RPL, J Supercomput 75 (7) (2019) 3555–3584.

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

[15] D. Trček, Towards trust management standardization, Computer Standards & Interfaces 26 (6) (2004) 543–548.

[16] F. Gómez Mármol, G. Martínez Pérez, Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems, Computer Standards & Interfaces 32 (4) (2010) 185–196.

[17] J. Bøegh, Y. Yuan, Towards a standard for service behavior trustworthiness management. 2nd International Conference on Digital Information and Communication Technology and Its Applications, 2012, pp. 189–194.

[18] R. Garg, ISO/IEC JTC 1/SC 7 Software and systems engineering, 2021, (https://www.iso.org/committee/45086.html). [Online; accessed 15-March-2021].

[19] M. Vinkovits, Towards requirements for trust management. 10th Annual International Conference on Privacy, Security and Trust, 2012, pp. 159–160.

[20] R. Abassi, S.G. El Fatmi, Towards a generic trust management model. 19th International Conference on Telecommunications, 2012, pp. 1–6.

[21] G. Costagliola, V. Fuccella, F.A. Pascuccio, Towards a trust, reputation and recommendation meta model, Journal of Visual Languages & Computing 25 (6) (2014) 850–857.

[22] S. Vavilis, M. Petković, N. Zannone, A reference model for reputation systems, Decis Support Syst 61 (2014) 147–154.

[23] A. Kanwal, R. Masood, M.A. Shibli, R. Mumtaz, Taxonomy for trust models in cloud computing, Comput J 58 (4) (2015) 601–626.

[24] S. Joshi, D.K. Mishra, A roadmap towards trust management & privacy preservation in mobile ad hoc networks. 2016 International Conference on ICT in Business Industry & Government, 2016, pp. 1–6.

[25] E. Viardot, Trust and standardization in the adoption of innovation, IEEE Communications Standards Magazine 1 (1) (2017) 31–35.

[26] C.-C. Wu, Y. Huang, C.-L. Hsu, Benevolence trust: a key determinant of user continuance use of online social networks, Information Systems and e-Business Management 12 (2) (2014) 189–211.

[27] D. Jelenc, Toward unified trust and reputation messaging in ubiquitous systems, Ann. Telecommun. (2020) 1–12.

[28] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T.H. Nguyen, F. Liu, T. Hewa, M. Liyanage, et al., 6G white paper: Research challenges for trust, security and privacy, arXiv preprint arXiv:2004.11665(2020).

[29] K. Ramezanpour, J. Jagannath, Intelligent zero trust architecture for 5g/6g tactical networks: Principles, challenges, and the role of machine learning, arXiv preprint arXiv:2105.01478(2021).

[30] E. Commission, Horizon 2020, 2020, (https://ec.europa.eu/programmes/horizon2020/en/h2020-sections-projects). [Online; accessed 07-December-2020].

[31] E.C.H. 2020, USA-Country page, 2017, (https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_localsupp_usa_en.pdf). [Online; accessed 02-March-2021].

[32] N.S. Foundation, Secure and Trustworthy Cyberspace (SaTC), 2021, (https://www.nsf.gov/pubs/2021/nsf21500/nsf21500.htm). [Online; accessed 02-March-2021].

[33] M. Surridge, G. Correndo, K. Meacham, J. Papay, S.C. Phillips, S. Wiegand, T. Wilkinson, Trust modelling in 5G mobile networks. 2018 Workshop on Security in Softwarized Networks: Prospects and Challenges, 2018, pp. 14–19.

[34] G. Sargsyan, N. Castellon, R. Binnendijk, P. Cozijnsen, Blockchain security by design framework for trust and adoption in IoT environment. 2019 IEEE World Congress on Services, 2019, pp. 15–20.

[35] C. Benzaid, P. Alemany, D. Ayed, G. Chollon, M. Christopoulou, G. Gür, V. Lefebvre, E.M. de Oca, R. Muüoz, J. Ortiz, A. Pastor, R. Sanchez-Iborra, T. Taleb, R. Vilalta, G. Xilouris, White paper: Intelligent security architecture for 5G and beyond networks, 2020, (????). 10.5281/zenodo.4288658.

[36] J.J.A. Esteves, A. Boubendir, F. Guillemin, S. Pierre, Edge-enabled optimized network slicing in large scale networks. 11th International Conference on Network of the Future, 2020, pp. 129–131.

[37] G. Carrozzo, M.S. Siddiqui, A. Betzler, J. Bonnet, G. Martínez Pérez, A. Ramos, T. Subramanya, AI-driven zero-touch operations, security and trust in multi-operator 5G networks: A conceptual architecture. 2020 European Conference on Networks and Communications, 2020, pp. 254–258.

[38] I.T.U.-T. Y. 3052, Overview of trust provisioning for information and communication technology infrastructures and services, 2017, (https://www.itu.int/rec/T-REC-Y.3052). [Online; accessed 05-December-2020].

[39] I.T.U.-T. Y. 3053, Framework of trustworthy networking with trust-centric network domains, 2018, (https://www.itu.int/rec/T-REC-Y.3053). [Online; accessed 05-December-2020].

[40] I.T.U.-T. Y. 3054, Framework for trust-based media services, 2019, (https://www.itu.int/rec/T-REC-Y.3054). [Online; accessed 05-December-2020].

[41] I.T.U.-T. S. 17, Security framework based on trust relationship for 5G ecosystem, 2020, (https://www.itu.int/md/T17-SG17-C-0821). [Online; accessed 05-December-2020].

[42] I.T. 23186:2018, Framework of trust for processing of multi-sourced data, 2018, (https://www.iso.org/standard/74844.html). [Online; accessed 05-December-2020].

[43] G.F. de Oliveira, R. Rabechini Jr, Stakeholder management influence on trust in a project: a quantitative study, Int. J. Project Manage. 37 (1) (2019) 131–144.

[44] G. Guo, E. Yang, L. Shen, X. Yang, X. He, Discrete trust-aware matrix factorization for fast recommendation. IJCAI, 2019, pp. 1380–1386.

[45] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, M. Sabadello, Decentralized identifiers (DIDs) v1.0, W3C Working Draft, 2021, (https://www.w3.org/TR/did-core). [Online; accessed 07-December-2020].

[46] C. Gong, D. Yu, L. Zhao, X. Li, X. Li, An intelligent trust model for hybrid DDosdetection in software defined networks, Concurrency and Computation: Practice and Experience 32 (16) (2020) e5264.

[47] T. Ranathunga, R. Marfievici, A. McGibney, S. Rea, A DLT-based trust framework for IoT ecosystems. 2020 International Conference on Cyber Security and Protection of Digital Services, 2020, pp. 1–8.

[48] 5GPPP, European Annual Journal 2020, 2020, (https://5g-ppp.eu/annual-journal). [Online; accessed 14-December-2020].

[49] A. Ghosh, A. Maeder, M. Baker, D. Chandramouli, 5G Evolution: a view on 5G cellular technology beyond 3GPP release 15, IEEE Access 7 (2019) 127639–127651.

[50] P. Kochovski, S. Gec, V. Stankovski, M. Bajec, P.D. Drobintsev, Trust management in a blockchain based fog computing platform with trustless smart oracles, Future Generation Computer Systems 101 (2019) 747–759.

[51] N. El Ioini, C. Pahl, A review of distributed ledger technologies. OTM Confederated International Conferences "On the Move to Meaningful Internet Systems", 2018, pp. 277–288.

[52] T.E.U.A. for Cybersecurity, Threat landscape for 5G networks report: Updated threat assessment for the fifth generation of mobile telecommunications networks (5G), 2020, (https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks). [Online; accessed 23-December-2020].

[53] H. El-Sayed, H.A. Ignatious, P. Kulkarni, S. Bouktif, Machine learning based trust management framework for vehicular networks, Veh. Commun. (2020) 100256.

[54] S. Deng, L. Huang, G. Xu, X. Wu, Z. Wu, On deep learning for trust-aware recommendations in social networks, IEEE Trans Neural Netw Learn Syst 28 (5) (2016) 1164–1177.

[55] L. Liu, Z. Ma, W. Meng, Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks, Future Generation Computer Systems 101 (2019) 865–879.

[56] N. Kolokotronis, S. Brotsis, G. Germanos, C. Vassilakis, S. Shiaeles, On blockchain architectures for trust-based collaborative intrusion detection. 2019 IEEE World Congress on Services volume 2642, 2019, pp. 21–28.

[57] Y. Shoukry, S. Mishra, Z. Luo, S. Diggavi, Sybil attack resilient traffic networks: A physics-based trust propagation approach. 9th International Conference on Cyber-Physical Systems, 2018, pp. 43–54.

[58] L. Sharnagat, R. Babu, J. Adhikari, Trust evaluation for securing compromised data aggregation against the collusion attack in WSN. 2nd International Conference on Inventive Research in Computing Applications, 2020, pp. 1–5.

[59] V.B. Reddy, A. Negi, S. Venkataraman, V.R. Venkataraman, A similarity based trust model to mitigate badmouthing attacks in internet of things (IoT). 5th World Forum on Internet of Things, 2019, pp. 278–282.

[60] H. Xia, Z. Li, Y. Zheng, A. Liu, Y.-J. Choi, H. Sekiya, A novel light-weight subjective trust inference framework in MANETs, IEEE Trans. Sustainable Comput. 5 (2) (2020) 236–248.

[61] H. Xia, S.-s. Zhang, Y. Li, Z.-k. Pan, X. Peng, X.-z. Cheng, An attack-resistant trust inference model for securing routing in vehicular ad hoc networks, IEEE Trans. Veh. Technol. 68 (7) (2019) 7108–7120.

[62] I.V. Paputungan, A.F.M. Hani, M.F. Hassan, V.S. Asirvadam, Real-time and proactive SLA renegotiation for a cloud-based system, IEEE Syst. J. 13 (1) (2018) 400–411.

[63] S. Li, I. Doh, K. Chae, Non-redundant indirect trust search algorithm based on a cross-domain trust model in content delivery network. 19th International Conference on Advanced Communication Technology, 2017, pp. 72–77.
[64] C. Burnett, T.J. Norman, K. Sycara, Bootstrapping trust evaluations through stereotypes. 9th International Conference on Autonomous Agents and Multiagent Systems, 2010, pp. 241–248.
[65] M. Ghafoorian, D. Abbasinezhad-Mood, H. Shakeri, A thorough trust and reputation based RBAC model for secure data storage in the cloud, IEEE Trans. Parallel Distrib. Syst. 30 (4) (2018) 778–788.
[66] G.F. Camilo, G.A.F. Rebello, L.A.C. de Souza, O.C.M.B. Duarte, A secure personal-data trading system based on blockchain, trust, and reputation. 2020 IEEE International Conference on Blockchain, 2020, pp. 379–384.
[67] K. Papadakis-Vlachopapadopoulos, R.S. González, I. Dimolitsas, D. Dechouniotis, A.J. Ferrer, S. Papavassiliou, Collaborative SLA and reputation-based trust management in cloud federations, Future Generation Computer Systems 100 (2019) 498–512.
[68] C. Giebler, C. Gröger, E. Hoos, H. Schwarz, B. Mitschang, Leveraging the data lake: Current state and challenges. International Conference on Big Data Analytics and Knowledge Discovery, 2019, pp. 179–188.
[69] A. Vathy-Fogarassy, T. Hugyák, Uniform data access platform for SQL and nosqldatabase systems, Inf Syst 69 (2017) 93–105.
[70] V.L. Lemieux, Blockchain and distributed ledgers as trusted recordkeeping systems. Future Technologies Conference, 2017, pp. 41–48.
[71] M.D. Alshehri, F.K. Hussain, A fuzzy security protocol for trust management in the internet of things (fuzzy-Iot), Computing 101 (7) (2019) 791–818.
[72] K.A. Awan, I.U. Din, M. Zareei, M. Talha, M. Guizani, S.U. Jadoon, Holitrust-A holistic cross-domain trust management mechanism for service-centric internet of things, IEEE Access 7 (2019) 52191–52201.
[73] W. Kong, X. Li, L. Hou, Y. Li, An efficient and credible multi-source trust fusion mechanism based on time decay for edge computing, Electronics (Basel) 9 (3) (2020) 502.
[74] Y. Chen, G. Dong, J. Bai, Y. Hao, F. Li, H. Peng, Trust enhancement scheme for cross domain authentication of PKI system. 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2019, pp. 103–110.
[75] X. Fan, Q. Chai, L. Xu, D. Guo, DIAM-IoT: A decentralized identity and access management framework for internet of things. 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, 2020, pp. 186–191.
[76] R. Ansey, J. Kempf, O. Berzin, C. Xi, I. Sheikh, Gnomon: Decentralized identifiers for securing 5G IoT device registration and software update. 2019 IEEE Globecom Workshops, 2019, pp. 1–6.
[77] R. Kantola, J. Llorente Santos, N. Beijar, Policy-based communications for 5G mobile with customer edge switching, Security and Communication Networks 9 (16) (2016) 3070–3082.
[78] T.H. Noor, Q.Z. Sheng, L. Yao, S. Dustdar, A.H.H. Ngu, Cloudarmor: supporting reputation-based trust management for cloud services, IEEE Trans. Parallel Distrib. Syst. 27 (2) (2016) 367–380.