The Journal of Supercomputing
https://doi.org/10.1007/s11227-023-05765-4

A survey on IoT trust model frameworks

Davide Ferraris[1] · Carmen Fernandez-Gago[1] · Rodrigo Roman[1] · Javier Lopez[1]

Accepted: 26 October 2023

Abstract
Trust can be considered as a multidisciplinary concept, which is strongly related to the context and it falls in different fields such as Philosophy, Psychology or Computer Science. Trust is fundamental in every relationship, because without it, an entity will not interact with other entities. This aspect is very important especially in the Internet of Things (IoT), where many entities produced by different vendors and created for different purposes have to interact among them through the internet often under uncertainty. Trust can overcome this uncertainty, creating a strong basis to ease the process of interaction among these entities. We believe that considering trust in the IoT is fundamental, and in order to implement it in any IoT entity, it is fundamental to consider it through the whole System Development Life Cycle. In this paper, we propose an analysis of different works that consider trust for the IoT. We will focus especially on the analysis of frameworks that have been developed in order to include trust in the IoT. We will make a classification of them providing a set of parameters that we believe are fundamental in order to properly consider trust in the IoT. Thus, we will identify important aspects to be taken into consideration when developing frameworks that implement trust in the IoT, finding gaps and proposing possible solutions.

Keywords Trust · Metrics · Models · Frameworks · Internet of things (IoT) · System development life cycle (SDLC)

Carmen Fernandez-Gago, Rodrigo Roman, and Javier Lopez have contributed equally to this work.

✉ Davide Ferraris
ferraris@uma.es

Carmen Fernandez-Gago
mcgago@uma.es

Rodrigo Roman
rroman@uma.es

Javier Lopez
javierlopez@uma.es

[1] NICS Lab, University of Malaga, Edificio de Investigación Ada Byron, Arquitecto Francisco Peñalosa, 18, 29071 Malaga, Spain

Published online: 17 November 2023

1 Introduction

The Internet of Things (IoT) is a paradigm allowing humans and smart entities to cooperate among them anyhow and anywhere [1]. Moreover, IoT entities ecosystems are growing each year, and "it is expected that there will be more than 64B IoT devices worldwide by 2025".[1] This prediction states that the IoT paradigm will define how the world will be connected. For this reason, many opportunities will arise, but also many problems [2]. A way to mitigate them is offered by trust. In fact, an entity should interact with another one only if trust is established between them. However, due to the uncertainty, interoperability, and heterogeneity of IoT, achieving trust is still a challenge. Besides, considering the fact that research communities have tackled these aspects separately, a holistic approach should be desirable [3].

Nevertheless, trust is difficult to define. It concerns different aspects and topics ranging from Philosophy to Computer Science [3], and it is strongly dependent on the context. This is a strong point in common with IoT, where it is possible to have different contexts for different entities. Thus, if we consider trust in these contexts, we can enhance the protection of such entities allowing only the trusted ones to interact with them.

Moreover, trust is strongly dependent on other properties like security and privacy [4, 5] and these relationships are even more important during an IoT entity development [6]. Statement also claimed by Mohammadi et al. [7], where the authors declares that trust mechanisms are fundamental in the development of IoT entities and this task requires more research.

For these reasons, in our opinion, it is crucial to consider trust since the initial phases of the System Development Life Cycle (SDLC) in order to develop the trust relationships among the entities in a systematic way. This approach can help to protect the entities and to give them important rules of behaviour during the interactions with other entities.

During the interaction of two entities under a trust perspective, we can state that usually there are at least two actors involved: the trustor and the trustee. The trustor is the one who actively trusts, and the trustee is the one who keeps the trust. The trustor needs the trustee to perform an action or fulfil a goal considering a particular context. This goal is not achievable by the trustor alone. In this case, trust metrics are useful to compute a trust level that helps the trustor to decide if a trustee can be trusted [8]. Therefore, this value must be computed before the two actors begin the collaboration. Moreover, the trust level could change over time positively or negatively due to the right or wrong behaviour of the trustee [9].

In this paper, we will analyse how trust and IoT have been considered during the years in the state of the art and which framework to develop trust in the IoT has been developed.

In order to perform such analysis, we will focus on several parameters that we consider important for implementing trust in the IoT. Moreover, we classify the

[1] https://techjury.net/blog/internet-of-things-statistics/.

existing IoT frameworks considering important aspects such as the phases of the SDLC (i.e. requirements elicitation), trust related domains (i.e. security and privacy) and general activities related to trust (i.e. decision-making process). In the literature there are many other surveys on trust and IoT [10–13], but to the best of our knowledge, there are no surveys analysing the relationship between trust and IoT during the whole SDLC. With this paper we want to fill this gap.

The paper is structured as follows, in Sect. 2, we will analyse the concept of trust and trust management frameworks, and how they have been defined in the state of the art during the years. In Sect. 3, we will discuss about IoT and its connections with trust. Then, in Sect. 4 we will present existing frameworks that implement trust in IoT. In Sect. 5, we explain the methodology used in order to analyse the frameworks and, in Sect. 6, we will make a classification of the frameworks according to the parameters explained. Finally, in Sect. 7, we describe challenges and issues that remain open and in 8 we conclude the paper and discuss about future work.

2 Trust and trust management

In this section, firstly, we will analyse how trust can be defined presenting several definition defined by authors in the state of the art. Then, we will discuss about trust management, trust metrics and trust models.

2.1 Analysis of the concept of trust

"Trust is a common phenomenon" [14], but it is also a difficult concept to define "because it is a multidimensional, multidisciplinary and multifaceted concept [15]". Trust is defined in British English by the Cambridge Dictionary as "to believe that someone is good and honest and will not harm you, or that something is safe and reliable", in American English as "to have confidence in something, or to believe in someone" and in business English as "belief that you can depend on someone or something".[2] Thus, we have three similar definitions, but not the same, in the same dictionary about the same word in three similar areas, that can give an idea about the difficulty to define trust.

However, analysing these definitions, there is a distinction respect to people ("someone") and objects ("something"). In the former case, there is a reference respect to the goodness and honesty of the person we trust and that he/she will not harm us. In the latter case, we refer to the object implying that it is safe and reliable and basically that its utilization will not harm us and it will work as we have expected. Thus, we can state that these definitions are general. Moreover, they can give an important hint that trust is strongly related to the context.

In the state of the art, there are many definitions of trust applicable to different aspects. Erickson [16] stated that "trust means many things to many people".

[2] http://dictionary.cambridge.org/dictionary/english/trust.

Accordingly with this definition, we can understand why it is hard to define and explain what trust is. Moreover, many fields of studies such as Sociology, Psychology, Philosophy and Information Technology have to deal with trust in different ways. For this reason, McKnight [17] stated that "Trust has been defined in so many ways by so many different researchers across disciplines that a typology of the various types of trust is sorely needed".

Thus, giving a meaning to trust is a challenge that many authors in the past years have tackled [4, 18–24].

Mayer et al. [18] defined trust as a "willingness to be vulnerable to another party".

McKnight and Chervany [19] explained that trust intention is "the extent to which one party is willing to depend on the other party in a given situation with a feeling of relative security, even though negative consequences are possible".

Gambetta [20] affirmed that "trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action".

Mui et al. [21] stated that "trust as a subjective expectation an agent has about another's future behaviour based on the history of their encounters".

For Ruohomaa et al. [22] "trust is the extent to which one party is willing to participate in a given action with a given partner, considering the risks and incentives involved".

Hoffman [4] defined trust "as the expectation that a service will be provided or a commitment will be fulfilled".

Jøsang [23] stated that "trust is a personal and subjective phenomenon that is based on various factors or evidence" and also that "trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends".

Olmedilla et al. [25] specified that "trust of a party A to a party B for a service X is the measurable belief of A in that B behaves dependably for a specified period within a specified context (in relation to service X)".

Finally, Agudo et al. [24] defined that trust is related to "the level of confidence that an entity participating in a network system places on another entity of the same system for performing a given task".

Even though all the definitions are different, they share some underlying concept. All the authors cited above stated that trust is strictly dependent on the actors involved in a trust interaction. Typically, there are two entities (at least) involved in a trust interaction, one is the trustor (the entity which places trust) and the other one is the trustee (the entity in which trust is placed) [5, 14, 24, 26].

In order to guarantee a trust interaction, we can state that it is necessary that "the trustor trusts the trustee". Analysing this sentence we can identify:

1. "the *trustor*" is the entity which places trust (active trust);
2. "the *trustee*" is the entity on which trust is placed (passive trust);
3. "*trusts*" is the action between the two entities.

The trust action happens when an individual (the "trustor") requires the service of another individual (the "trustee"). Depending on the fulfilment of the action or how it is performed, the level of trust of the trustor can change positively or negatively. This means that the future interactions will be dependent on the outcome of past interactions affecting the level of trust of the trustor.

A concept related to trust is trustworthiness. It can be defined as a characteristic of a person [5] or of something [16] that is the object of somebody's trust. In other words it is a characteristic of the trustee.

Moreover, Pavlidis [5] stated that "a trustworthy system is a system that has the capability of meeting customer trust and the capability to meet their stated, unstated, and even unanticipated needs".

McKnight and Chervany [17] defined four concepts related to trustworthiness: benevolence, competence, integrity, and predictability.

- **Benevolence**: the trustor is important for the trustee and for this reason he acts properly in order to not to hurt him.
- **Competence**: the trustee is able to do what the trustor wants (and this can be the reason why the trustor asks for help to the trustee).
- **Integrity**: the trustee is honest and he acts accordingly to what the trustor asks him for without malicious intentions.
- **Predictability**: the trustor can anticipate the behaviour of the trustee and have a knowledge *a-priori* about the exchange.

According to McKnight and Chervany [17], only one of these four concepts is not enough to establish a trust relationship. For example, if the trustee is honest but has no competence to finalize the action requested by the trustor, then the latter might not want to establish the relationship. In fact, he cannot trust the trustee to perform that action. On the other hand, if the trustee is competent but he is not honest, the relationship is likely not worth to be established because the trustor cannot trust the trustee fearing a possible betrayal.

Trustworthiness determines if someone (or something) is able to be trusted, the higher the trustworthiness, the higher the possibility to be trusted. When the desired level of trust of the trustor matches the trustworthiness of the trustee there is no disequilibrium in the trust relationship. The other possibilities are trusting less or trusting more than the trustworthiness. In the first case, there is a loss about the opportunities, in the second case there is a possible loss because the trustor is vulnerable [27, 28].

Trustworthiness is very important for both humans and things. When we talk about a trustworthy thing or a software, it is considered as a high quality resource [29]. Moreover, a system can be defined trustworthy and be accepted from the customers if its capability meets the stakeholder needs, not only the ones asked by them but also the ones that they did not know [5].

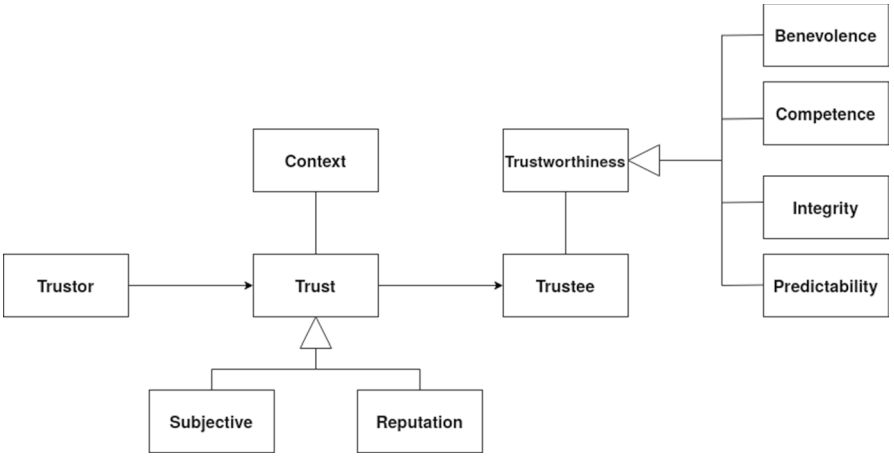

Fig. 1 Conceptual Model related to trust action

Strongly related to trust, reputation is defined as "the opinion that people in general have about someone or something, or how much respect or admiration someone or something receives, based on past behaviour or character".[3]

Mui [21] stated that "reputation is defined as a perception a party creates through past actions about its intentions and norms".

Moreover, reputation is also defined as objective trust.[4]

We can say that trust and reputation are connected but they are not the same. Mostly, reputation can be a parameter for trust decision [23].

In fact, Jøsang [23] asserts that:

"*I trust you because of your good reputation.*" (1)

"*I trust you despite your bad reputation.*" (2)

These are two positive definitions.

Hoffman stated that "Metrics must be defined to measure user trust and distrust of a system" [4] and Gambetta [20] defined distrust symmetrical respect trust. For the sake of completeness, in addition to trust, distrust and no trust, Marsh defined also untrust and mistrust [30].

Thus, following these definitions, we can also produce two negative assertions:

"*I distrust you despite your good reputation.*" (3)

"*I distrust you because of your bad reputation.*" (4)

With these four definitions, we can understand better that reputation is a parameter for considering trust, but it is not the only one in that affect the outcome of a

[3] http://dictionary.cambridge.org/dictionary/english/reputation.

[4] wiki.p2pfoundation.net/Trust_Metrics.

trust computation. In fact, for example it is possible to trust someone or something "despite a bad reputation".

In Fig. 1, we can see a conceptual model about trust. It includes the actors performing a trust action and the parameters important to be taken into consideration.

The conceptual model is helpful for the readers in order to visualize how trust can be considered for the actors involved. Thus, we can see that the trustor is the one who has to trust the trustee. Trust is connected to the context and it can be subjective (i.e. the trustor already know the trustee) or it can be objective (i.e. reputation). On the other hand, the trustee is chosen according to its trustworthiness, which is composed of the four parameters proposed by McKnight and Chervany [17].

In the next subsection, we will discuss about trust management, metrics and models.

2.2 Trust management, metrics and models

In order to integrate trust in any system, such as IoT ecosystems, it is highly recommended to consider it within a trust management framework. However, a framework is usually composed of three important parts: management, metrics and models [31]. It is then necessary to provide an overview of these concepts.

Trust management "can be conceptualized in two ways. Firstly, as a process according to which an entity becomes trustworthy for other entities. Secondly, as a process that enables the assessment of the reliability of other entities, which in turn is exploited in order to automatically adapt its strategy and behaviour to different levels of cooperation and trust" [32]. The first trust management framework in the literature was PolicyMaker [33]. It was described by Blaze as a trust management system "that will facilitate the development of security features in a wide range of network services". Moreover, this framework can be considered as the most general form of trust management system. More recently, Ruan et al. [31] proposed a general trust management framework that is composed of three context-dependent phases:

- **Trust Modelling**: in this phase, there is a mapping of the available trust raw data from the fields into trust metrics.
- **Trust Inference**: it focuses on propagating and aggregating the obtained trust metrics over the whole network or over the part of interest.
- **Decision Making**: Decision making refers to the use of the produced trust knowledge to support decision making. This process allows the entity to decide how to act according to the data which has been collected and computed.

From the above cited works, we can observe that trust models and trust metrics are a fundamental parts of trust management. In addition, we can observe that trust is strictly connected to the context and in order to perform a trust decision, it is useful to have a related activity such as decision-making.

Concerning trust metrics, Beth et al. [34] published the first type of modern trust metric. It is composed of a set of rules used to derive the trustworthiness

value of a node between 0 and 1, using subjective and objective trust. Then, Levien [8] defined the simplest trust metric as the following. There are three elements:

1. a designated "seed" node indicating the root of trust (S)
2. a "target" node (T)
3. a directed graph

This is considered as a basis for the other trust metrics. All the trust metrics contain at least these three elements. A trust metric is useful to determine whether the node T is trustworthy or not. For more complicated metrics, the edges can contain rules, weights or controls. Moreover, transitivity can be implemented and in this case we can also consider propagation and aggregation as important trust metrics.

Considering trust models, Moyano et al. [26] made a classification of them. This work is important also because it is useful to extract some similar features from different kind of models. Thus, following this premise, it is possible to create a general framework containing these features. The classification used by Moyano divided the trust models into two main categories:

- **Decision Models:** These models' task is to make access control decisions more adaptable, substituting the two-step authentication process into a single one-step trust decision. Policy and negotiation models belong to this category. These models work with policies and credentials, granting access by policies requiring specific credentials.
- **Evaluation Models:** They take into consideration several parameters in order to evaluate the reliability of an entity. These parameters can be related to propagation models (i.e. trust factors are propagated along a trust chain) or behaviour models (i.e. trust factors are measured). An important sub-type of the latter are reputation models, where the entities compute an initial trust value starting from other entities' opinion about a given entity.

Policy models (as Policy Maker [33]) are a sub-type of decision models, they have rules that are used in order to give or not access to a resource. These rules are named policies and they are written by using a policy language [26]. Other type of decision models are negotiation models (as Trust Builder [35]). Trust negotiation models perform a negotiation strategy protocol, where two entities exchange credentials and policies in a step-by-step protocol until a trust decision is made. This strategy is performed in order to protect the privacy of the entities revealing sensitive information only if they are needed. A particular type of evaluation models are behaviour models. These models are often built in a systematic way and through three phases [26]:

1. Assign a trust value to the entities belonging to the system.
2. Monitoring the entities and their attributes.
3. Assign values to the monitored attributes merging them to compute a final result called *trust or reputation score*.

The final score is a value showing how much the trustor trusts the trustee and it can be uni-dimensional or multi-dimensional [23]. In the second case, the values could be obtained from different aspects of trust. Trust metrics are used to calculate these values and they compute variables such as security or utility in order to provide a final total score to relations [26].

Reputation models are helpful to compute an initial trust value, in case the trustor has never had previous interactions with the trustee. These models can be centralized or distributed. In the first case, an entity (a trusted third party) collects information reputation about the other entities and share these values among all the other entities. In the second case, every entity collects the information about other entities and shared it with the other entities. In both cases, "the model might consider how certain or reliable this information is (e.g. credibility of witnesses), and might also consider the concept of time (e.g. how fresh the trust information is)" [26]. Propagation Models assume that some trust relationships are available in advance. Then, this information must be shared and disseminate to other entities. In fact, these entities have no knowledge about other entities or whether they are trusted or not.

3 Trust management in the context of IoT

We have presented trust generally, now we will describe it within the IoT ecosystem. However, before providing an overview of existing trust management frameworks for the IoT, we have firstly to present what IoT is. Then, we will present an overview of how trust management has been considered in the IoT ecosystem.

3.1 Internet of things (IoT)

One of the first technologies used to allow things communicate among them was called Machine to Machine (M2M). As Watson stated, M2M "is a term used to describe the technologies that enable computers, embedded processors, smart sensors, actuators and mobile devices to communicate with one another, take measurements and make decisions, often without human intervention" [36]. In M2M, the "machines" use a network to communicate with remote application infrastructures only for purposes of monitoring or controlling the machine itself. IoT is an upgrade of this paradigm that allows the objects to interact on their own and with the environment.

About Internet of Things, we can observe that it is composed of two words: Internet and things. With these two words, we can understand the scope of this technology, which connects things among them through the Internet. Surely, the Internet brings many possibilities (i.e. to provide communication anywhere in the world), but also many problems can arise (i.e. threats or cyber-attacks). The word thing is generic. These things can be inanimate or humans (i.e. connected by smart-phones, laptops or tablets). In fact, through IoT we can connect different types of things. How to connect them in a protected and trusted way is one of the main challenges in

this area. In this paper, we will use the term things, devices or entities equally for the same purpose.

An interesting definition of what IoT is useful for has been written by Gazis [37]: "IoT is understood as the (r)evolutionary transition into an era where physical assets and virtual assets will be treated uniformly and, for all intents and purposes, be largely indistinguishable to the processes involving them. The sheer scale of IoT suggests that harmonized global standards will be paramount in realizing a seamless treatment across the physical facet and the virtual facet of things".

We can state that, IoT is a concept and a paradigm that considers pervasive presence in the environment of a variety of things that through wireless/wired connections and unique addressing schemes are able to interact with each other cooperating to create new applications/services and reach common goals. In this context, the research and development challenges to create a smart world are numerous and hard to implement. A world where the real, digital and the virtual are converging to create smart environments that provide energy, transport and services among the smart entities. Moreover, according to the heterogeneity of the IoT, we can state that it is composed of different entities developed by different vendors, each of them with a different purpose and a different life-cycle. We want to focus on the word different to make clear that it is a complete heterogeneous environment in every aspect.

Hence, the goal of the IoT is to enable smart entities in order to be connected any-time, any-place, with anything and anyone ideally using any path network and any service [1]. Things can make themselves recognizable and they become "intelligent" by making or enabling context-related decisions. They can provide information about themselves or access information provided by other things. Moreover, together with other smart entities they can be components of complex services. Anyhow, it is expected that these entities have to interact with each other often under unclear conditions. Mechanisms useful to address this need of information can be solved considering trust as a requirement in order to overcome uncertainty. Thus, with the IoT enabling smart homes and smart cities, it is possible to connect everyday entities and control them remotely. To ease this deployment, the manufacturers of the IoT devices allow the owners of such devices to control them even when they are away from their home network. The functionality enables connected devices to be synchronized and take instructions from other smart entities devices[5] and services.[6] One issue is related to the fact that manufacturers of smart things usually include different communication technologies, such as Zigbee or Zwave [38]. These technologies are embedded with either proprietary or one of the many standard protocols [37]. Moreover, they usually cannot communicate directly with each other [39] but with a central station that allow the interactions among them through a "legitimate man-in-the-middle". Another issue is related to the use of different versions of the same technology. For example, in the case of Bluetooth Low Energy (BLE), backward compatibility with previous versions of the same protocol is not always guaranteed [40]. One adopted solution for this problem has traditionally been for the manufacturers to create their own IoT smart hub

[5] http://www2.meethue.com/en-gb/.

[6] https://developer.amazon.com/alexa.

corresponding to the supported devices [41]. Considering these aspects, the challenges in building a set of heterogeneous smart entities allowed to cooperate with each other grows harder.

However, we can distinguish between two main IoT architectures: centralized or distributed. In a centralized approach, we have a central device called smart hub, which is a gateway usually managing group of mostly passive devices. The primary control belongs to the hub itself. The major threat related to this kind of architecture is that, when the smart hub is compromised or stop working, the whole architecture will fail. As Singh [42] stated, many attacks can be performed against the smart home hub. A message modification attack or a replay attack are possible examples of attacks that can have a major impact on a smart home environment. For example, using a replayed signal, the attacker can indefinitely send a command as continuously open and close a window. On the other hand, with a message modification attack, the attacker can modify a parameter set by the user or by the system. Thus, in the event of a fire, for example, the threshold level related to the smoke detection can be modified and this can result in the alarm being switched on too late or remaining switched off. This is a safety risk and it can lead to serious consequences for everybody living in the smart home or the neighbours. On the other hand, in a distributed approach, all the entities have determined rules [43]. Usually, when a condition is satisfied, the related device will execute an action locally and independently without a smart hub command. Substantially, a peer-to-peer communication is expected in this type of network [44]. According to Roman et al. [43], the major risk in a distributed architecture lies in the fact that the entities are not well protected as the central unit is in a centralized architecture. In fact, if an attacker knows how to target a particular node, it will be compromised, for example, leaking private information. Anyway, there are possible different types of this architecture, like the one proposed by Parra [45] where some nodes are in the middle of the communication. It is a sort of mix between a centralized and a distributed architecture where a problem is raised in the case one of these middle nodes fail. If this happens, the architecture will also be partially or completely damaged.

Anyhow, these architectures have been considered in order to create frameworks used in the IoT [3, 46] and some of these structures can be applied to different IoT fields, such as smart cities, smart grids or smart homes [45]. Concerning smart grids, some of these architectures are well known in the industrial control systems [47] where the networks are divided into two or more parts, using firewalls to protect the more vulnerable networks from direct attacks exploited through the Internet. This approach enhances security, trust and privacy [48]. Anyhow, independently from the architecture, to interact, these objects have to communicate among them. As we have shown earlier, the communication can be difficult among different vendors for many different issues. Trust can help to address this need and to make the entities trust each other during their communication.

3.2 Trust in the IoT

In the state of the art, several authors have proposed how to consider trust in the IoT. However, due to the uncertainty, interoperability and heterogeneity of the IoT environment, achieving trust is still a challenge.

Leister et al. [49] stated that "the Internet of Things will connect many different devices. In order to realise this, users must be willing to trust the devices and communication that happens automatically". Moreover, because these aspects have been tackled by unrelated research communities, a holistic approach is desirable [3].

Azzedin et al. [50] stated that the field of trust related to IoT is still in its infancy. With their work, they want to "raise the awareness and the need of behavior trust modeling" in information fusion and IoT areas. In fact, trust in the IoT is very important because in order to begin an interaction, the smart devices have to trust each others.

Elkhodr et al. [51] focused on the fact that in IoT is very important to know the origin of the source of data and understand whether it is possible to trust them or not. Moreover they stated that "this requires not only accurate, secure, and correct data collection processes; but also provisioning of data provenance throughout the life-cycle of an IoT device and the data it produces". Furthermore, in the majority of the cases, the interacting smart entities have never communicated among them in the past. So, they do not know directly each other. For this reason, it is important to create a trust relationship to allow smart devices to communicate among them in a trusted way [52]. In addition, to be trusted is a prerequisite for being socially accepted by a software or an IoT entity [27]. In fact, if there is no trust, it will be difficult to sell a product and increase its market [53].

Wang et al. [54] stated that "indicating trust or distrust of a node is a key issue in the trust management of IoT".

Yan et al. [52] declared that "trust management plays an important role in the IoT for reliable data fusion and mining, qualified services with context-awareness, and enhanced user privacy and information security. It helps people overcome perceptions of uncertainty and risk and engages in user acceptance and consumption on IoT services and applications".

Fernandez-Gago et al. [3] stated that "the Internet of Things (IoT) is a paradigm based on the interconnection of everyday objects. It is expected that the things involved in the IoT paradigm will have to interact with each other, often in uncertain conditions. It is therefore of paramount importance for the success of IoT that there are mechanisms in place that help overcome the lack of certainty. Trust can help achieve this goal". However, in an environment such as the IoT, trust can be related to different aspects. Therefore, there is the possibility that in the same scenario there can be different contexts with different trust relationships. In fact, IoT is dynamic and this aspect affects the trust relationships because if a thing is trusted in a particular context, this could not be true for another context. In this case, if the context change, the trust relationship can change too.

Also reputation is very important in an IoT environment, especially if two or more entities did not have any past interaction among them, reputation can be used as a parameter to define the initial trust level. This is a general aspect, but it

is very important also for the IoT. Hussain et al. [55] stated that trust and reputation are always important in any kind of interaction among IoT entities even this relationship is among Humans-to-Humans (H2H), Machines-to-Machines (M2M) or Human–Machine-Interactions (HMI). They proposed "a context-aware trust evaluation model to evaluate the trustworthiness of a user in a Fog based IoT (FIoT)". They considered a "context-aware multi-source trust and reputation based evaluation system which helps in evaluating the trustworthiness of a user effectively". Ursino et al. [56] stated that "if a thing can have a profile and a behaviour like a human, it is not out of place to extend the concept of trust and reputation to things and to define ad hoc approaches for their computation". The authors studied trust and reputation of a "thing" in multiple IoTs scenario proposing a context-aware approach to evaluate them. However, they've modelled differently the way things and persons are considered. In fact, they have observed that "the number and the variety of available things is leading researchers to model the existing reality as a set of IoTs interacting with each other, instead of a unique IoT." This is an interesting point to be taken into consideration during the development of a smart IoT entity.

Equally to trust management, **reputation management** can be centralized or distributed [43]. In a centralized architecture there is a node that contains all the reputation values of all the nodes. On the other hand, in a distributed architecture each node must store separately the reputation values of all the other nodes of the system. In a reputation system, when an IoT device wants to establish a connection with another device, it needs a reputation value to instantiate its starting trust level. In a centralized architecture (i.e. with a central IoT hub), to obtain the reputation value of the other IoT device, the requesting IoT entity asks to the central hub the reputation value. Once the value is obtained, the requesting IoT device will decide if proceed with the exchange of information. On the other hand, in a distributed architecture, every IoT device possesses some information about the other entities and if a new connection is about to be created the IoT entities exchange their information among them. In both architectures, trust is crucial in order to decide which node to trust and interact to or not. Summarizing, we can state that in a centralized approach the amount of data that must be computed by the single IoT devices are less, but this creates a bottle neck in the communications. On the other hand, in the distributed apporach, the IoT devices needs more computational power.

However, there are researchers investigating how it is possible to reduce the amount of data to be computed in IoT. Li et al. [57] focused on the fact that IoT allow the connection among many heterogeneous devices and trust is fundamental in order to assess the quality of the different available services. Moreover, they consider context crucial because it is possible to trust a service for a particular purpose and not for another. They proposed a "new context-aware trust model for lightweight IoT devices" without storing information about the past behaviours of the nodes because of their limited computational power. In fact, the model needs only a limited amount of stored information and it can resist to several attacks such as badmouthing and on-off.

Another possibility is presented by Fortino et al. [58], where they suggest to "use the capabilities of nearby devices having suitable resources, given that they make their resources available for free or with a determined cost". They propose a solution

"where each IoT device is associated with an agent that helps its device in choosing reliable partners for its tasks". They use reputation as a "countermeasure against malicious IoT devices".

In a subsequent work, Fortino et al. [59] have also analysed the up-to-date IoT architectures explaining how to integrate them with nodes belonging both to the fog and edge computing paradigms. Edge computing is strongly used in IoT, Sadique et al. [60] investigated an integration of distributed trust management in the IoT through edge computing technology, considering scalability and heterogeneity of the IoT devices. Moreover, Junejo et al. [61] proposed a "trust management system for fog-enabled cyber physical systems". They consider the trust values computed by their model in order to assess a credibility factor for each node of the system. This factor helps to avoid and isolate malicious fog nodes and preserve the others.

Furthermore, about Fog computing and trust, Alemneh et al. [62], proposed a two-way trust management system for fog computing. The authors aim that guaranteeing trust you can also provide security and privacy. More specifically, they proposed a "logic-based trust management system that enables a service requester to verify whether a service provider can give reliable and secure services and lets the service provider check the trustworthiness of the service requester".

Summarizing, in the state of the art trust and IoT have been investigated by several authors and some of them have proposed different frameworks in order to include trust in a system or a software. In the next part, we will both present frameworks developed to include trust in the IoT and also some general frameworks (not specific for the IoT) that can be used (even if with a lower impact) in the IoT.

4 Frameworks for trust and IoT

In this section, we present frameworks developed in the state of the art to include trust in the IoT. We have chosen these works, because each of them presented interesting approaches in order to compute trust in different ways and using several architectures. Even if some of them are not recent, to the best of our knowledge the insights presented by them are still valuables. However, each of the work that we will present here has flaws. We will discuss them in Sect. 6, where we compare all the frameworks provided in this section according to six important parameters.

However, we have highlighted how IoT is a dynamic and heterogeneous environment, for this reason determining the real intention of the devices is a fundamental dilemma for a human. Thus, in order to assist devices to join an IoT network in a correct way, Køien [63] proposed a subjective logic system to model human-to-device trust interaction. Hence, the author studied trust in an IoT device and services in multi-faceted software/hardware approaches considering trust properties such as transitivity, integrity, or benevolence.

In IoT, we can also consider Cloud of Things (CoT). Abualese et al. [64] stated that CoT is a paradigm strongly used by e-government and, in this aspect, trust is of critical importance and also a challenge. Thus, they proposed a framework in order to enhance trust among IoT devices connected to the cloud. Their framework is composed of four layers. One of them is dedicated to trust in order to authenticate the

IoT devices. They used several authentication methods "to differentiate the access control for each device". In order to tackle the low-power of the IoT nodes, Fortino et al. [65] defined a CoT virtualizing physical devices over the cloud environment and integrating them with software agents to honour their responsibilities. Considering parameters and an adequate number of participants, they demonstrated that their CoT Agent Grouping (CoTAG) algorithm rapidly converged to deal with untrusted agents and computation overhead. CoTAG considers mutual trust such as local reputation and suitable voting.

Considering Wireless Sensor Network (WSN), Ali et al. [66] outlined a trust scheme for WSN, where data aggregation has been considered for external mobile components for distributing the data towards the base station. Such components were either portable sensors or smart mobiles representing clusters in IoT networks. The authors employed a beta distribution cluster-based routing algorithm, and a dynamic forgetting factor in reducing trust manipulation by malicious components.

Mendoza et al. [67] proposed an IoT distributed trust management framework considering direct interaction such as neighbors discovering and indirect observation (i.e. trust table exchanging, evaluate recommendation, and refresh scores). Local trust calculation mechanisms were divided into different phases initiated by the assignation of negative/positive values to honest/dishonest nodes.

Pal et al. [68] proposed a trust management framework focusing on access control mechanisms (i.e. decision models) improving decision-making processes under uncertainty. They provided an attribute-based identity management. In their proposed trust model, the access control decision has been made considering three different types of trust: direct, recommended and derived. Then, Bernabe et al. [69] proposed a trust-aware access control mechanism (TACIoT). In order to perform authorized decisions, this approach considers four parameters: quality of service, reputation, security, and social relationships. Therefore, to handle the information uncertainty, a fuzzy logic method is used, which relies on historical trust evidence. However, due to scarcity of evaluation on trust accuracy, they also planned experiments on identity features to ensure secure interaction and shared data within communities in a trusted way. In addition, Mahalle et al. [70] proposed a fuzzy trust-based decision-making model for access control (FTBAC). In order to compute a trust value, the framework considers parameters such as experience, knowledge, and recommendation. They are outlined to obtain access privileges in a loT network. The authors demonstrated the flexibility and scalability of their work. In fact, the number of devices does not deteriorate its efficiency.

On the other hand, considering evaluation models and analysing the fact that mobile technologies are enablers for IoT, Bica et al. [71] proposed a security framework with a multi-layer architecture addressing trust evaluation of sensing entities based on reputation scores computed by a Bayes algorithm. Moreover, DeMeo et al. [72] proposed a Reputation Framework for the IoT embedded with a Reputation Agent (RA) acting inside an entity. This RA is separated from its belonging entity in order to estimate an "honest" reputation value. This is an interesting approach, but it is vulnerable to self-promotion attacks in the case that the device is manipulated. Surely, a reputation score given by another trusted entity is more reliable. Furthermore, they state that it would be infeasible to effectively apply an

approach based only on authentication deal with trust issues in a wide environment such IoT.

Ruan et al. [73] proposed a trust management framework for IoT that is based on the measurement theory [74]. However, the authors considered only two metrics: trustworthiness and confidence. An interesting aspect is that they have modelled interactions between the IoT entities dividing them into four types of interactions: human/human, things/things and human/things interactions (in both directions). Moreover, they have considered reputation in order to calculate a trust level showing how trust can be helpful in recognizing which nodes are malicious or trusted. However, they have analysed only two types of attackers, so their framework is useful only against certain types of threats. Moreover, Ruan et al. [31] proposed a general trust management framework. It is composed of three phases. The first one is called "Trust Modeling", in this phase the available trust raw data are collected from the fields and computed with trust metrics. The second phase, named "Trust Inference", focuses on propagating and aggregating the obtained trust values over the system. The final phase, "Decision Making", will use the trust values computed in the previous phases in order to support the decision making process. Each of these phases is dependent on the context. This is a focus point to take into consideration. However, this framework was not developed specifically for IoT and it covers only one phase of the SDLC (the modelling phase). Then, Sharma et al. [75], have presented a generic framework to manage trust in the IoT considering both qualitative and quantitative parameters. They have proposed a trust management solution considering all the requirements useful to perform trust management. This framework is interesting but its main weakness is that there is only one feedback from the very last phase coming back to the first phase. This is a huge limitation in the case any issue is encountered in the middle of the framework. In addition, another disadvantage is that the context has never been taken into consideration. Moreover, Bahutair et al. [76] considered an adaptive trust model for IoT services. The trustworthiness of these systems is assessed by the users utilization. In order to determine if a system can be trusted or not, an algorithm process several trust factors through four different stages. The first stage predicts the trust factors. The second stage compute these parameters in order to predict the trustworthiness of the system. Then, in the third stage, a "usage-to-factor model" is built to detect how important is each factor for different scenarios. Finally, the last stage is composed of two models. Their aim is to compute a trust value according to the scenario chosen in the previous phase.

Recently, Battah et al. [77] proposed a general trust framework to regulate IoT service interactions using reputation systems and blockchain technology. They proposed a reward-penalty scheme through a customizable architecture for IoT devices. In order to guarantee this, they implemented smart contracts to store information without using centralized models.

According to SDLC there are only a few works considering it for trust and IoT. One of them has been presented by Fernandez-Gago et al. [3]. They moved forward with respect to the previous works introducing a framework to help designers and developers in considering trust in the IoT. They stated that privacy and identity requirements must be taken into consideration during trust and reputation management in order to enhance trust. However, in this framework there is

no feedback between phases and there is no connection among privacy, trust and identity requirements. Finally, they model only the first phases of SDLC. Starting from this work, Ferraris et al. developed a trust-by-design framework for the IoT [6]. The authors proposed a framework in order to guarantee trust during the development of an IoT entity considering the whole SDLC. Moreover, this framework guarantees a careful planning from the developer perspective. In addition, starting from the fact that trust is strongly related to other properties such as privacy and security, it is considered the possibilities to connect them since the requirement phase. Other two important aspects are traceability and the context. The former is provided among the different requirements and among the different phases of the framework. The latter is fundamental in order to consider trust in a particular IoT interaction.

Privacy in the IoT has been considered also by Dwarakanath et al. [78]. The authors proposed a trust-based approach for distributed complex event processing (TrustCEP). The authors leveraged trust among different users according to their past interactions. However, this trust management model is effective in the case adversaries are a minority of the total nodes.

Other works focusing on context are the following. Wang et al. [79] developed a context-aware trust management model (CATrust). It can be used both for P2P and IoT and it analyses the behaviour pattern if the context changes, instead of estimating truthfulness considering satisfactory/unsatisfactory history data. By taking into consideration recommendation filtering mechanisms and quarantining dishonest nodes, CATrust recognizes colluded nodes. Then, Saied et al. [80] designed a context-aware and multiservice trust management system for the IoT to mitigate the lack due to the heterogeneity of entities. Their model provided the IoT nodes with a dynamic trust value based on past behaviours in order to achieve a required task in cooperative service and then convinced the most suitable partners for the cooperation. The authors claimed that the proposed system detached malicious nodes intrusions. Moreover, Neisse et al. [81] presented a dynamic context-aware trust framework for the IoT. They have also considered privacy and security, together with identity requirements. They focused on the fact that a tradeoff between privacy and security exists and it must be tackled not only by the researchers, but also by society in general. However, they recognized that a limitation of their approach lies on the fact that the perception of the context can be ambiguous according to the data collected by the sensors used. Thus, they confirm that the consideration of the context is crucial as a pre-requisite for an effective framework for IoT.

Finally, we consider frameworks related to trust in the growing segment of Social Internet of Things (SIoT)., Lin and Dong [82] developed an SIoT dynamic trust model composed of fundamental factors such as trustor and trustee, context, trustworthy estimation, and its consequences). Unique features of SIoT trust are considered mutual protection of trustor and trustee. Infers trust by exploring historical features. Update trust with delegation results of both positive and negative factors, and adjust it considering the influence of dynamic environments. Moreover, Magdich et al. [83] proposed a work regarding a study on the effectiveness of trust management in relation with social attacks. They proposed a trust model that classify the nodes behaviours using machine

learning algorithms. Through this aspect, they want to limit the possible interactions both with attacker nodes and poor service provider nodes.

5 Methodology

In this section, we will present the six parameters that we believe are fundamentals in order to consider trust properly in IoT. Such, parameters will be then used in order to analyse the existing frameworks.

The first of the six parameters are related to which trust models are used in the frameworks. The models can be related to the main ones considered in [26] or they can be related to adaptive trust models similar to the one presented in [41]. We have deeply described them in Sect. 2.2.

Then, we will consider trust attributes such as the characteristics of trust that we have identified in the state of the art. We will present them in the following sub section.

Thirdly, we will take into account which IoT architecture has been considered in the selected paper. The more known architectures are usually centralized and distributed as discussed in [1]. We have described them earlier in Sect. 3.1 and we believe that SDLC can be helpful in carefully planning solutions for trust in the IoT.

Thus, we believe that analysing the SDLC and how the existing frameworks apply to it, and in which phases trust is considered is of paramount importance. It could aid to adapt the development of the entity to the multiple aspects of trust. In fact, if we consider trust early in the SDLC, we can start building requirements according to it [84] and such requirements can be helpful in the following phases such as the model phase, where the requirements can be used in order to create diagrams and models that predict how the IoT entity will behave and interact with other IoT entities under a trust perspective. These previous phases will be fundamental to develop [85], verify and validate [86] the IoT entity. Finally, it is acknowledged by the research community that considering properties such as security or trust earlier in the SDLC, we can avoid problems later in the final phases. This process is called left-shift [87, 88].

Therefore, we consider also that trust can be enhanced if other properties are considered such as security or privacy. We call them domain as we have done when developing the TrUStAPIS methodology in [84]. We will present them in the following subsections.

Finally, we will consider different activities connected to trust that can enhance it in the IoT. They are related to the context consideration, traceability, decision-making, risk and threat analysis.

In the following subsections, we will analyse the aforementioned parameters that were not described earlier: trust characteristics, trust connected properties and activities related to trust.

Table 1 Characteristics of trust

Direct	[34]
Indirect	[89]
Transitive	[15, 90]
Directed	[15]
Dynamic	[5, 9, 91]
Context-dependent	[26, 89]
Local	[89, 90]
Global	[89]
Specific	[92, 93]
General	[92, 93]
Asymmetric	[94]
Subjective	[9, 15]
Objective	[89]
Composite-property	[9, 15]
Measurable	[15]

5.1 Characteristics of trust

In order to properly consider trust in a system such as the IoT, it is important to elicit trust characteristics. In fact, according to them, it is possible to model different aspects of IoT.

We have identified fifteen characteristics of trust that must be taken into consideration in order to implement trust in a system such as the IoT. We have summarized them in Table 1 where the first column is about the characteristic and the second one contains the works defining such characteristic.

The characteristics of trust are here presented and described:

1. **Direct.** This property means that trust is based on direct experiences between the trustor and the trustee [34]. In this case, we can say also that trust is history-dependent.
2. **Indirect.** We can talk of indirect trust, when the trustor and the trustee did not have past interactions. In this case, trust is built on the opinion and the recommendation of other entities trusted by the trustor [89].
3. **Transitive.** We can also refer to the possibility that trust is transitive [90]. In fact, trust is conditionally transferable, as Yan stated, we can imagine the possibility to transmit/receive trust information along a chain of recommendations [15]. However, in this case context is fundamental.
4. **Directed.** Trust is also directed because there is an oriented relationship between the trustor and the trustee [15]. This means that if A trusts B, we cannot also imply that B trusts A.
5. **Dynamic.** Trust can change over time, but it is not strictly time dependent. Chang [91] stated that "trust builds with time". In fact, a trustor could trust the trustee about something in a period of time, but this trust level could change in a following period because something could have happened [5] in order to

modify the original trust level. Moreover, as Grandison stated [9], trust must be able to adapt to the context in which a trust decision has been made and can change according to different contexts.

6. **Context-dependent.** As we mentioned before, trust can change depending on the purpose where it is used. "In general, trust is a subjective belief about an entity in a particular context [15]." and more specifically "where the trust of a node i in a node j varies from one context to another [89]".
7. **Local.** Trust can be **local** [89] because it depends on the considered couple of trustor and trustee (i.e. Alice and Bob) and if we consider other two couples (i.e. Alice and Charlie, and Bob and Charlie), it is possible that Alice distrust Charlie, even if Bob trusts Charlie [90].
8. **Global.** As Abdelghani stated "trust also called reputation means that every node has a unique trust value in the network which can be known by all other nodes [89]".
9. **Specific.** We can state that trust can be specific [92, 93]. This happens because it is possible that the trustor trusts the trustee only for a specific action or service.
10. **General.** On the other hand, trust can be general [92, 93]. Trust is general if the trustor trusts the trustee generally and not only for a specific action.
11. **Asymmetric**. This means that two entities tied by a relationship may trust each other in different ways, so the fact that A trusts B does not imply that B should trust A [94]. This is connected to the definition of "directed".
12. **Subjective.** Trust is subjective because it is related to a personal opinion based on various factors (i.e. past experience) and these factors can have different weights [9]. Trust is different for each individual in a particular situation [15].
13. **Objective.** On the other hand, trust can be also **objective** "such as when trust is computed based on Quality of Service (QoS) properties of a device [89]". Furthermore, an objective parameter to compute trust is also known as **reputation**.
14. **Composite-property.** Trust is usually a composite-property because can be composed of many different attributes. For example as Grandison [9] stated it can be composed of "reliability, dependability, honesty, truthfulness, security, competence, and timeliness". Thus, compositionality is an important feature for trust calculations [15] and every attribute could have different weight.
15. **Measurable.** Finally, trust is measurable. In fact, "trust values can be used to represent the different degrees of trust an entity may have in another. [15]." This characteristic is the basis for the computation of a final trust value during trust management.

The aforementioned characteristics and their relationships are explained in Fig. 2.

The external circle means that the characteristics written there are always present. Then the characteristics inside the internal circle are still important in every aspects (i.e. directed and asymmetric). *Transitive* is written in italic because it is not always true and it is filled in a separated rectangle. Finally, we can see that there are three couples connected by dotted lines. These couples are mutually exclusive. In fact, trust can be specific or general, subjective or objective and local or global. In the same time, trust can be for example specific, objective and global. Finally, in the

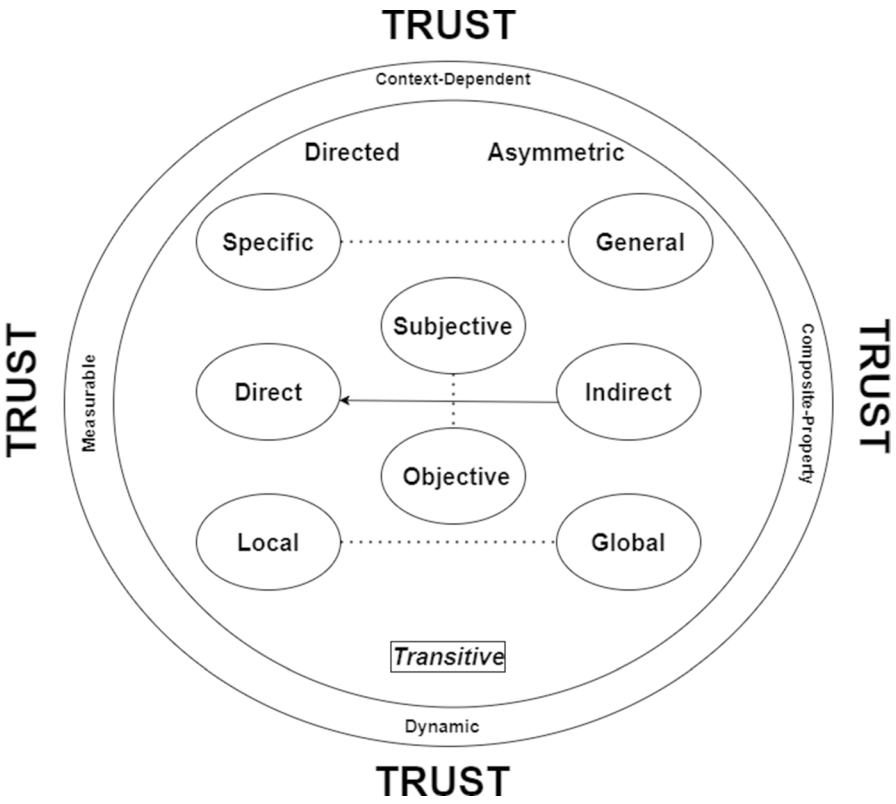

Fig. 2 Trust characteristics and their relationships

centre of the diagram there is the final couple: direct and indirect. In this case, we have an arrow moving from indirect to direct and it means that sometimes it is possible that the indirect trust can create the direct trust. This situation happens when there is no direct knowledge (i.e. no past interactions), thus in order to start building a trust value, we need an indirect parameter and this interaction is represented by the arrow.

5.2 Trust connected properties

In this sub section, we focus on trust connected properties such as security and privacy, we will refer to them also as domains. In the state of the arts, several authors highlighted the importance of considering trust together with other properties.

According to Hoffman et al. [4] and Pavlidis [5] trust is strongly dependent on other properties or domains (i.e. privacy, identity and security). Moreover, in the state of the art, there are several works about trust properties that proposed a classification of them [15, 95]. Some of these properties have been considered by

multiple authors in the following years. However, we will focus on the ones presented by Hoffman and Pavlidis that basically contains also the others.

Hoffman [4] proposed a trust model which considers the following properties related to trust: reliability & availability, privacy, audit & verification mechanisms, security, usability and user expectations.

Reliability, privacy, security and usability are also considered by Pavlidis [5]. The author considers also availability as a sub-property of security. Moreover, he takes into consideration safety and maintainability.

We focus on the properties taken into consideration by both authors. They are the following:

- **Availability.** It means that the actions of the systems are not paused or stopped for long periods.
- **Privacy**. Privacy concerns some features like granting confidentiality or anonymity. This property can enter in conflict with accountability [96]. Moreover, privacy is also important, because nowadays the information systems can collect very easily a huge amount of personal information, this aspect raises a risk about the possibility that those data can be accidentally or intentionally disclosed. This situation can affect users' trust negatively. For Pavlidis, privacy has four sub properties: anonymity, unobservability, pseudonimity and unlinkability. Anonymity is the ability to not be identified, unobservability is related to the possibility to not be observed and pseudonimity gives the possibility to use aliases. Unlinkability can be derived by anonymity and unobservability.
- **Security.** Security is composed of sub properties like to grant that the entities involved in a process are authenticated, that they have rights to access data and that the data are not corrupted. However, it is not only a property of trust as Yan stated: "trust is beyond security. It is a solution for enhanced security [15]". In fact, for Pavlidis, *security* must be taken into consideration especially in the case we do not consider trust in the design of a system. In this case, we need to make the system secure as much as we can because it is the only defence against malicious entities. On the other hand, if we consider trust, it is possible to relax some security features because the users will be trusted to perform particular activities. For Pavlidis, security has five sub properties. Confidentiality, integrity and availability are known as the CIA triad. Authentication and authorization are very important properties also for trust.
- **Usability**. This property is important because, according to Hoffman, if a system is difficult to be used and understood, a user trust could be affected. Furthermore, if a system is difficult to use in a correct way, it is possible to use it incorrectly. This may lead to problems and, as a consequence, this can lower the overall trust level on the system itself [95].
- **Reliability**. It is an attribute that is very important for a system trustworthiness. In fact, reliability has been defined as "the probability that a system will perform a specified function within prescribed limits, under given environmental conditions, for a specified time" [97]. Anyway, we will consider it as a sub-set of trust.

- **Safety**. Safety is strongly related to the physical domain. Preventing a user to be harmed will increase the trustworthiness of the system, because the user will perceived the system as safe and trusted.

Hence, we can affirm that trust can be connected to other domains or properties (i.e. privacy or security) and these domains have characteristics fundamentals to define them. This aspect shall be taken into consideration for trust management. Ferraris et al. [84] took the works of Hoffman and Pavlidis into consideration and moved forward specifying six domains connected to trust: safety, security, privacy, identity, availability and usability.

5.3 Activities

In the state of the art, many authors discussed about how trust can be enhanced not only by other properties, but also by other activities such as decision-making [98, 99], traceability [100, 101], risk management [102], threat analysis [103] and context considerations [79].

- **Decision-Making**: This property can significantly enhance trust management. Especially in an ecosystem such as IoT. In fact, in this complex and interconnected environment, trust can play a critical role in guiding decisions. Decision-makers can rely on trusted IoT data to optimize processes, predict outcomes, and respond effectively to changing conditions. As we have discussed earlier, dynamicity is crucial for trust and IoT. Moreover, trust management systems can assess and quantify the credibility and reliability of IoT entities, ensuring that decisions are based on data and interactions that are reliable and secure [99]. Ferraris et al. proposed a decision-making process in order to solve conflicts among requirements elicitation in IoT [98]. This process is based on Analytic Hierarchy Process (AHP) initially proposed by Saaty [104].
- **Traceability**: Traceability plays an important role in trust management in various domains [100]. By providing a transparent and auditable record of actions and transactions, traceability provide accountability and integrity within systems and processes. This transparency is essential for building trust among stakeholders. In the IoT, traceability enhances trust by providing transparency, accountability, and verification of data, actions, and interactions. It is a vital component for ensuring that IoT systems operate reliably and securely while meeting regulatory and user trust expectations.
- **Risk Management**: Risk management and trust management are closely intertwined concepts, particularly in the fields of cybersecurity, business and decision-making [102]. Risk management entails the identification, assessment, and mitigation of potential threats and vulnerabilities within a system or organization. Trust management is the opposite as we described in Sect. 2. The connection between the two lies in the fact that a robust trust management system can be instrumental in effective risk management. By assessing and quantifying trustworthiness, organizations can make more informed decisions about who

or what to trust, thereby mitigating risks associated with untrusted entities. A strong foundation of trust and credibility is essential for effective risk management, ensuring that risks are managed prudently and trust is maintained throughout the decision-making process.

- **Threat analysis**: Threat analysis is a fundamental component of trust management in the realm of cyber security and risk assessment [103]. By systematically identifying potential vulnerabilities and malicious actors, threat analysis provides the necessary insights to perform trust and security measures. Through a comprehensive examination of potential threats and their potential impact on a system, trust management can address and mitigate the possible attacks. By understanding the landscape of threats, trust management can make informed decisions about access control processes. Threat analysis assists in building trust by creating a safer digital environment, ensuring the integrity of data, and increasing the confidence of users and stakeholders. Finally, the synergy between threat analysis and trust management is crucial for maintaining the security and reliability of digital systems in an increasingly interconnected world such the one called IoT.
- **Context**: Context is at the centre of trust and IoT considerations as we have discussed in the previous sections. For example, the context of use, environmental factors, security and privacy considerations and the history of a device performances can influence the level of trust that the final users will place in IoT technologies. For example, a healthcare IoT device may require a higher level of trust due to the critical nature of the data it handles, while a smart home device may have different trust requirements according to different possibilities as presented in [41]. Understanding and adapting to the context in which IoT systems will behave, it is an essential part for building and maintaining trust among entities. Additionally, context-aware trust management can help mitigate risks, improve user experiences, and ensure the reliable operation of IoT solutions [79].

All these definitions are strongly connected among them. Thus, we can see how these connections can improve them especially in trust and IoT which can be enhanced from their implementations.

6 Analysis of IoT trust frameworks

As we have proposed in Sect. 5, we have identified six parameters that we believe are important when considering trust in the IoT. In Table 2, we have collected them in six columns. The first one is related to which kind of models have been developed in the selected work (i.e. trust decision model). The second column contains trust attributes where are collected the characteristics of trust summarized in Sect. 5.1, trust metrics such as data aggregation, trust actors (i.e. trustor and trustee) and trust parameters such as reputation. Then, there is the IoT Architecture developed within the selected framework. The fifth column is related to the SDLC and if it has been considered in the selected work. Then, there are the domains identified by [4, 5, 84] related to trust (i.e. privacy or security) and that we have summarized in Sect. 5.2.

Table 2 Frameworks properties

Authors	Models	Trust attributes	IoT architecture	SDLC	Domains	Activities
Abualese et al. [64]	X		X			
Ali et al. [66]		X	X			
Bahutair et al. [76]	X		X			X
Battah et al. [77]	X	X	X		X	
Bernabe et al. [69]	X	X	X		X	
Bica et al. [71]		X			X	
De Meo et al. [72]		X				
Dwarakanath et al. [78]	X	X	X			
Fernandez-Gago et al. [3]	X	X	X	X	X	X
Ferraris et al. [6]	X	X	X	X	X	X
Fortino et al. [65]	X	X	X			
Lin et al. [82]	X	X	X			
Køien [63]	X	X	X			
Magdich et al. [83]	X	X	X		X	X
Mahalle et al. [70]	X	X	X			
Mendoza et al. [67]		X	X			
Neisse et al. [81]	X	X	X		X	X
Pal et al. [68]	X	X			X	X
Ruan et al. [73]		X	X			
Ruan et al. [31]	X	X		X		X
Saied et al. [80]	X	X	X			X
Sharma et al. [75]		X		X		
Wang et al. [79]	X	X	X			X

Finally, in the last column we consider activities that are not strictly related to trust but they are important in order to maximize its level in each framework (i.e. traceability, decision-making), we have presented them in Sect. 5.3.

For each line of Table 2, we have written the first author of the paper presenting the frameworks explained in Sect. 4. In this table, we show which work covered the parameters, where the parameters has been considered we put an X. Otherwise, the field is left in blank. The table is located in the Appendix Section.

For each framework, we will explain in detail which parameters are considered and how they have been implemented.

6.1 Frameworks analysis

In Table 2, we can observe the composition of the frameworks according to the six parameters (if they are considered).

We start with a generic analysis in order to check the parameters implemented in the works. Then, we will analyse the frameworks more in details.

Thus, we can observe that only in [3] and [6] all the parameters that we have identified have been considered, however if we go into details both of the work lack in fulfil the six parameter completely. The other works focus only on several aspects without considering a specific IoT architecture such as in [68, 71–73, 75] or without a clear consideration of trust attributes [64, 76]. Moreover, the SDLC is considered only in [3, 6, 31, 75], but only one of them have represented all the phases [6], the other three implemented only early phases [3, 31, 75].

Then, in [69], even if SDLC and trust related activities are not considered, all the other parameters have been investigated (i.e. models, trust attributes, IoT architectures and trust related domains). On the other hand, there are works that consider only two parameters, for example [64, 66] or even only a single parameter, for example the trust attributes in [72].

About context, it is directly considered in [79–81], but it is the only activity taken into account by the same authors. Moreover, trust attributes such as reputation are considered in [67, 77, 79, 105] or past history relationships in [78, 80, 82]. Finally, there are a few authors that did not considered a model specification [66, 67, 71–73, 75].

We will now present more specific considerations about the works showed in Table 2.

Starting with Fernandez-Gago et al. [3], we can state that the authors proposed both decision and evaluation models for trust. We have described them in Sect. 2.2. However, the trust attribute considered is mostly reputation, which is the higher factor that the decision maker will take into consideration in order to perform a choice among different operators. The "winner" is the one that has the higher rank among the available ones. The architecture is strongly related to the scenario. In their example, they propose a system composed of several IoT devices communicating with a central hub. Thus, we can define it as a centralized architecture. However, as the authors suggested, it is also open to a distributed one. A weakness is that the SDLC is considered only for the early phases (i.e. requirements, model and development). Even if these phases are fundamentals in order to create the right system, other phases should be taken into consideration such as verification and validation. Moreover, it considers only privacy and identity as connected properties to trust. Even if they are very important, other domains should be taken into consideration such as security and safety in order to holistically consider the system. Finally, we can observe that the context is taken into consideration. This is a very important parameter, because it can delimit the trust parameters according to the chosen context context and we can state that trust change according to the context. Finally, they implement decision-making in order to choose the most trusted operator to fulfil a particular goal.

Another interesting work is the one developed by Ruan et al. [31]. This work considers several phases of the SDLC and analyse trust with its characteristics and related activities such as decision-making (that is crucial for one of the three phases considered). However, it is not specific for IoT, thus it does not propose any particular architectures and it does not consider any of the other domains connected to trust. This aspect has been tackled by another work of the same author [73] where, even if the SDLC is not considered and they do not propose a specific model, they take into

consideration the differences among the possible interactions among actors in an IoT environment. For example, if we have a Device-to-Device (D2D) communication, the rules and the implementations will be very different from a Human-to-Device (H2D) interaction. About trust attributes, as we explained before, they have considered metrics and trustworthiness. However, this work considers only two parameters, but the two works combined can partially cover all the parameters except the connected domains.

More generally, if we consider Wireless Sensor Network (WSN), Ali et al. [66] have implemented a framework that considers data aggregation of the composite properties of trust in order to create a trusted area where the nodes can exchange information among them. In order to discriminate among good nodes and bad nodes, the authors implement a threat model under the perspective of the attackers. However, without a full consideration of other important domains such as security, the work cannot cover properly this aspect.

Then, Pal et al. [68] considered an important aspect belonging to a trust relationship, especially for an IoT environment where it merges a direct and an indirect recommendation system. This is useful because it is possible that two IoT entities know each other and can interact according to what happened in a direct experience, but it is also possible that two entities that does not know each other wants to interact. In this case, a derived trust must be considered in order to allow or not this kind of communications. However, they did not present a complete architecture and they did not consider at all the SDLC.

In Ferraris et al. [6], the authors proposed an adaptive trust model that is mostly explained in [41]. This, model is important especially in a smart home environment, but it can be specified also for other environments (i.e. smart grid), but not for distribute architectures. Basically, it is divided into three different phases: join, stay and leave. These phases are always present in an IoT environment. In the first case, a trust decision is performed for new devices joining the network. Thus, analysing the device (i.e. reputation and known issues), another important parameter that is considered is the context in which it will behave interacting with other devices. Then, the stay phase is a continuous monitoring on the behaviour of the devices. If a suspect behaviour will be performed by an entity of the network, a trust decision will be performed. This decision is similar to the join procedure and in the case it produces a negative output, the device will be banned from the network or put into quarantine. Finally, the leave procedure is basically a disconnection from the network. According to trust attributes, the authors consider reputation and a large set of the characteristics presented in Table 1. The IoT Architecture is strongly connected to the adaptive trust model discussed before. In fact, according to the trust decision and the typology of the IoT device, it can be connected to an internal or an external network. The internal network provides a better protection for IoT devices that have a limited computational power. Moreover, the trust level for this network is higher than the external network. In the external network, there will be considered also devices belonging to the Bring Your Own Device (BYOD) paradigm [106]. However, the trust monitoring is the same for the internal or external network. In this work, the SDLC is fully considered since the early phases of it to the final ones. Thus, in the need phase it is analysed why an IoT device should be developed. Then,

in the requirements and model phases, the IoT device is strictly analysed in order to design all the possible functionalities and interactions. In the development phase, these functionalities are built and developed. Then, in the verification and validation phases, test and checking are performed to analyse that the IoT device functionalities properly work and to reflects its intended purpose. Finally, the utilization phase is the one where the IoT device will interact with other devices and users for its intended purpose. The domains analysed are a combination of the ones proposed by Hoffman and Pavlidis [4, 5]. Finally, the activities proposed by this IoT framework wants to cover a wide range of possible aspects. Traceability allows the connections among phases and among elements of the IoT device under development. Decision-making, threat modelling and risk management are strongly connected in order to perform trust decisions. Then, documentation is collected in each phase and the gates are the activities allowing the continuation of the flow during the SDLC phases.

Related to the joining process in an IoT network, Køien [63] proposed a trust model for the interaction between humans and IoT devices. Moreover, the author considered trust attributes such as transitivity, integrity, or benevolence. According to them, the author encouraged Trust Network Analysis-Subjective Logic (TNA-SL) models analysing the behaviour of an entity in an asymmetric network where tryst is asymmetrically propagated as well as reputations/opinions broadcasting. However, according to the fact that his research lacked of other important activities such as risk management, he inspired other researchers in this area [107].

About the SDLC, Sharma et al. [75], have presented a generic framework to manage trust in the IoT where they focused especially on the requirements phase considering qualitative and quantitative parameters, the following phases are just for the development of the requirements. However, even if the framework is interesting, it has some flaws such as a single feedback from the final phase to the first one and it never consider context that is a crucial aspect when considering trust and IoT.

On the other hand, context has been considered by Bahutair et al. [76]. In their work, the authors considered an adaptive trust model for IoT. It compute the trustworthiness of an entity following a four stages architecture. This is an interesting work, with only a few limitations depending on the fact that it does not consider trust-related domains such as security, privacy or identity.

According to the framework developed by Mendoza et al. [67], they have considered how trust can be useful using discoveries protocols in an IoT architecture where the neighbors use indirect trust in order to start computing a direct trust value. Some disadvantages are higher network traffic and energy consumption due to higher update interval, otherwise this method will suffer of long delayed false diagnosis. This can be a problem in other connected research lines such as the growing Green IoT [108] paradigm. However, their work did not consider other parameters and probably the SDLC consideration could have helped in finding a different solution with a lower energy consumption.

About the framework proposed by Abualese et al. [64], it has considered specifically IoT under the perspective of Cloud of Things (CoT). Thus, from this point, he enhanced the possibilities for IoT devices connected to the clouds to enable their interactions following trust decision models rules. Even if the work is very

interesting and highly focused on a particular area, it does not consider specifically any trust attributes, neither the SDLC, nor trust connected domains or activities. In the same area, Fortino et al. [65] defined CoT but from another perspective. In fact, the authors implemented trust evaluation models especially considering reputation parameters instead of decision models. With their experiments, they showed that in small groups of IoT nodes, their algorithm rapidly converged according to the reputations of the agents. Allowing the trusted nodes to deals with untrusted nodes. Their approach considers that trust is computed starting from local reputation. However, SDLC is not considered, neither trust connected activities or domains, limiting the overall contribution.

Accoring to the evaluation models, Bica et al. [71] proposed an interesting framework that addresses trust evaluation in a mobile architecture considering security and reputation. It is valuable even if it is not specific for IoT, but this work can be useful for future frameworks that can implement missing aspects such as a SDLC consideration and trust connected activities.

Focusing on reputation, De Meo et al. [72] proposed a framework fully based on reputation where a general entity has inside a reputation agent. However, it acts as a separated entity in order to evaluate the behaviour of the entity. Even if the framework considers only a general idea on how trust and reputation can be used, it can be considered as a starting point for works that consider root of trust [109] for IoT devices.

Another work that major consider reputation has been developed by Mahalle et al. [105]. The authors performed an interesting analysis about their IoT architecture. In fact, they proposed an algorithm to explore nodes following recommendation systems and shared knowledge. Thus, it is possible to compute a trust value to allow IoT entities exchange communications among them. Then, in order to perform this activity, reputation is a fundamental parameter according to the trust level that an IoT device has in the other known IoT entities. In fact, it they trust another entity, they can start the computation of a trust value following the recommendation system, otherwise they will explore other nodes in order to compute a trust value for an unknown IoT entity.

Moreover, reputation has been considered in the recent work developed by Battah et al. [77]. The authors proposed a decentralized architecture that take into consideration also trust related domains such as privacy and security.

Moving forward, we analyse another study starting from a completely different approach. In fact, Dwarakanath et al. [78] considered only history dependence among devices avoiding reputation analysis. Moreover, they restrict the possible interactions only to H2D and D2D, avoiding the consideration of H2H, because they consider that a human user, in order to interact with another human (under an IoT perspective), must use a device. Thus, for them, H2H is a subset of D2D.

According to decision-making, an interesting work is the one proposed by Bernabe et al. [69]. The authors perform a decision model analysis considering mostly access control. However, they implement also particularity of evaluation models such as reputation and history dependencies among entities. Connecting to this aspect, they propose an IoT architecture that is strongly connected to the social relationship among the entities. Thus, an IoT device belonging to a user can trust another user if the latter has

a social relationship with the former. On the other hand, if there are no social relationships, the IoT devices cannot trust the user avoiding the interaction. Overall, we can state that important domains such as privacy are not considered and we believe that especially in a social IoT environment, it must be taken into consideration. However, they consider important domains such as identity and security in order to guarantee that the interactions are secure and performed with identified entities.

A most recent work proposing a framework that considers trust in the SIoT is the one presented by Magdich et al. [83]. They focus especially on reputation aspects. However, they considered separately an important parameter such as the context only in relation to a specific attack (i.e. Opportunistic Service Attack (OSA)).

According to the context considerarion, we want to highlight the works of Saied et al. [80] and Wang et al. [79]. They consider context precisely and according to it, they compute a different trust value. But they did not consider other domains related to trust such as privacy or identity. However, we found a more recent work where Neisse et al. [81] fill this gap considering some domains in addition to the context. However, as we mentioned before, we believe that also the consideration of the SDLC could have improved the effectiveness of these works.

Finally, an important aspect that is not always directly considered in IoT frameworks is delegation. Lin et al. [82] define precisely trustor and trustee actors and in order to decide if a trustor-trustee interaction can be fulfiled, they analyse the trustworthiness of the trustee and the history among them. Thus, if the trustor trusts the trustee, the former can delegate the latter in order to perform a particular activity. However, the interactions are performed only in a SIoT environment.

Summarizing, in most frameworks, SDLC is not considered. Only several authors mentioned it [3, 6, 75]. We believe that this is a strong limitation. In fact, in order to properly consider trust in the IoT, it is better to implement it since the first phases. Moreover, trust is strongly related to other domains such as privacy and security. Only some papers consider them [3, 6, 68, 69, 77]. This is a weakness, because a holistic consideration of these domains increases trust in a virtuous circle increasing each of the domains considered. Then, six papers avoid to propose a specific model [66, 67, 71–73, 75].

To conclude, we believe that in order to consider holistically trust in an environment such as the IoT, we have to consider related properties, the context and we have to carefully planning it through a complete SDLC. We have analysed a lack of this aspect in the literature and we want to encourage its utilization in the future works related to this field. Moreover, we believe that considering the strong points presented in this survey, it will be possible to create a complete framework that can be helpful for the development of IoT devices. We will now present possible lines of research that we believe must be tackled by the research community in order to effectvely consider trust in the IoT.

7 Challenges and open issues

In this paper, we have collected and analysed different works and we have proposed an approach that should be taken into account to include trust in an IoT entity. However, IoT and trust cover different aspects and there are open research issues about this two topics that need to be tackled by the researcher communities. We list next those that we believe could be interesting to solve and be tackled in the future:

Integration of security, trust and reputation requirements and model methodologies

Methodologies for security requirements elicitation (i.e. TROPOS, Secure TROPOS, I*, TrUStAPIS [84, 110–112]) can be merged in order to provide developers with a complete tool for requirements elicitation leading to well-established best practices. This consideration can also be useful for the modelling phase, where our model-driven approach [113] and other existing methodologies such as UMLTrust [114], or SecureUML [115] can be analysed together to explore different methodologies that can be helpful in the SDLC of any system. Investigating a way to integrate these methodologies for including security, trust, and reputation can lead to an excellent benefit for SDLC and developers.

Configuration and visual support for trust and reputation implementation

Several works have proposed supports for developers or stakeholders to visualize data related to the development of trust in the IoT [84, 116]. Anyhow, extra steps in this direction can boost productivity by focusing on the core functionalities of a trusted IoT entity. It can also be a way to provide developers with tools that will help them writing code to create libraries or frameworks into a well-known practice to be implemented during the development phase. This could be more effective if the frameworks were also integrated into other phases of the SDLC to enable an automatic verification of the entities under development.

Creation of a standard trust model for the IoT

With part of our research [117], we have analysed the trust models of three different manufacturers (Google, Amazon, Philips), finding that their trust models are very different among them. For this reason, we believe that according to the future work that we have mentioned earlier, it is essential that in the near future a standard trust model will be created to be implemented for IoT entities in order to improve trust and security aspects. In fact, differences among IoT entities will lead to difficulty in implementing both trust and security among IoT entities and users. If a standard protocol is taken into consideration and developed, it will increase trust in IoT devices and their users [43].

Trust and Social Internet of Things

Social Internet of Things (SIoT) is a new concept binding the IoT entities and their users with the IoT entities and users of their friends, family members, or colleagues. This is an emerging field tackled by several authors [83, 89, 94, 118, 119], and the SIoT concept must be further clarified and explored. Moreover, this line of research can be merged with the previous one because SIoT can be considered as two dimensional, where also the relationships among users

are important and must be considered in a trust model. Typically, in IoT paradigms, this dimension is not considered. However, in a strongly connected world where users have many relationships among them, this parameter can be helpful for developing trust models that take these connections under consideration. Besides, exploring where and how the SIoT can be applied both in the professional and consumers IoT is needed. In fact, SIoT can also be helpful in business IoT (i.e. industrial IoT [120]), specifying the interaction of IoT entities and users according to their duties. Moreover, it is also considered together with Machine Learning [121, 122].

Machine Learning for Trust Computation

Machine learning offers a promising avenue to address the inherent uncertainty associated with trust metrics in various domains, such as online recommendations and social networks. Trust is a complex, multifaceted concept influenced by dynamic and context-dependent factors. Machine learning algorithms can help analysing vast datasets and identifying hidden patterns, enabling more accurate and adaptive trust predictions. These algorithms can learn from historical interactions, user behaviour and context information to build more sophisticated trust models. Additionally, machine learning can aid in the detection of trust violations, potentially mitigating risks associated with misleading or malicious actors. By continually refining and adapting trust metrics based on real-time data, machine learning provides a valuable tool for enhancing trust assessment and management in an increasingly interconnected digital world [121, 122].

Trust ontology in the IoT

A trust ontology in the IoT is a structured and semantically defined framework that captures and represents the complex and multifaceted concept of trust within the IoT ecosystem [123]. An ontology provides a systematic way to model and analyse trust relationships, trustworthiness attributes and the factors that influence trust in IoT devices. Thus, by using ontologies, IoT systems can achieve a shared understanding of trust-related concepts and facilitate communication and decision-making processes among various entities. Trust ontologies help in standardizing the representation of trust data, making it easier to exchange and integrate information about the trustworthiness of IoT entities. They can serve as an important tool for developing context-aware and adaptive trust management systems that enhance the security, reliability, and transparency of IoT environments.

Green IoT and Trust

Another important topic that must be tackled by the research community is related to the energy efficiency consumption of the IoT devices. The growing numbers of devices will become an energy consumption issue. Thus, it will be fundamental to guarantee trust considering also the energy aspect. Several authors [108, 124–126] have already started investigating this field, but the research community should consider it in the near future, in order to provide a sustainable IoT environment for the planet. The green IoT can bring important changes in the world helping reducing the greenhouse effect enabling a sustainable world.

8 Conclusion

In this paper, we have delved into how trust and IoT have been presented in the state of the art by different authors. Even if research on the fields of trust and IoT have been conducted, it is necessary to improve this effort. We have analysed works where trust and IoT have been considered together focusing on frameworks for trust and IoT. Analysing them, we have classified several parameters that we believe are fundamentals such as SDLC, domains connected to trust and different characteristics of trust. Thus, we have collected the identified works highlighting which parameters are considered and which ones are missing in order to provide a novel guide to properly consider trust in the IoT. Finally, we have provided a set of challenges and open issues that in our opinion should be tackled by the research community.

For future work, we will follow the guidelines proposed in this survey in order to provide a whole trust management framework. Moreover, we will contribute on the challenges proposed at the end of the paper. In fact, we think that these issues must be tackled and solved in order to improve the IoT environment.

Acknowledgements This work has been partially supported by the projects: BIGPrivDATA (UMA20-FEDERJA-082) from the FEDER Andaluc'ıa 2014-2020 Program. Moreover, we thank Huawei Technologies for their support.

Author Contributions The authors contributed equally to this work.

Funding Funding for open access publishing: Universidad Málaga/CBUA.

Availability of data and materials Not applicable.

Declarations

Conflict of interest Not applicable.

Ethical approval Not applicable.

References

1. Roman R, Najera P, Lopez J (2011) Securing the internet of things. Computer 44(9):51–58
2. Čolaković A, Hadžialić M (2018) Internet of things (IoT): a review of enabling technologies, challenges, and open research issues. Comput Netw 144:17–39

3. Fernandez-Gago C, Moyano F, Lopez J (2017) Modelling trust dynamics in the internet of things. Inf Sci 396:72–82
4. Hoffman LJ, Lawson-Jenkins K, Blum J (2006) Trust beyond security: an expanded trust model. Commun ACM 49(7):94–101
5. Pavlidis M, Designing for trust (2011) CAiSE (Doctoral Consortium), pp 3–14
6. Ferraris D, Fernandez-Gago C, Lopez J (2018) A trust-by-design framework for the internet of things. In: NTMS'2018-security track (NTMS 2018 security track), pp 1–4
7. Mohammadi V, Rahmani AM, Darwesh AM, Sahafi A (2019) Trust-based recommendation systems in internet of things: a systematic literature review. HCIS 9(1):1–61
8. Levien RL (2002) Attack resistant trust metrics. Ph.d. thesis, University of California at Berkeley
9. Grandison T, Sloman M (2000) A survey of trust in internet applications. IEEE Commun Surv Tutor 3(4):2–16
10. Aaqib M, Ali A, Chen L, Nibouche O (2023) Iot trust and reputation: a survey and taxonomy. J Cloud Comput 12(1):1–20
11. Altaf A, Abbas H, Iqbal F, Derhab A (2019) Trust models of internet of smart things: a survey, open issues, and future directions. J Netw Comput Appl 137:93–111
12. Fotia L, Delicato F, Fortino G (2023) Trust in edge-based internet of things architectures: state of the art and research challenges. ACM Comput Surv 55(9):1–34
13. Guo J, Chen R, Tsai J (2017) A survey of trust computation models for service management in internet of things systems. Comput Commun 97:1–14
14. Marsh SP (1994) Formalising trust as a computational concept. Ph.d. thesis, Department of Computing Science and Mathematics, University of Stirling
15. Yan Z, Holtmanns S (2008) Trust modeling and management: from social trust to digital trust. IGI Glob 290–323
16. Erickson J, (2009) Trust metrics. In: Collaborative technologies and systems, CTS'09, international symposium, pp 93–97
17. McKnight DH, Chervany NL (2000) What is trust? A conceptual analysis and an interdisciplinary model. In: AMCIS 2000 proceedings, vol 382, pp 827–833
18. Mayer Roger C., Davis James H., Schoorman F. David (1995) An integrative model of organizational trust. Acad Manag Rev 20(3):709. https://doi.org/10.2307/258792
19. McKnight DH, Chervany NL (1996) The meanings of trust, Technical Report MISRC Working Paper Series 96-04
20. Gambetta D (2000) Can we trust trust. In: Trust making and breaking cooperative relations, vol 13, pp 213–237
21. Mui L, Mohtashemi M, Halberstadt A (2002) A computational model of trust and reputation. In: Proceedings of the 35th Annual Hawaii International Conference on System Sciences, 2002. HICSS. IEEE, pp 2431–2439
22. Ruohomaa S, Kutvonen L (2005) Trust management survey. In: International Conference on Trust Management. Springer, pp 77–92
23. Jøsang A, Ismail R, Boyd C (2007) A survey of trust and reputation systems for online service provision. Decis Support Syst 43(2):618–644
24. Agudo I, Fernandez-Gago C, Lopez J (2008) A model for trust metrics analysis. In: International Conference on Trust, Privacy and Security in Digital Business. Springer, pp 28–37
25. Olmedilla D, Rana O F, Matthews B, Nejdl W (2006) Security and trust issues in semantic grids. In: Dagstuhl Seminar Proceedings, Schloss Dagstuhl–Leibniz–Zentrum für Informatik, pp 1–11
26. Moyano F, Fernandez-Gago C, Lopez J (2012) A conceptual framework for trust models. In: 9th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2012, vol 7449 of Lectures Notes in Computer Science. Springer, pp 93–104
27. Cofta P (2007) Confidence, trust and identity. BT Technol J 25(2):173–178
28. Cofta P (2007) Trust, complexity and control: confidence in a convergent world. Wiley, New York
29. Miller KW, Voas J (2009) The metaphysics of software trust. IT Prof 11(2):52–55
30. Marsh S, Dibben M R (2005) Trust, untrust, distrust and mistrust-an exploration of the dark(er) side. In: International Conference on Trust Management. Springer, pp 17–33
31. Ruan Y, Durresi A (2016) A survey of trust management systems for online social communities-trust modeling, trust inference and attacks. Knowl Based Syst 106:150–163
32. Louta M, Michalas A (2010) Towards efficient trust aware e-marketplace frameworks. In: Encyclopedia of E-business development and management in the global economy, pp 273–283

33. Blaze M, Feigenbaum J, Lacy J (1996) Decentralized trust management. In: IEEE Symposium Security and Privacy Proceedings, pp 164–173
34. Beth T, Borcherding M, Klein B (1994) Valuation of trust in open networks. In: European Symposium on Research in Computer Security. Springer, pp 1–18
35. Winslett M, Yu T, Seamons KE, Hess A, Jacobson J, Jarvis R, Smith B, Yu L (2002) Negotiating trust in the web. IEEE Internet Comput 6(6):30–37
36. Watson DS, Piette MA, Sezgen O, Motegi N, Ten Hope L (2004) Machine to machine (m2m) technology in demand responsive commercial buildings
37. Gazis V (2016) A Survey of Standards for Machine-to-Machine and the Internet of Things. IEEE Commun Surv Tutor 19(1):482–511
38. Pei Z, Deng Z, Yang B, Cheng X (2008) Application-oriented wireless sensor network communication protocols and hardware platforms: a survey, Industrial Technology. In: IEEE International Conference, pp 1–6
39. Gill K, Yang SH, Yao F, Lu X (2009) A zigbee-based home automation system, IEEE, Transactions on consumer. Electronics 55(2):422–430
40. Bronzi W, Frank R, Castignani G, Engel T (2026) Bluetooth low energy performance and robustness analysis for inter-vehicular communications. Ad Hoc Netw 37:76–86
41. Ferraris D, Fernandez-Gago C, Daniel J, Lopez J (2019) A segregated architecture for a trust-based network of internet of things. In: 16th IEEE Annual Consumer Communications and Networking Conference (CCNC), pp 1–6
42. Singh S, Sharma PK, Park JH (2017) Sh-secnet: an enhanced secure network architecture for the diagnosis of security threats in a smart home. Sustainability 9(4):1–19
43. Roman R, Zhou J, Lopez J (2013) On the features and challenges of security and privacy in distributed internet of things. Comput Netw 57(10):2266–2279
44. Dohr A, Modre-Opsrian R, Drobics M, Hayn D, Schreier G (2010) The internet of things for ambient assisted living. In: 2010 Seventh International Conference Information Technology: New Generations (ITNG), pp 804–809
45. Parra J, Hossain MA, Uribarren A, Jacob E, El Saddik A (2009) Flexible smart home architecture using device profile for web services: a peer-to-peer approach. Int J Smart Home 3(2):39–56
46. BlR Stojkoska, Trivodaliev KV (2017) A review of internet of things for smart home: challenges and solutions. J Clean Prod 140:1454–1464
47. Stouffer K, Falco J, Scarfone K (2011) Guide to industrial control systems (ics) security. NIST Spec Publ 800(82)
48. Porambage P, Ylianttila M, Schmitt C, Kumar P, Gurtov A, Vasilakos AV (2016) The quest for privacy in the internet of things. IEEE Cloud Comput 3(2):36–45
49. Leister W, Schulz T (2012) Ideas for a trust indicator in the internet of things. SMART 12:31–34
50. Azzedin F, Ghaleb M (2019) Internet-of-things and information fusion: trust perspective survey. Sensors 19(8):1929
51. Elkhodr M, Alsinglawi B (2019) Data provenance and trust establishment in the internet of things. Secur Privacy e99
52. Yan Z, Zhang P, Vasilakos AV (2014) A survey on trust management for internet of things. J Netw Comput Appl 42:120–134
53. Masthoff J (2007) Computationally modelling trust: an exploration. In: Proceedings of the SociUM Workshop Associated with the User Modeling Conference, pp 1–10
54. Wang EK, Chen C-M, Zhao D, Ip WH, Yung KL (2019) A dynamic trust model in internet of things. Soft Comput 1–10
55. Hussain Y, Zhiqiu H, Akbar MA, Alsanad A, Alsanad AA-A, Nawaz A, Khan IA, Khan ZU (2020) Context-aware trust and reputation model for fog-based iot. IEEE Access 8:31622–31632
56. Ursino D, Virgili L (2020) An approach to evaluate trust and reputation of things in a multi-iots scenario. Computing 102(10):2257–2298
57. Li N, Varadharajan V, Nepal S (2019) Context-aware trust management system for iot applications with multiple domains. In: IEEE 39th International Conference on Distributed Computing Systems (ICDCS), pp 1138–1148
58. Fortino G, Fotia L, Messina F, Rosaci D, Sarné GM (2019) A reputation mechanism to support cooperation of iot devices, AI & IoT jointly held with AI* IA 2019. In: The 18th International Conference of the Italian Association for Artificial Intelligence, CEUR, pp 1–12
59. Fortino G, Fotia L, Messina F, Rosaci D, Sarné GM (2020) Trust and reputation in the internet of things: state-of-the-art and research challenges. IEEE Access 8:60117–60125

60. Sadique KM, Rahmani R, Johannesson P (2018) Trust in internet of things: an architecture for the future iot network. In: International Conference on Innovation in Engineering and Technology (ICIET), pp 1–5
61. Junejo AK, Komninos N, Sathiyanarayanan M, Chowdhry BS (2019) Trustee: a trust management system for fog-enabled cyber physical systems. IEEE Trans Emerg Top Comput 9(4):2030–2041
62. Alemneh E, Senouci SM, Brunet P, Tegegne T (2020) A two-way trust management system for fog computing. Futur Gener Comput Syst 106:206–220
63. Køien GM (2011) Reflections on trust in devices: an informal survey of human trust in an internet-of-things context. Wirel Pers Commun 61(3):495–510
64. Abualese H, Al-Rousan T, Al-Shargabi B (2019) A new trust framework for e-government in cloud of things. Int J Electron Telecommun 65
65. Fortino G, Messina F, Rosaci D, Sarné GM (2018) Using trust and local reputation for group formation in the cloud of things. Futur Gener Comput Syst 89:804–815
66. Ali BA, Abdulsalam HM, AlGhemlas A (2018) Trust based scheme for iot enabled wireless sensor networks. Wireless Pers Commun 99(2):1061–1080
67. Mendoza CV, Kleinschmidt JH (2018) A distributed trust management mechanism for the internet of things using a multi-service approach. Wirel Person Commun 103(3):2501–2513
68. Pal S, Hitchens M, Varadharajan V (2019) Towards the design of a trust management framework for the internet of things. In: 13th International Conference on Sensing Technology (ICST), pp 1–7
69. Bernabe JB, JlH Ramos, Gomez AFS (2016) Taciot: multidimensional trust-aware access control system for the internet of things. Soft Comput 20(5):1763–1779
70. Mahalle PN, Thakre PA, Prasad NR, Prasad R (2013) A fuzzy approach to trust based access control in internet of things. In: Wireless VITAE IEEE, pp 1–5
71. Bica I, Chifor BC, Arseni SC, Matei I (2019) Reputation-based security framework for internet of things. In: International Conference on Information Technology and Communications Security. Springer, pp 213–226
72. De Meo P, Messina F, Postorino M N, Rosaci D, Sarné G M (2017) A reputation framework to share resources into iot-based environments. In: 2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC), pp 513–518
73. Ruan Y, Durresi A, Alfantoukh L (2016) Trust management framework for internet of things. In: IEEE International Conference Advanced Information Networking and Applications (AINA), pp 1013–1019
74. Hand DJ (1996) Statistics and the theory of measurement. J Roy Stat Soc Ser A (Stat Soc) 445–492
75. Sharma A, Pilli ES, Mazumdar AP, Govil M (2016) A framework to manage trust in internet of things. In: International Conference Emerging Trends in Communication Technologies (ETCT). IEEE, pp 1–5
76. Bahutair M, Bougeuttaya A, Neiat AG (2019) Adaptive trust: usage-based trust in crowdsourced iot services. In: IEEE International Conference on Web Services (ICWS), pp 172–179
77. Battah AA, Iraqi Y, Damiani E (2022) A trust and reputation system for iot service interactions. IEEE Trans Netw Serv Manage 19(3):2987–3005
78. Dwarakanath R, Koldehofe B, Bharadwaj Y, Nguyen TAB, Eyers D, Steinmetz R (2017) Trustcep: adopting a trust-based approach for distributed complex event processing. In: 18th IEEE International Conference on Mobile Data Management (MDM), pp 30–39
79. Wang Y, Chen R, Cho JH, Swami A, Lu YC, Lu C-T, Tsai JJ (2016) Catrust: context-aware trust management for service-oriented ad hoc networks. IEEE Trans Serv Comput 11(6):908–921
80. Saied YB, Olivereau A, Zeghlache D, Laurent M (2013) Trust management system design for the internet of things: a context-aware and multi-service approach. Comput Secur 39:351–365
81. Neisse R, Steri G, Baldini G, Tragos E, Fovino IN, Botterman M (2022) Dynamic context-aware scalable and trust-based iot security, privacy framework. In: Internet of things applications-from research and innovation to market deployment. River Publishers, pp 199–224
82. Lin Z, Dong L (2017) Clarifying trust in social internet of things. IEEE Trans Knowl Data Eng 30(2):234–248
83. Magdich R, Jemal H, Ayed MB (2022) A resilient trust management framework towards trust related attacks in the social internet of things. Comput Commun 191:92–107
84. Ferraris D, Fernandez-Gago C (2020) Trustapis: a trust requirements elicitation method for iot. Int J Inf Secur 19(1):111–127

85. Ferraris D, Fernandez-Gago C, Lopez J (2022) Novel approaches for the development of trusted IoT entities. In: IFIP International Conference on ICT Systems Security and Privacy Protection, pp 215–230
86. Ferraris D, Fernandez-Gago C, Lopez J (2022) Verification and Validation Methods for a trust-by-design framework for the IoT. In: IFIP Annual Conference on Data and Applications Security and Privacy, pp 183–194
87. Nguyen J, Dupuis M (2019) Closing the feedback loop between UX design, software development, security engineering, and operations. In: Proceedings of the 20th Annual SIG Conference on Information Technology Education, pp 93–98
88. Chen L (2015) Continuous delivery: huge benefits, but challenges too. IEEE Softw 32(2):50–54
89. Abdelghani W, Zayani C A, Amous I, Sèdes F (2016) Trust management in social internet of things: a survey. In: Conference on e-Business, e-Services and e-Society. Springer, pp 430–441
90. Christianson B, Harbison WS (1996) Why isn't trust transitive? International workshop on security protocols. Springer, pp 171–176
91. Chang J, Wang H, Gang Y (2006) A dynamic trust metric for p2p systems. In: Fifth International Conference on Grid and Cooperative Computing Workshops. IEEE, pp 117–120
92. Kenning P (2008) The influence of general trust and specific trust on buying behaviour. Int J Retail Distrib Manag 36(6):461–476
93. Morrow Jr J, Hansen MH, Pearson AW (2004) The cognitive and affective antecedents of general trust within cooperative organizations. J Manag Issues 48–64
94. Nitti M, Girau R, Atzori L (2014) Trustworthiness management in the social internet of things. IEEE Trans Knowl Data Eng 26(5):1253–1266
95. Presti SL, Butler M, Leuschel M, Booth C (2007) Holistic trust design of e-services. In: Trust in e-services: technologies, practices and challenges. IGI Global, pp 113–139
96. Nuñez D et al. (2013) D: C-5.1 metrics for accountability. Project Deliverable D 35
97. Stapelberg RF (2009) Handbook of reliability, availability, maintainability and safety in engineering design. Springer, Berlin
98. Ferraris D, Fernandez-Gago C, Lopez J (2023) POM: a trust-based ahp-like methodology to solve conflict requirements for the IoT. In: Collaborative Approaches for Cyber Security in Cyber-Physical Systems, pp 145–170
99. Lăzăroiu G, Neguriţă O, Grecu I, Grecu G, Mitran PC (2020) Consumers' decision-making process on social commerce platforms: online trust, perceived risk, and purchase intentions. Front Psychol 11:890
100. Matzembacher DE, do Carmo Stangherlin I, Slongo LA, Cataldi R (2018) An integration of traceability elements and their impact in consumer's trust. Food Control 92:420–429
101. Steinauer DD, Wakid SA, Rasberry S (1997) Trust and traceability in electronic commerce. Stand View 5(3):118–124
102. Dimitrakos T, Dilshener T, Kravtsov A, La Marra A, Martinelli F, Rizos A, Rosetti A, Saracino A (2020) Trust aware continuous authorization for zero trust in consumer internet of things. In: IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp 1801–1812
103. Zheng D, Luo Q, Ritchie BW (2022) The role of trust in mitigating perceived threat, fear, and travel avoidance after a pandemic outbreak: a multigroup analysis. J Travel Res 61(3):581–596
104. Saaty TL (2008) Decision making with the analytic hierarchy process. Int J Serv Sci 1(1):83–98
105. Mahalle P, Babar S, Prasad N R, Prasad R (2010) Identity management framework towards internet of things (iot): roadmap and key challenges. In: International Conference on Network Security and Applications. Springer, pp 430–439
106. Miller KW, Voas J, Hurlburt GF (2012) Byod: security and privacy considerations. It Prof 14(5):53–55
107. Thapa SJ (2021) Understanding security risks and users perception towards adopting wearable. Internet Med Things
108. Khan ZA (2018) Using energy-efficient trust management to protect iot networks for smart cities. Sustain Cities Soc 40:1–15
109. Zhao S, Zhang Q, Hu G, Qin Y, Feng D (2014) Providing root of trust for ARM TrustZone using on-chip SRAM. In: Proceedings of the 4th International Workshop on Trustworthy Embedded Devices, pp 25–36
110. Bresciani P, Perini A, Giorgini P, Giunchiglia F, Mylopoulos J (2004) Tropos: an agent-oriented software development methodology. Auton Agent Multi-Agent Syst 8(3):203–236

111. Mouratidis H, Giorgini P (2007) Secure tropos: a security-oriented extension of the tropos methodology. Int J Software Eng Knowl Eng 17(02):285–309
112. Yu E, Liu L (2001) Modelling trust for system design using the i* strategic actors framework. In: Trust in cyber-societies. Springer, pp 175–194
113. Ferraris D, Fernandez-Gago C, Lopez J (2020) A model-driven approach to ensure trust in the iot. HCIS 10:1–33
114. Uddin MG, Zulkernine M (2008) Umltrust: towards developing trust-aware software. In: Proceedings of the 2008 ACM symposium on applied computing. ACM, pp 831–836
115. Lodderstedt T, Basin D, Doser J (2002) Secureuml: a uml-based modeling language for model-driven security. In: International Conference on the Unified Modeling Language. Springer, pp 426–441
116. Mavropoulos O, Mouratidis H, Fish A, Panaousis E, Kalloniatis C (2016) Apparatus: reasoning about security requirements in the internet of things. In: International Conference on Advanced Information Systems Engineering. Springer, pp 219–230
117. Ferraris D, Bastos D, Fernandez-Gago C, El-Moussa F (2020) A trust model for popular smart home devices. Int J Inf Secur 1–17
118. Atzori L, Iera A, Morabito G, Nitti M (2012) The social internet of things (siot)-when social networks meet the internet of things: concept, architecture and network characterization. Comput Netw 56(16):3594–3608
119. Sharma V, You I, Jayakody DNK, Atiquzzaman M (2019) Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things. Futur Gener Comput Syst 92:758–776
120. Wang J, Wang M, Zhang Z, Zhu H (2022) Toward a trust evaluation framework against malicious behaviors of industrial iot. IEEE Internet Things J 9(21):21260–21277
121. Ali-Eldin AM (2022) A hybrid trust computing approach for IoT using social similarity and machine learning. PLoS ONE 17(7):e0265658
122. Sagar S, Mahmood A, Sheng QZ, Zhang WE (2020) Trust computational heuristic for social internet of things: a machine learning-based approach. In: ICC 2020-2020 IEEE International Conference on Communications (ICC), pp 1–6
123. Kotis K, Katasonov A (2012) An ontology for the automated deployment of applications in heterogeneous IoT environments. Semant Web J (SWJ)
124. Sharma PK, Kumar N, Park JH (2020) Blockchain technology toward green iot: opportunities and challenges. IEEE Netw 34(4):263–269
125. Hellaoui H, Koudil M, Bouabdallah A (2020) Energy efficiency in security of 5g-based iot: an end-to-end adaptive approach. IEEE Internet Things J 7(7):6589–6602
126. Ilyas M, Ullah Z, Khan FA, Chaudary MH, Malik MSA, Zaheer Z, Durrani HUR (2020) Trust-based energy-efficient routing protocol for internet of things-based sensor networks. Int J Distrib Sensor Netw 16(10):1–20