SPECIAL SECTION ON SPECIAL SECTION: CLOUD - FOG - EDGE COMPUTING IN CYBER-PHYSICAL-SOCIAL SYSTEMS (CPSS)

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 24, 2020, accepted March 10, 2020, date of publication March 20, 2020, date of current version April 8, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2982318

Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges

GIANCARLO FORTINO[1], LIDIA FOTIA[2], FABRIZIO MESSINA[3], DOMENICO ROSACI[4], AND GIUSEPPE M. L. SARNÉ[2], (Member, IEEE)

[1]Department DIMES, University of Calabria, 87036 Rende, Italy
[2]Department DICEAM, Mediterranea University of Reggio Calabria, 89122 Reggio, Italy
[3]Department DMI, University of Catania, 95126 Catania, Italy
[4]Department DIIES, Mediterranea University of Reggio Calabria, 89122 Reggio, Italy

Corresponding author: Giancarlo Fortino (g.fortino@unical.it)

This work was supported by the NeCs Laboratory of the Mediterranea University of Reggio Calabria.

ABSTRACT This paper deals with the principal aspects emerging from the application of trust techniques to the IoT domains with respect to the particular viewpoint of an IoT environment. We consider intelligent agents technology to add social behavior to the community of the smart objects, and we analyze the fundamental role of the concepts of trust and reputation in this perspective. Also, we analyze the existing architectures for IoT and explain how to integrate IoT with fog/edge computing. Besides discussing the main proposals present in the literature, the key contribution of this paper consists of providing a comparative study of the main current architectures for modeling trust in IoT environments. In this setting, we propose a comparison based on the important characteristics of the IoT layer and the architecture type. Such an analysis allows us to highlight both advantages and limitations of each approach, and to discuss the emerging research challenges.

INDEX TERMS Internet of Things, multi-agent system, reputation, trust, edge/fog computing.

I. INTRODUCTION

In 1999, Kevin Ashton predicted the Internet of Things (IoT) age [8], as an era in which people and objects would be linked over the Internet. The most relevant aspect of IoT is that it achieves multi-dimensional and context-aware smart environments for every aspect of our life. From a general viewpoint, IoT can be assumed to form a global network infrastructure formed by smart objects which can be heterogeneous and provided of cooperating, sensing and reasoning capabilities. More in detail, in real time such smart objects can sense the environment where they are living and acting to modify it by using a wide range of different sensory, communication, networking, information technologies and social interactions. These smart objects can monitor and collect data about human life, and these data can be aggregated, fused, processed and analyzed in order to extract helpful information to allow omnipresent services. Recently, an overwhelming amount of IoT applications and services have been emerging into markets, e.g., supervision, health care, security, transport, and distant object monitor and control.

In this context, *Trust management* (TM) plays an important role for allowing reliable data mining and fusion, in order to provide qualified services with context-aware intelligence, and for enhancing user privacy and information security. It helps people to overcome perceptions of uncertainty and risk, and engages in user acceptance and consumption on IoT services and applications.

In this paper, we describe the principal aspects emerging from the application of trust techniques to IoT domains discussing in particular how the traditional trust concepts developed in the domains of the Information Systems and Multi-Agent Systems (that we will consider in Section II) can be adapted to the IoT. In particular, we will consider the particular viewpoint of an IoT that exploits the intelligent agents technology to add social behavior to the community of the smart objects and we will analyze the fundamental role of the concepts of trust and reputation in this perspective. Section V is entirely devoted to examine this aspect. Then, in Section III, we analyze the existing architectures for IoT, highlighting the problems of Three-Layer architecture that have been largely overcome by the SoA architecture. While in the Section IV, we explain how to integrate IoT with fog/edge computing. Also, in Section VI, we will discuss

The associate editor coordinating the review of this manuscript and approving it for publication was Francesco Piccialli.

the features of the main proposals present in the literature, categorized on the basis of the particular used approach (hierarchical model, reputation mechanisms, derived from social networking, fuzzy techniques, mechanisms based on nodes past behavior or on routing strategies) and we analyze the most relevant available solutions related to trust in IoT. Furthermore, the key contribution of this paper consists of providing a comparative study of the main architectures proposed in the literature for modeling trust in IoT environments. In this setting, we propose a comparison based on some important characteristics of the IoT layer and the architecture type. This analysis allows us to highlight both advantages and limitations of every approach, and to discuss the emerging research challenges. We present the results of this analysis in the final Section VII.

II. TRUST

Trust is a complex concept influenced by different measurable and non-measurable properties. It is linked to security because system security and user safety is necessary to obtain trust. On the other hand trust is more than security. It relates goodness, strength, reliability, availability, ability, or other characters of an entity. For this reasons, trust is more arduous to establish, ensure and maintain.

The term trust is being used in the literature with a variety of meanings. Among them, there are two widely accepted, common definitions of trust: reliability trust and decision trust. Reliability trust can be understood as the reliability of something or somebody, as confirmed by the definition of Gambetta [29]:

Definition 1 (Reliability Trust): Trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends.

However, trust can be more complex than Gambetta's definition indicates. Indeed, Falcone and Castelfranchi [25] admit that having high reliability in a person is not enough to start a situation of dependence on that person. In particular, they write: "For example, it is possible that the value of the damage per se (in case of failure) is too high to choose a given decision branch, and this independently either from the probability of the failure (even if it is very low) or from the possible payoff (even if it is very high). In other words, that danger might seem to the agent an intolerable risk." For this reason, the trust definition of McKnight and Chervany [52] is more accurate and general.

Definition 2 (Decision Trust): Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible.

This definition implies a certain risk attitude in the sense that the trusting party is willing to accept the situational risk. In the literature, there are a few computational trust models that explicitly take risk into account [30]. In [50], the author avoids expressing measures of trust directly, and instead develops a model around other elements such as transaction values and the transaction history of the trusted party. Instead [36] discerns reliability trust from decision trust, and develops a mathematical model for decision trust based on more finely grained primitives, such as agent reliability, utility values, and the risk attitude of the trusting agent.

A. TRUST MODEL CONCEPTS

By our studies we can observe that trust has been conceptualized in several ways. Indeed in the literature, there are many trust models [7], [20]–[22], [32], [60], [62]. Moreover, some of them address behavioral problems [18], [32], [41].

In the following of this section, we briefly discuss the main trust concepts: behavior trust, reputation, honesty, accuracy.

1) BEHAVIOR TRUST

Behavior trust is considered as a needful element in any Internet-based transaction. In open and dynamic environments, the devices come into contact with other unknown and possibly hostile devices. In the literature, there is a lot of confusion regarding the definition and management of the behavior trust [5], [20], [23], [32]. Thus we cite a common, accepted definition of behavior trust: *a device is trustworthy if there is a firm belief in the competence of the device to act as expected such that this firm belief is not a fixed value associated with the device but rather it is subject to the device's behavior and applies only within a specific context at a given time* [13].

2) REPUTATION

In a dynamic environment, devices are vulnerable to risks because of unknown, incomplete, or distorted information about each other. One way to solve this problem is to use the concept of reputation [24], [53]. When a device x wants to collaborate with another unknown device y, it can rely on other for information pertaining to y. The definition of reputation is contained in [13]: *The reputation of an entity is an expectation of its behavior based on other entities' observations or the collective information about the entity's past behavior within a specific context at a given time.*

Moreover, the reputation value depends on two factors: (i) the honesty of the information source and (ii) the accuracy of the information received.

3) HONESTY

When asking for information about a device, the reputation value could be compromised by devices that are not well-informed or that have a wrong perception. This happens because there are devices that have a malicious behavior and want to alter the reputation calculation. The definition of honesty is: *A recommender is said to be honest if the information, pertaining to a specific entity within a specific context at a given time, received from entity is the same information that entity believes in* [13].

Honesty is a critical factor in any trust model. It cannot be assumed that the devices are honest. For this reason, it is necessary to implement a mechanism to compute honesty and use this measure to weed out and prevent dishonest recommenders from influencing the recommendation network.

4) ACCURACY

The goal is to ensure that the received information pertaining to device y is reliable. The definition of accuracy is: *a recommender is said to be accurate, if the deviation between the information received from it pertaining to the trustworthiness of a given entity y in a specific context at a given time and the actual trustworthiness of y within the same context and time is within a precision threshold* [13].

III. IoT ARCHITECTURE

This section analyzes the existing architectures for IoT: (i) Three-Layer Architecture and (ii) SoA-Based Architecture.

A. THREE-LAYER ARCHITECTURE

The three-layer architecture represents a common basis architecture which is realized in many systems [72]. The generic IoT architecture is composed by three layers: 1) application layer, 2) network layer, and 3) perception layer.

1) PERCEPTION LAYER

This layer (also known as sensor layer) is located at the bottom of the architecture [10]. The perception layer cooperates with physical objects using smart devices (as RFID, sensors, etc.). The main goal is to interrelate objects in the IoT network, and to estimate, gather and process the state information of these objects through deployed smart devices. Finally, the processed information is transmitted to the upper level through layer interfaces.

2) NETWORK LAYER

The network layer is central in the IoT architecture: because it is located in the middle layer of architecture [40] and receives all the information released by perception layer; it establishes the path that the data must travel to the IoT hubs, devices, and applications through integrated networks.

3) APPLICATION LAYER

The application layer, also called the business layer, is located in the top of the architecture [3]. It receives the data from the network layer and exploits it to release the required services. This layer contains a number of applications with different requirements. For example, smart grid, smart transportation, smart cities, etc. [67].

In order to overcome the limits of the three-layer architecture, the recent literature has proposed the service-oriented architectures (SoAs), which represents a generic and flexible multilayer architecture for IoT.

B. SoA-BASED ARCHITECTURE

SoA is a component-based approach used to connect several functional units of an application through interfaces and protocols [9]. SoA represents a tool to design the workflow of coordinated services, and favors the reuse of software and hardware components.

Adopting the SoA approach in the IoT architecture will generate four layers: the perception layer, network layer, service layer, and application layer. In particular, the perception layer is the bottom layer of the architecture, and estimates, gathers and extracts the data of the devices [33]. The network layer defines routes and caters data transmission through integrated heterogeneous networks. The service layer is between network layer and application layer, produces services to the application layer, as service discovery, service composition, service management, and service interfaces [9]. The application layer supports several applications, like smart grid, smart cities, and so on.

IV. FOG/EDGE COMPUTING FOR IoT

Now, we present an approach on how to integrate IoT with fog/edge computing. First of all, we remark that the IoT devices produce more information that can be collected and processed through big data to turn it into something that is useful. Moreover, data coming from IoT applications are unstructured, and need further processing to deduce helpful information. The big data and IoT can operate well with each other. IoT will influence big data in data storage, data processing, and analytics. In particular, in IoT, continuous flows of data will influence the data storage capacity in various organizations. A solution is to displace the data into the cloud, but an organization must consider the nature of the IoT data to select a technology for performing big data processing and analytics. For example, NoSQL document databases may be appropriate because they supply high throughput and low latency.

In several IoT applications, the miriads of IoT devices are located in large geographical areas. The large amount of produced data must be stored, processed, and analyzed efficiently [26]. Unlike the cloud infrastructure can perform all the operations related to the data, fog/edge computing can support the entire process because fog resources are closer to the IoT devices [66].

A fog/edge computing node is any device with the ability of storage, computing, and network connectivity, as illustrated in the Figure 1. These devices are placed anywhere with a network connection, and gather the data of other devices affiliated with IoT applications. In this way, data with high priority can be processed at once by fog/edge computing nodes, as they are closer to the IoT devices that produce the data.

On the other hand, the fog/edge computing introduce new challenges in the IoT. For example, it is necessary to efficiently handle fog/edge computing infrastructure and assign the resources to IoT devices. Each fog/edge service node has limited computing and storage capability, therefore they must be optimally administrated and positioned for IoT devices to supply requested services efficiently. Another challenge is how to efficiently manage fog/edge computing resources. The allocation of the fog/edge nodes is a delicate and

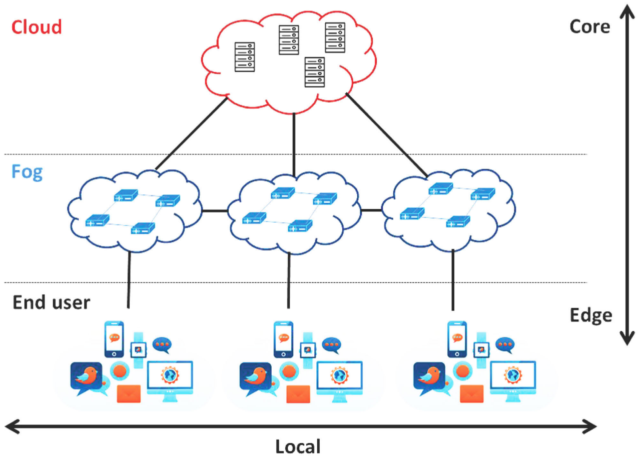

FIGURE 1. The Fog/Edge computing.

TABLE 1. Related works on trust assessment.

Used technique	Paper
Social networking	[11], [12], [29], [44]
Fuzzy technique	[22], [34], [35], [38], [54]
Cooperative approach	[33], [36], [46], [49]
Identity-based method	[32], [40]

complex phase because fog/edge nodes, such as service availability, energy consumption, and even revenue. Also, trust, security and privacy issues (authentication, access control, intrusion detection, trust management, etc.) in fog/edge computing infrastructures that integrate with IoT resent numerous challenges [17], [19], [28], [54], [59], [70].

V. TRUST IN IoT

The concept of trust is already present in different IoT contexts and with different meanings. As shown in previous section, it is an elaborate notion which currently has not been correctly contextualized in the scientific literature. The primary problem with most approaches towards trust definition is that they do not allow to fix metrics and evaluation methodologies. Also, in order to meet the trust requirements, it is necessary to manage identity and access control.

The proposals present in the literature are based on: hierarchical model, reputation mechanisms, approaches derived from social networking, fuzzy techniques, mechanisms based on nodes past behavior or on routing strategies. Our work analyzes the most relevant available solutions related to trust in IoT field. We summarize them in Table 1 and we present the related discussion later in this section.

A. SOCIAL NETWORKING

In [14] and [15], the authors analyze the impact of the trust of the individual IoT entities. The smart objects are human-carried or human-related devices, so they are located in public areas and communicate with each other via wireless channels, thus are subject to malicious attacks. Often smart objects are heterogeneous and must work together to complete a task. The social relationships are divided into three categories: friendship, ownership and community. In particular, the users are friends among them (i.e., friendship), users have the devices (i.e., ownership) and the devices are part of several communities (i.e., community).

Malicious nodes realize trust related attacks to interrupt the basic operation of IoT, as self-promoting, bad-mouthing and good-mouthing. In [14], the authors propose trust management protocol for IoT that is distributed, encounter-based, and activity-based. In particular, two nodes that interact with each other release a trust evaluation and exchange it with other nodes, so they calculate an indirect rate that seems a recommendation. The parameters used for the calculation of the trust are: honesty, cooperativeness, and community-interest. Therefore, this dynamic protocol is able to find the best parameter of trust even if the environments change dynamically, in order to maximize the performance of the application.

An analogue approach to evaluate the trust is presented in [56]. The authors propose the integration of social networking concepts into IoT, called Social Internet of Things (SIoT). In other words, the smart objects in IoT are able to institute social relationships in an autonomous way. Also, they introduce a reputation-based trust mechanism to limit the malicious behaviors aimed at misleading other nodes, In this way, only trusted nodes can use services and information delivery. A subjective model for the management of trustworthiness is defined, such as those introduced in [37], [42], [64], [74], [75]. Every node calculates the trust of the friends by using its experience and the opinion of the common friends. Therefore, a node selects the service provider with the highest trust level.

In the social network context, in [39] Lacuesta *et al.* introduce a secure distributed ad hoc network. It ensures a quick, easy and secure access to users to surf the Web because is based on direct peer-to-peer interactions and communities creation. In the network, every device and community have an identity and change the trust of other nodes by considering their behavior. Among the parameters to be taken into consideration are: physical proximity, fulfillment, consistency of answer, hierarchy on the trusted chain, similar properties, common goals and warrants, history of interaction, availability. Chains of confidence will allow the establishment of groups or communities and unique identities for the access to services as well as for the spreading of group information. Security is established when users access the network through the use of the trust chain generated by nodes, which he/she crosses.

B. FUZZY TECHNIQUE

In [49], the authors show that the traditional access control models are not appropriate in contexts where identities are not known in advance, as the decentralized and dynamic IoT scenarios. Indeed, the devices prefer to share services and resources only with those it trusts [14], [56]. Then the authors introduce a Fuzzy approach to the Trust Based Access Control (FTBAC). The trust is computed in

FTBAC by considering the following factors: experience, knowledge and recommendation. The trust values are then mapped to permissions, requests for access along with credentials establish a proof for consenting the access or not. FTBAC consists of three levels: Device Layer, Request Layer and Access Control Layer. The first layer comprise all IoT devices and our communications. The second layer collects experience, knowledge and recommendation information and computes fuzzy trust value. The third layer is involved in decision making process and associates the calculated fuzzy trust value with the access permissions, by following the principle of least privilege. The simulation results prove that FTBAC ensures flexibility and scalability and it is energy efficient. Indeed, managing access through a solution based on cryptographic protection enhances the trust level, but it produces extra overhead in terms of time and energy consumption.

Wang *et al.* [71] presents a fuzzy approach to calculate the trust. It is composed by three layers: sensor layer consisting of physical devices, core layer that includes access network and Internet, and application layer that comprises distributed networks, application systems and interfaces. For the users, IoT system is considered as a Service Provider and the trust management allows the IoT to provide more qualified services to any Service Requester. This trust model incorporates three passages: extraction, transmission, and decision-making. To carry out the layered trust mechanism, the authors utilize a fuzzy set theory and formal semantics-based language. Also, they define security policies based on a decision-making function according to user trust score. The user can enter to the IoT only if his/her credential satisfies these security policies. Noteworthy, this paper does not define a new trust model, but institutes an overall framework that includes the trust models already defined.

In [45], [46], the authors describe a trust model to preserve the user security by matching location-aware, identity-aware information and authentication history. When a user requires a service, he/she obtains a value of trust. There are three authentication approaches, one for each trust value (i.e, high, medium and low). In the case of low trust value, the users must provide biometric information. If the value trust is medium, they must use a PIN for login. Finally, in the case of high trust value, they do not use extra key because already signed on the VID. The target is to obtain a classification of the services through a fuzzy approach in order to appraise the sensitivity of the transmitted information.

For trust management, Gu *et al.* [31] propose a layered IoT architecture composed by three layers: sensor, core and application. In particular, a formal semantics-based and the fuzzy set theory are exploited to implement the trust mechanism. Each level has a different management of the trust to achieve the following objectives: self-organization, routing and multi-service. Each user (i.e., service request) collects the trust information and executes the final decision-making taking into account his policy requests.

C. COOPERATIVE APPROACH

Liu *et al.* [44] introduce a hierarchical trust model for IoT to detect malicious behavior of neighboring nodes. They propose a Verifiable Caching Interaction Digest (VCID) to monitor object-reader interaction. Also, the paper contains a long-term reputation mechanism to administrate the trust of organizations.

In [63], the authors define a decentralized approach to handle cooperation in a heterogeneous IoT architecture. In particular, they introduce a trust management system for IoT able to evaluate the trust of a node based on its past behavior. This model calculate trust value regarding both direct observations and indirect observation coming from the neighboring nodes. The trust management system consists of several phases: (*i*) collects the trust value of the nodes; (*ii*) establishes a collaborative service with the nodes; (*iii*) performs self-updates by retrieving information from past experiences; (*iv*) for each interaction during the learning phase, sets a recommendation score to each node.

In [58], Ping *et al.* define an attack-resistant trust management model for distributed routing in IoT. In distributed routing systems, this model calculates and propagates the reputation, allows to establish reliable trust relations between self-organized nodes and overcomes possible attacks. Reference [47], the authors propose a trust system based on node behavior detection. The recommended trust and history statistical trust are computed by evidence combination and Bayes algorithm.

D. IDENTITY-BASED METHOD

Liu *et al.* [43] use a Web Social Networks and determine a trust management for IoT based on an identity-based key agreement that happens through a distributed self-organizing key negotiation process. To improve security for the network lifetime, this protocol limits attacks from outside the network and identifies malicious nodes.

In [51], the authors introduce an identity-based network protocol to monitor the movements of the nodes from a host-to-host during the delivery processes. Also, it must divide the node identification from host addressing. The mutual authentication of nodes takes place through signature of the identity attributes, emitted by a trusted third party. Note that the identity information is disclosed only to the authorized subjects. Also, nodes and a Domain Trusted Entity constitute a globally trusted infrastructure by the pre-sharing of cryptographic certificates. The communications that take place between them are protected by cryptographic protocols and signature mechanisms.

Reference [68] highlights that existing trust and reputation approaches are inflexible because they not dynamically adapt themselves to the evolution of the environment. Therefore, they are not suitable for the heterogeneous and dynamic IoT context. For this reason, the authors define a flexible mechanism to identify the most appropriate trust and reputation model in heterogeneous environments.

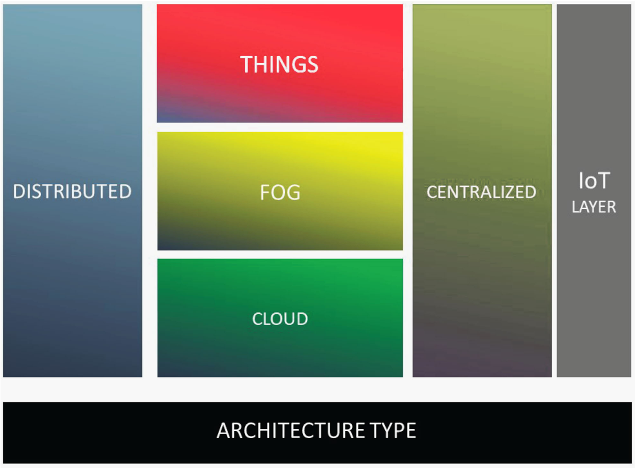

FIGURE 2. The architecture type.

TABLE 2. The IoT architectures.

Reference Paper	IoT Layer			Architecture Type	
	Thing	Fog	Cloud	Centralized	Distributed
Abderrahim et al. [2]			✓	✓	
Abderrahim et al. [1]	✓			✓	
Alqahtani et al. [3]			✓		✓
Alshehri et al. [5]	✓			✓	
Azad et al. [8]	✓				✓
Azad et al. [9]	n.a.	n.a.	n.a		✓
Bao et al. [11]	✓				✓
Bao et al. [13]	✓				✓
Chen et al. [14]	n.a.	n.a.	n.a.	✓	
Jayasinghe et al. [24]	✓			✓	
Kouicem et al. [28]		✓			✓
Mabodi et al. [37]	n.a.	n.a.	n.a		✓
Namal et al. [43]			✓	✓	
Saied et al. [49]			✓	✓	
Shayesteh et al. [51]	✓			✓	
Truong et al. [53]			✓	✓	
Xiao et al. [55]	✓			✓	

VI. IoT ARCHITECTURES FOR TRUST

In this section, we summarize the architectures proposed in the literature for modeling trust in IoT environments, as shown in Figure 2. The trust values are saved in the things, the fog, or the cloud. In particular, if the information is stored in the things, when the candidate is selected, the following factors must be taken into account: power and computation capabilities, thing availability, and link quality metrics. In Table 2, we show the two architectures used in the case just discussed: centralized and distributed. In particular, there are two architectures when the fog node is a directory: centralized or distributed. While, if the trust information is stored in the cloud, a fully centralized architecture is used.

A. CENTRALIZED ARCHITECTURES

Jayasinghe *et al.* [34] introduce a centralized architecture for trust evaluation in IoT. In this proposal, trust computing and prediction module work on the cloud. They use a publish-subscribe paradigm in which Service Providers (SPs) and Service Consumers (SCs) exchange information with the broker. In particular, SPs post the sensor data to the broker and SCs receive notifications regarding their interests from the broker. Abderrahim *et al.* [2] propose a centralized architecture for their trust model. Each IoT device must register with a centralized service server and itemize their services. After receiving the feedback from the devices, the server calculates and stores the reputation and contextual trust values. Also, these authors enhance the proposal in [34] introducing a clustered architecture to strengthen security and minimize the number of stored trust values on each object [1].

Truong *et al.* [69] describe a centralized architecture for trust management based on recommendation, reputation and knowledge trust metrics. Recommendation metric is considered as the opinion of trustor-related entities to trustee. Reputation metric is inserted to collect the global opinions on the trustee. The knowledge metric represents the information released by the trustee to ascertain its trustworthiness based on trust metrics (i.e., cooperativeness, honesty, experience, and community of interest). They propose a fog-based architecture to solve the scalability issue. In [63], the authors propose a centralized architecture where a trust entity stores the trust value of each IoT device and selects the best device to offer a request. Also, in [73], the authors introduce a centralized architecture to manage the trust. In particular, service and path discovery are stored in a centralized database server. There is also a central server that calculates, stores, and updates trust values of the IoT objects.

Chen *et al.* [18] propose a new IoT trust architecture that contains five layers: reputation management layer, organization layer, software defined network control layer, node layer, and object layer. Also in this case, the node and organization reputations are managed through a reputation management centralized repository. In [55], Namal *et al.* suggest a system of distributed trust agents to produce and filter trust parameters managed in a centralized manner. Also, in [6] a centralized trust management architecture is introduced where a supernode plays the role of centralized trust manager. In particular, the system is partitioned into clusters and the supernode uses a central repository to store the trust value of the smart objects. In [65], the authors propose a centralized scheme to estimate the entity trusts that offloads the overhead from the resource-constrained IoT devices to a central unit in the cloud, and avoids much of the communication overhead.

B. DISTRIBUTED ARCHITECTURES

In [11], the authors propose a distributed architecture for modelling trust. Each object releases services and feedback trust values. The reputation score for machines are calculated in a distributed manner. The encrypted feedback and the reported non-interactive zero-knowledge proof by interacting machines are stored in decentralized public bulletin board. Bao and Chen [14] model the trust through a distributed IoT architecture, where the trust management is executed on each smart object. Subsequently, they improve the architecture to minimize the computation and the storage cost: each object saves and updates only trust of the objects of its interest [16]. In order to allow IoT objects to save tamper-proof trust information, Kouicem *et al.* [38] use their blockchain-based architecture to model trust. The blockchain provides a

TABLE 3. Research challenge.

IoT Characteristic	Effect	Future changes
Resource limitation	Slow processing of information.	Provide security with a few resource consumption.
Mobility	Unstable link of communication.	Security solutions for application mobility requirements, and for interacting with components and systems that have different protocols, configurations and standards.
Heterogeneity of devices	No open standard for IoT.	Security solution (protocol, method) have to consider varying hardware specification. The developer must implement security based on their own standard.

tamper-proof data structure but it is not efficient compared to storage footprint and lookup time [27], [35], [57], [61], [76]. But in this case, each object creates unnecessary redundancy by storing the data of the whole system.

Mabodi *et al.* [48] introduce a multi-level trust-based intelligence schema using the cryptographic authentication to avoid gray hole attacks in IoT. In particular, the scheme checks the trust level for the nodes in the network, finds and eliminates the malicious gray hole nodes using control packets. Moreover, Azad *et al.* [12] present a framework for computing and updating the trustworthiness of participants in the network in a self-enforcing manner. The trust score of each device is automatically updated based on its previous trust score and the up-to-date tally of the votes by its peers in the network with zero-knowledge proofs to enforce that every participant follows the protocol honestly. Alqahtani *et al.* [4] design a trust-based monitoring scheme to improve the security features in cloud-assisted IoT environments. This scheme employs middleware and intelligent agents for managing user and communication-level security.

VII. CONCLUSION AND RESEARCH CHALLENGES

The goal of this section is to point out on the main limitations of the proposals analyzed in this work and to highlight the points to be strengthened in the near future. We summarize the main issues in Table 3, with particular reference to the emerging challenges.

First of all, centralized trust architectures for IoT have several problems: they introduce a single-point of failure and are unable to handle the dynamic nature of IoT systems. Furthermore, with this architecture bottlenecks are possible, as all devices must interact with a single centralized trust entity consuming energy and disrupting communication bandwidth.

Distributed trust architectures for IoT are divided in the following manner: thing-layer-based, fog-layer-based, or cloud-layer-based. For example, in [11], [14], [16] the authors propose trust model at the things layer which has limited computing and energy resources. Note that the things are unable to offer like trust computation, trust propagation, trust updates, and trust storage. In fact, only the architecture in [38] introduce the trust model in the fog layer. The use of the blockchain allows to store the trust values of the nodes and to ensure scalability mobility.

Another issue to consider is that trust model functionality is often implemented in the cloud, which introduces limitations very similar to centralized IoT architectures. Recall that our goal is to create safe and reliable smart environments, this becomes very complicated with things that have low power, memory, and processing data sources. In literature there are various trust models that cope with trust attacks but use high consumption of resources, therefore they are not compatible with IoT. A suitable solution is represented by the fog computing because it enables trust operations to be done directly at the network's edge. We discussed extensively on how integrate IoT with fog/edge computing and we have highlighted that there are several open problems. We observed that, in literature, the application of trust models is not adequately addressed, for this reason we discussed the integration of the edge/computing and the IOT.

We also discussed the important issues that are still open. In praticular, it is necessary to propose new IoT architectures for modeling trust. These architectures must be efficient, scalable, support mobility and taking into account the constrained capabilities of IoT devices. Hence, the distributed architectures at the fog layer need to be deepened to avoid the problems of bottleneck deriving from the cloud and the limited capabilities of the things. The fog layer enables trust computation, trust storage, and advertisement. So in order to fill this research gap, trust models with fog computing needs further investigation. In conclusion, the main goal of this survey is to supply a accurate understanding of IoT and its integration with fog/edge computing, an explanation of the concepts of trust and reputation and all the problems that derive from their application to the IoT context, the highlighting areas that remain unresolved, in an effort to advance the development of IoT.

REFERENCES

[1] O. Ben Abderrahim, M. H. Elhdhili, and L. Saidane, "TMCoI-SIOT: A trust management system based on communities of interest for the social Internet of Things," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 747–752.

[2] O. Ben Abderrahim, M. H. Elhedhili, and L. Saidane, "CTMS-SIOT: A context-based trust management system for the social Internet of Things," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 1903–1908.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[4] F. Alqahtani, Z. Al-Makhadmeh, A. Tolba, and O. Said, "TBM: A trust-based monitoring security scheme to improve the service authentication in the Internet of Things communications," *Comput. Commun.*, vol. 150, pp. 216–225, Jan. 2020.

[5] M. Alruwaythi and K. E. Nygard, "Fuzzy logic approach based on user behavior trust in cloud security," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT)*, May 2019, pp. 1–6.

[6] M. D. Alshehri and F. K. Hussain, "A centralized trust management mechanism for the Internet of Things (CTM-IOT)," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.* New York, NY, USA: Springer, 2017, pp. 533–543.

[7] A. Altaf, H. Abbas, F. Iqbal, and A. Derhab, "Trust models of Internet of smart Things: A survey, open issues, and future directions," *J. Netw. Comput. Appl.*, vol. 137, pp. 93–111, Jul. 2019.

[8] K. Ashton, "That'Internet of Things' thing," *RFID J.*, vol. 22, pp. 97–114, Jun. 2009.

[9] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[10] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social Internet of Things (SIoT)—When social networks meet the Internet of Things: Concept, architecture and network characterization," *Comput. Netw.*, vol. 56, no. 16, pp. 3594–3608, Nov. 2012.

[11] M. A. Azad, S. Bag, F. Hao, and K. Salah, "M2M-REP: Reputation system for machines in the Internet of Things," *Comput. Secur.*, vol. 79, pp. 1–16, Nov. 2018.

[12] M. A. Azad, S. Bag, F. Hao, and A. Shalaginov, "Decentralized self-enforcing trust management system for social Internet of Things," *IEEE Internet Things J.*, early access, Jan. 3, 2020, doi: 10.1109/JIOT.2019.2962282.

[13] F. Azzedin, "Taxonomy of reputation assessment in peer-to-peer systems and analysis of their data retrieval," *Knowl. Eng. Rev.*, vol. 29, no. 4, pp. 463–483, Sep. 2014.

[14] F. Bao and I.-R. Chen, "Dynamic trust management for Internet of Things applications," in *Proc. Int. Workshop Self-Aware Internet Things*, 2012, pp. 1–6.

[15] F. Bao and I.-R. Chen, "Trust management for the Internet of Things and its application to service composition," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2012, pp. 1–6.

[16] F. Bao, I.-R. Chen, and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems," in *Proc. IEEE 11th Int. Symp. Auto. Decentralized Syst. (ISADS)*, Mar. 2013, pp. 1–7.

[17] F. Chen, T. Xiang, X. Fu, and W. Yu, "User differentiated verifiable file search on the cloud," *IEEE Trans. Services Comput.*, vol. 11, no. 6, pp. 948–961, Nov. 2018.

[18] J. Chen, Z. Tian, X. Cui, L. Yin, and X. Wang, "Trust architecture and reputation evaluation for Internet of Things," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 8, pp. 3099–3107, Aug. 2019.

[19] Z. Chen, G. Xu, V. Mahalingam, L. Ge, J. Nguyen, W. Yu, and C. Lu, "A cloud computing based network monitoring and threat detection system for critical infrastructures," *Big Data Res.*, vol. 3, pp. 10–23, Apr. 2016.

[20] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562–583, 4th Quart., 2011.

[21] A. Comi, L. Fotia, F. Messina, G. Pappalardo, D. Rosaci, and G. M. L. Sarne, "Using semantic negotiation for ontology enrichment in e-Learning multi-agent systems," in *Proc. 9th Int. Conf. Complex, Intell., Softw. Intensive Syst.*, Jul. 2015, pp. 474–479.

[22] A. Comi, L. Fotia, F. Messina, G. Pappalardo, D. Rosaci, and G. M. L. Sarné, "Forming homogeneous classes for e-learning in a social network scenario," in *Intelligent Distributed Computing IX*. New York, NY, USA: Springer, 2016, pp. 131–141.

[23] A. Comi, L. Fotia, F. Messina, D. Rosaci, and G. M. L. Sarné, "Grouptrust: Finding trust-based group structures in social communities," in *Proc. Int. Symp. Intell. Distrib. Comput.* New York, NY, USA: Springer, 2016, pp. 143–152.

[24] P. De Meo, L. Fotia, F. Messina, D. Rosaci, and G. M. L. Sarné, "Providing recommendations in social networks by integrating local and global reputation," *Inf. Syst.*, vol. 78, pp. 58–67, Nov. 2018.

[25] R. Falcone and C. Castelfranchi, "Social trust: A cognitive approach," in *Trust Deception Virtual Societies*. New York, NY, USA: Springer, 2001, pp. 55–90.

[26] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarné, "Using blockchain for reputation-based cooperation in federated iot domains," in *Proc. Int. Symp. Intell. Distrib. Comput.* New York, NY, USA: Springer, 2019, pp. 3–12.

[27] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarne, "Using blockchain in a reputation-based model for grouping agents in the Internet of Things," *IEEE Trans. Eng. Manag.*, early access, Jun. 14, 2019, doi: 10.1109/TEM.2019.2918162.

[28] X. Fu, Z. Ling, W. Yu, and J. Luo, "Cyber crime scene investigations (C^{2}Si) through cloud computing," in *Proc. IEEE 30th Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2010, pp. 26–31.

[29] D. Gambetta, "Can we trust trust," *Trust, Making Breaking Cooperat. Relations*, vol. 13, pp. 213–237, Feb. 2000.

[30] T. Grandison and M. Sloman, "A survey of trust in Internet applications," *IEEE Commun. Surveys Tuts.*, vol. 3, no. 4, pp. 2–16, 4th Quart., 2000.

[31] L. Gu, J. Wang, and B. Sun, "Trust management mechanism for Internet of Things," *China Commun.*, vol. 11, no. 2, pp. 148–156, 2014.

[32] J. Guo, I.-R. Chen, and J. J. P. Tsai, "A survey of trust computation models for service management in Internet of Things systems," *Comput. Commun.*, vol. 97, pp. 1–14, Jan. 2017.

[33] E. Ilie-Zudor, Z. Kemény, F. van Blommestein, L. Monostori, and A. van der Meulen, "A survey of applications and requirements of unique identification systems and RFID techniques," *Comput. Ind.*, vol. 62, no. 3, pp. 227–252, Apr. 2011.

[34] U. Jayasinghe, A. Otebolaku, T.-W. Um, and G. M. Lee, "Data centric trust evaluation and prediction framework for IOT," in *Proc. ITU Kaleidoscope, Challenges for a Data-Driven Soc. (ITU K)*, Nov. 2017, pp. 1–7.

[35] K. Jong and A. De Haven Brandon, "An analysis of the behavior of a class of genetic adaptive systems," Ph.D. dissertation, Univ. Michigan, Ann Arbor, MI, USA, 1975.

[36] A. Jøsang and S. L. Presti, "Analysing the relationship between risk and trust," in *Proc. Int. Conf. Trust Manage.* New York, NY, USA: Springer, 2004, pp. 135–145.

[37] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in P2P networks," in *Proc. 12th Int. Conf. World Wide Web (WWW)*, 2003, pp. 640–651.

[38] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "An efficient architecture for trust management in ioe based systems of systems," in *Proc. 13th Annu. Conf. Syst. Syst. Eng. (SoSE)*, Jun. 2018, pp. 138–143.

[39] R. Lacuesta, G. Palacios-Navarro, C. Cetina, L. Peñalver, and J. Lloret, "Internet of Things: Where to be is to trust," *EURASIP J. Wireless Commun. Netw.*, vol. 2012, no. 1, p. 203, Dec. 2012.

[40] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in *Proc. Euro Med Telco Conf. (EMTC)*, Nov. 2014, pp. 1–5.

[41] C. Liang, F. Wen, and Z. Wang, "Trust-based distributed Kalman filtering for target tracking under malicious cyber attacks," *Inf. Fusion*, vol. 46, pp. 44–50, Mar. 2019.

[42] Z. Liang and W. Shi, "Enforcing cooperative resource sharing in untrusted P2P computing environments," *Mobile Netw. Appl.*, vol. 10, no. 6, pp. 971–983, Dec. 2005.

[43] T. Liu, Y. W. Guan, Y. Q. Yan, L. Liu, and Q. C. Deng, "A WSN-oriented key agreement protocol in Internet of Things," *Appl. Mech. Mater.*, vols. 401–403, pp. 1792–1795, Sep. 2013.

[44] W.-M. Liu, L.-H. Yin, B.-X. Fang, and H.-L. Zhang, "A hierarchical trust model for the Internet of Things," *Chin. J. Comput.*, vol. 35, no. 5, pp. 846–855, Nov. 2012.

[45] Y. Liu, Z. Chen, F. Xia, X. Lv, and F. Bu, "A trust model based on service classification in mobile services," in *Proc. IEEE/ACM Int. Conf. Green Comput. Commun. Int. Conf. Cyber, Phys. Social Comput.*, Dec. 2010, pp. 572–577.

[46] Y. Liu, Z. Chen, F. Xia, X. Lv, and F. Bu, "An integrated scheme based on service classification in pervasive mobile services," *Int. J. Commun. Syst.*, vol. 25, no. 9, pp. 1178–1188, Sep. 2012.

[47] Y. Liu, X. Gong, and Y. Feng, "Trust system based on node behavior detection in Internet of Things," *Tongxin Xuebao/J. Commun.*, vol. 35, pp. 8–15, Jun. 2014.

[48] K. Mabodi, M. Yusefi, S. Zandiyan, L. Irankhah, and R. Fotohi, "Multi-level trust-based intelligence schema for securing of Internet of Things (IoT) against security threats using cryptographic authentication," *J. Supercomput.*, vol. 156, pp. 1–25, Jan. 2020.

[49] P. N. Mahalle, P. A. Thakre, N. R. Prasad, and R. Prasad, "A fuzzy approach to trust based access control in Internet of Things," in *Proc. Wireless VITAE*, Jun. 2013, pp. 1–5.

[50] D. W. Manchala, "Trust metrics, models and protocols for electronic commerce transactions," in *Proc. 18th Int. Conf. Distrib. Comput. Syst.*, 1998, pp. 312–321.

[51] P. Martinez-Julia and A. F. Skarmeta, "Beyond the separation of identifier and locator: Building an identity-based overlay network architecture for the future Internet," *Comput. Netw.*, vol. 57, no. 10, pp. 2280–2300, Jul. 2013.

[52] D. H. McKnight and N. L. Chervany, "The meanings of trust," Carlson School Manage., Hubert H. Humphrey Center, Univ. Minnesota, Minneapolis, MN, USA, 1996.

[53] F. Messina, G. Pappalardo, A. Comi, L. Fotia, G. M. L. Sarné, and D. Rosaci, “Combining reputation and QoS measures to improve cloud service composition,” *Int. J. Grid Utility Comput.*, vol. 8, no. 2, pp. 142–151, 2017.

[54] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, “Security and privacy in fog computing: Challenges,” *IEEE Access*, vol. 5, pp. 19293–19304, 2017.

[55] S. Namal, H. Gamaarachchi, G. MyoungLee, and T.-W. Um, “Autonomic trust management in cloud-based and highly dynamic iot applications,” in *Proc. ITU Kaleidoscope, Trust Inf. Soc.*, Dec. 2015, pp. 1–8.

[56] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, “A subjective model for trustworthiness evaluation in the social Internet of Things,” in *Proc. IEEE 23rd Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2012, pp. 18–23.

[57] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, “Blockchain,” *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, 2017.

[58] P. Dong, J. Guan, X. Xue, and H. Wang, “Attack-resistant trust management model based on beta function for distributed routing in Internet of Things,” *China Commun.*, vol. 9, no. 4, pp. 89–98, 2012.

[59] I. Psaras, “Decentralised edge-computing and IoT through distributed trust,” in *Proc. 16th Annu. Int. Conf. Mobile Syst., Appl., Services*, Jun. 2018, pp. 505–507.

[60] M. Rashmi and C. V. Raj, “A review on trust models of social Internet of Things,” in *Emerging Research in Electronics, Computer Science and Technology* Springer, 2019, pp. 203–209.

[61] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT. Challenges and opportunities,” *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[62] D. Rosaci, G. M. L. Sarné, and S. Garruzzo, “Integrating trust measures in multiagent systems,” *Int. J. Intell. Syst.*, vol. 27, no. 1, pp. 1–15, Jan. 2012.

[63] Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent, “Trust management system design for the Internet of Things: A context-aware and multi-service approach,” *Comput. Secur.*, vol. 39, pp. 351–365, Nov. 2013.

[64] A. A. Selcuk, E. Uzun, and M. R. Pariente, “A reputation-based trust management system for P2P networks,” in *Proc. IEEE Int. Symp. Cluster Comput. Grid*, Apr. 2004, pp. 251–258.

[65] B. Shayesteh, V. Hakami, and A. Akbari, “A trust management scheme for IoT-enabled environmental health/accessibility monitoring services,” *Int. J. Inf. Secur.*, vol. 19, no. 1, pp. 93–110, Feb. 2020.

[66] I. Stojmenovic and S. Wen, “The fog computing paradigm: Scenarios and security issues,” in *Proc. Federated Conf. Comput. Sci. Inf. Syst.*, Sep. 2014, pp. 1–8.

[67] L. Tan and N. Wang, “Future Internet: The Internet of Things,” in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, vol. 5, Aug. 2010, pp. 376–380.

[68] G. Dólera Tormo, F. Gómez Mármol, and G. Martínez Pérez, “Dynamic and flexible selection of a reputation mechanism for heterogeneous environments,” *Future Gener. Comput. Syst.*, vol. 49, pp. 113–124, Aug. 2015.

[69] N. B. Truong, T.-W. Um, and G. M. Lee, “A reputation and knowledge based trust service platform for trustworthy social Internet of Things,” in *Proc. Innov. Clouds, Internet Netw. (ICIN)*, Mar. 2016, pp. 1–8.

[70] P. Varshney and Y. Simmhan, “Demystifying fog computing: Characterizing architectures, applications and abstractions,” in *Proc. IEEE 1st Int. Conf. Fog Edge Comput. (ICFEC)*, May 2017, pp. 115–124.

[71] J. P. Wang, S. Bin, Y. Yu, and X. X. Niu, “Distributed trust management mechanism for the Internet of Things,” *Appl. Mech. Mater.*, vols. 347–350, pp. 2463–2467, Aug. 2013.

[72] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, “Research on the architecture of Internet of Things,” in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, vol. 5, Aug. 2010, pp. 484–487.

[73] H. Xiao, N. Sidhu, and B. Christianson, “Guarantor and reputation based trust model for social Internet of Things,” in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2015, pp. 600–605.

[74] L. Xiong and L. Liu, “PeerTrust: Supporting reputation-based trust for Peer-to-Peer electronic communities,” *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 07, pp. 843–857, Jul. 2004.

[75] B. Yu, M. P. Singh, and K. Sycara, “Developing trust in large-scale peer-to-peer systems,” in *Proc. IEEE 1st Symp. Multi-Agent Secur. Survivability*, 2004, pp. 1–10.

[76] G. Zyskind, O. Nathan, and A. ’. Pentland, “Decentralizing privacy: Using blockchain to protect personal data,” in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 180–184.

GIANCARLO FORTINO received the Ph.D. degree in computer engineering from the University of Calabria (UniCal), Italy, in 2000. He is currently a Full Professor of computer engineering with the Department of Informatics, Modeling, Electronics, and Systems, UniCal. He is also an Adjunct Professor with the Wuhan University of Technology, Wuhan, China, and a Senior Research Fellow with the Italian National Research Council ICAR Institute. He is also the Co-Founder and the CEO of SenSysCal S.r.l., a Unical spinoff focused on the innovative Internet of Things (IoT) systems. He is the author of over 350 articles in international journals, conferences, and books. His research interests include agent-based computing, wireless (body) sensor networks, and the IoT. He is also a member of the IEEE SMCS BoG and the Chair of the IEEE SMCS Italian Chapter.

LIDIA FOTIA received the M.Sc. degree in telecommunication engineering and the Ph.D. degree in information engineering from the Mediterranea University of Reggio Calabria, in 2010 and 2014, respectively. She is currently a Postdoctoral Fellow with the Mediterranea University of Reggio Calabria. Her research interests include social networks and social internetworking analysis, privacy, security, trust, reputation, and intelligent agents.

FABRIZIO MESSINA received the Ph.D. degree in computer science from the Department of Mathematics and Informatics, University of Catania, Italy, in 2009. He is currently an Assistant Professor with the Department of Mathematics and Informatics. His research interests include distributed systems, complex networks, simulation systems, and trust.

DOMENICO ROSACI received the Ph.D. degree in electronic engineering, in 1999. He is currently an Associate Professor of computer science with the Department of Information, Infrastructures and Sustainable Energy Engineering, Mediterranea University of Reggio Calabria, Italy. His research interests include distributed artificial intelligence, multiagent systems, trust, and reputation in social communities. He is also a member of a number of conference PCs. He is also an Associate Editor of the *Journal of Universal Computer Science* (Springer).

GIUSEPPE M. L. SARNÉ (Member, IEEE) is currently an Assistant Professor of computer science with the Department of Civil, Energy, Environment and Materials Engineering, Mediterranea University of Reggio Calabria, Italy. His main research interests include distributed artificial intelligence, multi-agent systems, trust, and reputation systems. He is also a member of number of conference PCs. He is also an Associate Editor of *E-Commerce Research and Applications* (Elsevier) and *Big Data and Cognitive Computing* (MDPI).