Mohammadi *et al.*
Hum. Cent. Comput. Inf. Sci. (2019) 9:21
https://doi.org/10.1186/s13673-019-0183-8

Human-centric Computing and Information Sciences

RESEARCH Open Access

Trust-based recommendation systems in Internet of Things: a systematic literature review

Venus Mohammadi[1], Amir Masoud Rahmani[1*], Aso Mohammed Darwesh[2] and Amir Sahafi[3]

*Correspondence: rahmani74@yahoo.com
[1] Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran
Full list of author information is available at the end of the article

Abstract

Internet of Things (IoT) creates a world where smart objects and services interacting autonomously. Taking into account the dynamic-heterogeneous characteristic of interconnected devices in IoT, demand for a trust model to guarantee security, authentication, authorization, and confidentiality of connected things, regardless of their functionality, is imperative. However, as far as we know, against the centrality of trust-based recommendation mechanisms in the IoT environment, there is no ambient study for investigating its techniques. In this paper, we present a systematic literature review (SLR) of trust based IoT recommendation techniques so far. Detailed classifications based on extracted parameters as well as investigation existing techniques in three different IoT layers put forth. Moreover, the advantages, disadvantages and open issues of each approach are introduced that can expand more frontier in obtaining accurate IoT recommendation in the future.

Keywords: Internet of Things, IoT, Trust, Recommender system, Recommendation, Security, Systematic literature review

Introduction

During the past decades, in the era of wireless communications and embedded system, the concept of the Internet of Things (IoT) was first presented by Kevin Ashton in the year 1999 [1]. Along with the tremendous growth in the number of sensing devices connected to the Internet, we were a witness of emerging IoT into healthcare, transportation system, smart cities, agriculture, and other enterprises.

The IoT benefits cooperation of diverse computing systems such as sensors and smart devices to cloud computers. On the other side, the internet and mobile communication facilitate the spatiotemporal connection between distant people with common experience and values. More recently, technological evolution is introduced by intelligent sensor devices installed in the physical and virtual realm of IoT to act as or on behalf of human beings: the virtual robots [2]. This creates the possibility for physical objects present in a self-organized manner without a central administration and leads to meaningful human–machine interaction in IoT scenario [3].

As a matter of fact, practical deployment of IoT applications may raise challenges on establishing interoperability between autonomous devices. Despite the traditional assumption of a trustworthy operating environment [4], different sensors' manufacturers and service providers are susceptible to the selfish manner and performance degradation. Besides, due to low computational capabilities of sensor nodes and IoT decentralized infrastructure, cryptographic mechanisms are deficient in guaranteeing trustworthy, user/data security and resistance against adversaries. In this regard, we employ trustworthiness evaluation and a coherent recommendation to estimate friend nodes' reliability and isolate remain malicious nodes. Through attaining these perspectives, the network's security is achievable.

In the IoT network, each node is both a provider of information/services as well as a requester or a recommender. Upon query dissemination in the network, diversity of received information opens a challenge in deciding the most fitting one. Hence, recommender systems are tools that may better understand users' requirement and selects the most appropriate responder among all volunteer nodes to provide service [5]. In this context, each object keeps a transactional history and update interacted nodes' profile. Not only the direct observations of past participation but also the indirect recommendations are taken into account for trust derivation along with social relationships. Since the accuracy of trust computation relies on the number of received recommendations, nodes with higher trust value are more probable to be engaged in the next interaction. By terminating each transaction, objects rank each service and recommendation, respectively, and update their local records [6].

There are different types of recommender systems that vary in terms of prediction utility like addressed domain, knowledge used, location movements, users' preferences, items' properties, and users' ratings: First, the user-based collaborative filtering methods which refers as "people-to-people correlation" recommend items calculating the feedback (ratings) of users with similar tastes to the target user. Secondly, the content-based filtering approaches learn to recommend items analogous to the ones previously liked by the user. To find best-matching candidate features are compared with previously rated items. Thirdly, the location-based context-aware filtering uses the location of users to recommend items close to them [7]. There are other types, such as knowledge-based or community-based which due to less utilization or having common points are beyond scope of this study.

Bearing in mind, recommender system definition and current drawbacks such as cold-start problem and sparsity in the collaborative filtering (CF), bring up the need for human knowledge to classify items/users in the content-based filtering (CBF), and necessity for modeling the users' profile in the context-aware filtering (CAF) approaches [8]. Therefore, one of this paper's direction is to draw insight for tackling constraint in IoT environment such as the requirement for centralized authority and do the computation incompletely distributed environment and by the nodes themselves.

Moreover, despite cryptography ability to protect against external adversaries, internal adversaries of a benign node which turn malicious and disrupt transmission, cannot be tackled with traditional security mechanism. This deceptive behavior can only be detected by trust models that corporate with IoT devices to distinguish honest nodes. Trust—"reliance on the integrity, ability, or character of a person or thing"—is

an indispensable element in every social transaction. In a particular context, trust pertains as subjective anticipation or personal mindset of one entity by another which is not symmetric and will be built or evolve along with a particular time or context. From this origin, if trust is so pervasive and beneficial context, why not exploit this paradigm in the IoT environment [9].

In addition to hardware security alternatives for resisting against destructive attack, recently there are notable literatures which concerned trust management vital role for data fusion in IoT intelligent environment. However, due to the dynamic behaviors of sensor nodes and their resources limitation, establishing reliable end-to-end communication channel especially with external nodes, could be either unachievable or prohibitively costly. In order to envisaged current IoT security problems, we conduct a survey with a view to refine trust assessment method compared to previous stated ones. However, to the extent of our knowledge, no systematic, comprehensive survey and review in the field of trust-based recommendation mechanism in IoT environments exists, particularly schemes that conjointly took into account inherent IoT nodes' constraints and their vulnerability to malicious attacks [10]. This research reviews state-of-the-art "Internet of Things" studies through the literature analyzation, current trends identification, the description of the challenges and limitation to enhance trustworthy information retrieval by recommendation mechanism. By the end of compiling a comprehensive reference list, we finally depict open research questions and future directions relative to this subject to assist researchers. To achieve our objective, an SLR was taken based on the original guidelines as suggested by Kitchenham [11] with certain concertation on trust-related techniques in the IoT. This paper's contributions are as follows:

- Presenting an SLR in the trust model recommendation in IoT and paramount achievements in this field.
- Enumerate a summary of shortages and challenges related to trust evaluation and recommendation approaches in IoT.
- Explore significant methods of recommendation as well as trust management metric.
- Discuss important factors on the trustworthiness of recommendation in IoT and highlight open issues for later studies.

The rest of this paper is organized in the following manner: "Recommendation strategies" section depicts a sample scenario for a trustworthy recommendation in IoT and presents technical taxonomy in three different IoT layers. Besides in this section, we develop existing metrics and policies for organizing trust techniques in IoT environments and gives an explanation of mostly used dimensions in reviewed articles. "Conceptual methodology" section draws an article selection process based on the SLR method includes the process of question formalization, search query, sources arrangement based on inclusion/exclusion criteria as well as data extraction and quality analyzing. "Recommendation mechanisms based on IoT architecture" section overviews trust-based recommendation in the IoT environment systematically and classifies them on the basis of three IoT layers and summarize advantages and drawbacks of the approaches for selected articles while highlighting the effectiveness of each approach. "Discussion and statistics" section gives a discussion on explored articles and statistics and shows

the distribution of achievements during the investigation period. "Threats of validity" section insights threats invalidity and the paper limitations. "Open research issues and future direction" section illustrates open issues and suggests future research directions. "Summary and conclusion" section presents our final summary and conclusion.

Recommendation strategies

This section encompasses a technical review of recommendation strategies and trust computation standards in IoT for selected peer-reviewed articles according to the SLR method, additionally, categorize approaches into three main IoT layers and depict of taxonomy tree. Ultimately, we settle this section by common allocated simulation tools in applied articles.

IoT is a self-organized infrastructure of virtual "things" which seamlessly interact with their neighbor nodes in a dynamic manner. In a ubiquitous environment of IoT, there undoubtedly exist distinct entities offer analogous services anywhere anytime. A measure of reliability in data sources is extremely significant in boosting IoT security and privacy. In this respect, trust-based recommendation approach is adopted to discriminate users' information based on their trust ratio. Trust is a degree of belief to predict a node's future behaviors based on past competence and action observation within a certain context and time [12]. An intrinsic characteristic of a recommender system (RS) is priming as many recommenders as feasible to active user [13]. Hereupon the trustworthy performance of RS is measure in various aspect such as prediction accuracy and coverage, energy consumption, complexity, etc. where some mostly popular estimation metrics are enumerated in Table 1.

To the best of our knowledge, researches did not give any explanation on recommender techniques in IoT [14] and few of them fragmentary hint on trust-based sweeping entire network to provide a recommendation [15, 16]. Tan et al. [15] observed that trust collection should be implemented in the network layer. After analyzing routing in the network layer, we perceived three major trust factors that reflect the behavior of data transmission. The definition of utilized trust factors is given below:

Definition 1 Trust Proportion of successful packet transmission between nodes to all forwarded packets at a given timescale [17].

Definition 2 Communication trust if the interval between the source and the destination node is small, we rely on the direct packet transfer. In a case that number of packet interaction is not large enough to reflect trustworthiness between nodes, we have no choice to confide on common neighbors between source and destinations and infer based on their recommendation [18].

Definition 3 Energy trust this factor is estimated by the energy of forwarding nodes to receive or forward messages between source and destination nodes, whether directly or by means of intermediate nodes.

According to communication behavior of nodes in IoT, when the distance of two nodes is small enough, we should synthesize aforementioned three indicated factors in order to calculate comprehensive first-hand trust by including the trust history of the user profile and the predicted value. Then if the space among nodes is more than communication radius, we calculate the indirect trust, in lack of personal observation. In this regard, firstly we require to collect all recommenders from source to destination node. Secondly,

Table 1 Evaluation metrics in literatures

	Trust	Accuracy	QoS Interaction Availability Throughput Delay Reliability	Security AuthN- AuthZ- Confidentiality Integrity	Similarity Friendship Social contact Community of interest	Energy	Quality of recommend	Reputation	Social network
Chen et al. [94, 112, 115]	✓	✓	✓		✓				
Wang et al. [74, 97, 105]	✓	✓	✓				✓		
Fernandez-Gago et al. [123]	✓			✓					
Khan et al. (2016)	✓			✓				✓	
Nitti et al. [35]	✓		✓				✓		✓
Chen et al. [94, 112, 115]	✓				✓		✓		
Kang et al. [34]				✓	✓				
Bernabe et al. [28]			✓	✓					
Sfar et al. [81]	✓		✓	✓					
Sicari et al. [32]	✓			✓					
Atzori et al. [49]					✓				✓
Al-Turjman [33]	✓		✓			✓			
Guo et al. [109]	✓						✓		
Chen et al. [94, 112, 115]		✓	✓		✓	✓		✓	
Saied et al. [111]		✓					✓	✓	
Tormo et al. [129]		✓				✓		✓	
Ali et al. [131] Nieto and Lopez [56]	✓		✓	✓					
Kowshalya and Valarmathi [21]	✓				✓	✓			
Yu et al. [90]			✓	✓					
Margaris and Vassilakis [30]			✓		✓		✓		✓
Pinto et al. [53]			✓	✓					
Garc´ıa-de-Prado et al. [78]			✓						
Køien [67]				✓					
Roman et al. [83]	✓		✓	✓					
Cao et al. [54]	✓		✓						

Table 1 (continued)

	Trust	Accuracy	QoS Interaction Availability Throughput Delay Reliability	Security AuthN- AuthZ- Confidentiality Integrity	Similarity Friendship Social contact Community of interest	Energy	Quality of recommend	Reputation	Social network
Sicari et al. [86]		✓		✓					
Asiri and Miri [22]	✓								
Wang et al. [74, 97, 105]	✓	✓							
Mashal et al. [114]		✓							
Mashal et al. [113]		✓							
Dwarakanath et al. [95]	✓					✓			
Nguyen et al. [130]	✓								
Ali et al. [131]		✓							
Litescu et al. [60]		✓	✓						
Hellaoui et al. [87]									✓
Ko et al. [29]		✓							
Mahalle et al. [84]									
Tang and Meersman [125]					✓				
Chen et al. [94, 112, 115]		✓	✓			✓	✓	✓	✓
Al-Hamadi and Chen [99]	✓		✓						
Mendoza and Kleinschmidt [107]	✓						✓		
Lin and Dong [116]	✓					✓	✓		
Mahmud et al. [132]	✓	✓	✓			✓			
Fortino et al. [75]	✓		✓				✓	✓	
Chen et al. [126]	✓							✓	
Azad et al. [88]	✓	✓				✓		✓	

Table 2 Inclusion–exclusion criteria for review methods

Criterion	Rational
Inclusion 1: A study that is published in the trustful recommendation in the IoT field	We precisely examine how trust evaluation affects either reliability in IoT or indirectly assesses recommendation accuracy in this scenario
Inclusion 2: A study that is directed either by academics or practitioners	Both academic and industrial solutions are taken into account
Inclusion 3: A study that is peer-reviewed	This standard guarantees a precise quality level and a considerable amount of content
Inclusion 4: A study that is written in English	For suitability, we excluded papers published in other languages rather than English
Inclusion 5: Date of data extraction	From 2011 to December 2018
Exclusion 1: A study that made part of journals	Conference papers, doctoral dissertations, books, editorial notes, and unpublished papers were not involved, as researchers commonly refer journals to obtain and disperse information
Exclusion 2: A study that developed diverse recommendation mechanisms on the Internet	Only recommendation mechanism in the IoT is relevant to this study
Exclusion 3: Duplicate copies of exactly like study	Various reports of a study are in differing journals, the most thoroughgoing issues included

on the basis of trust propagation among neighbors, the indirect trust of this path can be achieved. Obviously, we should take in mind trust values, reputation, similarity, social network, energy and distance of nodes as three influential measures, while establishing trustworthy relation among them. However, all recommendations are not confidential; and certainly malicious and conflict recommendation occurs in IoT. Therefore, an apt method is required to assess the trustworthiness of a node's recommendation.

The trust-based recommendation offers worthwhile information to the users via trust, in which trust is a measure to believe in the willingness of user based on its previous competence. In a real environment, two users' simultaneous evaluation on the same item is not regular, and if there is no direct trust between the active users and the recommenders, we utilized transitive characteristic of trust. In other word, we propagate the existing direct trust. It means when node A trusts node B and B trusts node C, then A trusts C to some extent. Eventually, the active users build up indirect trust relationships with the recommenders on the basis of trust propagations and its trustworthy network will be broadened. Hereby, the sparsity and a low number of trusty users will be solved [12].

Our trust evaluation model aims to provide the trustworthiness in IoT scenarios with the interaction of disparate devices, by addressing trust value computation, trust aggregation and prohibiting the abnormal nodes with punishment. This model employs several trust metrics which are mentioned in Table 2. When nodes transmit recommended indirect trust to an object, some malicious parties abuse and provide a false or exaggerated recommendation to fraud benevolent parties or boost the trust value of colluded adversary peers. To overcome this manipulation, the dimension's values should be aggregated to achieve a final reliable score [19].

Security mechanism such as cryptography authenticates entities and assures the integrity of messages. Although the participation of abnormal and illegitimate entities is prevented, since malevolent entities could capture and manipulate legitimated nodes

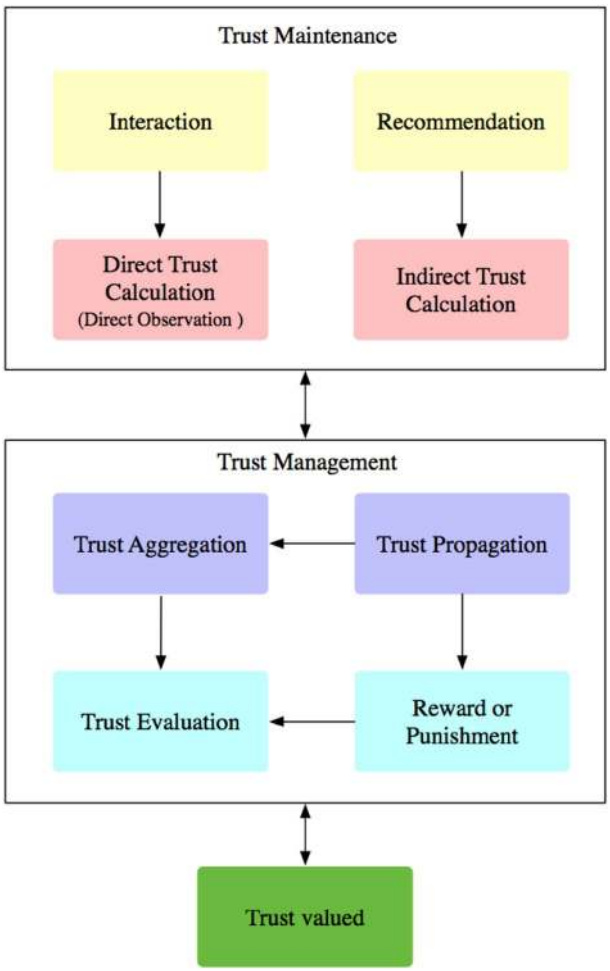

Fig. 1 Sample scenario for Trust-based recommendation Model in IoT

and exploit them as malicious, attackers will disable the authentication mechanism in a different form and penetrate in the network again. Therefore, despite identity protection based security mechanism, the IoT network still suffers various disobey. As a specific attack method could recognize susceptible nodes, we employ trust based evaluation mechanism to predict entities' behavior and take countermeasure values to either eliminate or void related threats. By means of trust concept, we determine the probable behaviors of nodes and exclude misbehaving ones from operations, while rewarding well-behaving nodes for benevolent collaboration in data transmission. In Fig. 1 we propose a trust-based recommendation model consists of three fundamental modules; trust maintenance, trust management, trust value; each are described below [20]:

Indirect trust evaluation When an evaluating node is incapable of directly assessing an encountered element's behavior, it builds a reliable trust path based on the indirect knowledge and opinions obtained from an intermediate node or a chain of trusted parties [21, 22].

Direct trust evaluation A node infers first-hand trust information by its personal experience which gathers either through one-to-one interaction with neighbors, or direct observation of nodes' social behaviors or attitudes towards one another [21, 22].

Recommendation To obtain trustworthiness of remote members in the network, a requesting node needs an assisting node's evaluations toward the target entity. These indirect trusts are named recommendation.

Trust aggregation To achieve overall trustworthiness degree, a node aggregates personal direct trust with received multiple recommendations. In this respect, trust aggregation method detects and excludes slandering recommendation by assigning a low trust weight to malicious nodes [23, 24].

Trust propagation After collecting the trust factor from a target node and evaluating trust value by the proposed model, the final result is propagated as recommendations. As soon as a node receives a recommendation, it should run the aggregating process [23].

Reward or punishment As soon as completion of the transaction, the requested either punishes or rewards the node's behavior either by positive or negative feedback. Nodes with high trustworthiness are involved in the next interaction and low score nodes are certainly isolated [22].

Taxonomy of trust-based recommendation

In view of the fact that trust is an imperative and elaborate concept in the decision-making process through unpredictable circumstances, in order to develop the most appropriate trust-based recommendation in a heterogeneous IoT environment, we have crafted recommendation taxonomy by planning a three-layered IoT architecture:

- *Physical layer* includes smart device environments and human social life by means of sensors, actuators and sensing technologies like RFID, NFC, WSN, etc. In this regard, information is converted to digital signals and transferred in the cyber world [25].
- *Network layer* processes and transforms perceived environment data through communication technologies, like Wi-Fi, WiMAX, LTE LoRA, etc. Since a large amount of data will be transmitted through IoT network cloud computing is responsible to store and process them.
- *Application layer* intelligently offers services to end user in a pervasive manner, and provides platforms (e.g. actuating machine) to accomplish the IoT perspective (e.g. secure transportation, confidentiality, identity management, authorization) [26].

Nevertheless, trustworthy IoT system implies on not only each layer's performance with regard to security, privacy, etc. but also can provide a comprehensive evaluation of encounter's ability for benevolent cooperation in confidential data forwarding process [27]. In this subsection, we represent a classification tree to categorize IoT recommendation models according to the adopted trust mechanisms in three design layers; works will belong to similar sub-class if their evaluation techniques are identical, any deviation will put them in a separated class. It is noteworthy that some works lay in two or more classes, which is unquestionable due to this job's trend concerning both abstract and concrete aspects of IoT structure. Our proposed taxonomy includes 24 identified

subcategories, which will be thoroughly explained further by concerning relevant experience.

Trust evaluation metrics

In this subsection, we investigate trust metrics for a recommendation in IoT. Reviewed literature in trust evaluation [28–35] proposed various metrics for trust computation in IoT environment and we summarize most pertained ones in Table 1.

Trust The Oxford Reference Dictionary defines trust as "*the firm belief in the reliability or truth or strength of an entity*". A trustworthy member is meant to perform expected interaction without fail, disclosing confidential information and rather provide service properly during acceptable timescales. Therefore, trust is an attribute of relating to believe in honesty, competence, security, reliability, dependability, and timeliness. Grandison and Sloman [36] stated trust as "*the firm belief in the competence of an entity to act dependably, securely and reliably within a specified context*". Gambetta [37] defined trust as "*Trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends*".

Accuracy In metrology, accuracy is a statistical bias; describes proximity between a measure results and the "true" value [38].

Quality of service The main object of the service recommendation scheme is to improve QoS and simultaneously resist against malicious node behavior which attempts on service decomposition. In order to fulfill this goal in a dynamic recourse constrained IoT environment, a dimension of six properties of trustworthiness evaluation factors is recapitulated of previous interactions to acquire coherent recommendation [39].

- *Successful-Interactions* percentage effective actions occur within a device over the total amount of previous.
- *Availability* means the proportion of total time that IoT device is up and operating at a given time interval, e.g., 99.999% ("five nines"), which assures legitimate user access to the resource, upon requirement.
- *Throughput* in IoT services, it is defined as a fortunate packet delivery rate across the network per unit time. This metric is affected by a given device processing power and physical medium.
- *Delay* indicates travel time of a bit of data over a communication channel from one device to other, or, from a more general point of view, a time between the cause and the effect of some physical change in the system being observed.
- *Reliability* specifies the probability of non-failure system operation over the entire interval. In IoT, reliability necessitates sensing devices, address handling, data processing, anomaly recognizing, maintenance, etc.
- *Performance* It measures the system efficiency during the process of collecting, analyzing and/or reporting information from the aspect of users' satisfaction from recommendation as well as timely execution.

Security Trust and confidence are said to "imply a feeling of security" [40]. Interactions often happen in uncertain conditions and security is a mechanism, to the extent that one node could rely on other ones in IoT scenario. Therefore, a node security method is

introduced to make the recommendation information more accurate and also improve the fault-tolerance. Moreover, building a trust model system will satisfy the trustworthy communication path and address security issues in networks [41]. Security is a combination of confidentiality, availability and integrity attributes prevents unauthorized and unauthenticated access, disclosure, modification, inspection, recording or destruction of information [42].

Similarity develops personalized trustworthy recommendation by analyzing and comparing social network information [43]. It is a crucial factor includes [44]:

- *The community of interest* two objects of communal interest probably share common interest, knowledge, and standard to an offered service of a similar device and visa versa. These objects are supposed to interact with each other and often increase performance.
- *Social contact* presents closeness of two nodes that have the same physical contacts and hence common sentiment towards devices which provide the same service.
- *Friendship* it is a fundamental intimacy factor in a social relationship for screening offered recommendations.

Energy consumption the content of energy consumed through the network. Since almost all entities in IoT are low power devices, applying trust scheme create a problem that nodes with higher trustworthy have more workload and are less time efficiency, thus energy conservation is of paramount importance [45].

Quality of recommendation offers already-existing, well-known trust models to requesters, which can complete these templates with further information, like trust and reputation entities [46]. In other word, recommendation metrics are coherent integration of already presented parameters.

Reputation is an opinion about an entity (a person, a social group, or an organization) built as a result of social evaluation upon three distinct criteria: cognitive representation, population object, and objective emergent property [46]. Jøsang [47] definition is "*Reputation is what is generally said or believed about a thing's character or standing*". This item recorded past transaction and feedback between nodes. Then by evaluating the given node's trustworthy performance, the impact of malicious nodes declined.

Social network is an important characteristic in SIoT for trust evaluation, because nodes in common environment assume to have a closer relationship and provide the value of trustworthy. Social relationship is a community of informational networks, characterized by their capacity to learn, process and exchange information among smart objects. They were categorized into five relationships as parental object relationship (POR), co-owner object relationship (OOR), co-worker object relationship (CWOR), co-location object relationship (CLOR) and social object relationship (SOR). Social computing in IoT identifies behavioral, contextual awareness, cooperation and quantitative aspects of virtual intelligent objects during relationship establishment by mimicking human social rules [48].

By taking inspiration of different relationship between individuals, a classification of objects is given below [49]:

- *Parental object relationship (POR)* Objects belong to the same family (model, manufacturer, production period, etc.);

- *Co-location object relationship (CLOR)* Objects attend concurrently in an exactly similar place;
- *Co-work object relationship (CWOR)* Objects encounter at their owners' workplace and cooperating in the same application;
- *Ownership object relationship (OOR)* Objects belong to the unique owner;
- *Social object telationship (SOR)* Objects encounter frequently while their owners getting in touch at the same bus/restaurant/gym every day.

Conceptual methodology

An SLR is a critical assessment of research studies which address a peculiar topic. For this purpose, researchers utilize a method of locating and assembling a literature body by employing a set of defined criteria. Typically, a systematic review of aggregates and synthesize existing knowledge regarding a research issue. It is argued this approach can identify gaps in earlier research, limit systematic error and chance effects, and enhance the legitimacy of the data evaluation. Mentioned benefits create more dependable results and provide background information for further investigation. An SLR method originated from the medical field [50] and recently there has been a move to use more evidence-based researches in the social science and engineering domains. This methodological approach has been adopted in publication since 2004.

Question formalization

The purpose of this review is to explore critical challenges through future community-based IoT systems, to identify areas where further studies are necessary to enhance recommendation accuracy. We also conceived that trust, as an irrevocable factor, has already been exploited for validating recommendation correctness. Moreover, we attempt to discriminate underutilized researches while concentrating and highlighting their likely gaps. This research aims to bring up the below-mentioned questions:

RQ1: *How do the publication trend in recommender system move with the evolution of IoT?* This is a statistical question aims at used datasets or benchmarks, considered case studies and the number of IoT trust and recommendation related publications

RQ2: *What is the significance of trust with the increasing growth of recommender system in IoT?* The question aims to evaluate IoT trust metrics in published studies over time and underline the necessity of recommendation accuracy in IoT

RQ3: *How much do current trust evaluation techniques meet the recommendation metrics in the IoT field?* The object of this question is to assess the compatibility of trust methods with regard to fundamental metrics of a recommender system in the IoT environment

RQ4: *Which defects and solutions were identified on the side of a recommender system for future trends in IoT?* This question investigates weakness in IoT recommendation and recognizes techniques to ensure trustworthiness accordingly

RQ5: *What are the main challenges of IoT with trust management?* This question enumerates some of the encountered challenges for establishing trust in IoT environment

RQ6: *What are the open issues of IoT with trustworthy recommendation?* This question emphasizes future directions for new practitioners.

Dissecting above mentioned questions includes different stages of query probing, source assignment, estimation criteria, data withdrawal techniques, and synthesis strategy, which eventually end up precise responses within the paper scope.

Search query

Search strings are primarily defined on academic databases by breaking down each question into individual facets and selecting the most competitive keywords with respect to this subject. After variant steps of utilizing a list of synonyms and alternative spelling considering subject headings used in journals and databases during initial analysis other terms will be obtained. The sophisticated search string can then be constructed by examining the coverage of outcomes by associating the Boolean OR and Boolean AND of the primary pilot. Hence, four keywords *"Internet of Things"*, "*IoT"*, "*recommender system"*, and "*trust"* were selected. Specified technology evaluation string is:

[(*Internet of Thing*) OR (*IoT*)] AND [(*recommender system*) OR (*recommendation*) OR (*trust*) OR (*trustworthy*)]

In the preliminary stage, the aforementioned string was integrated Boolean AND with words as "Survey", "Review" and "Overview" and applied on the title of articles, to accentuate lack of comprehensive investigation and technical comparison on existing approaches up to now.

[(survey) OR (review) OR (overview)] AND [(*Internet of Thing*) OR (*IoT*)] AND [(*recommender system*) OR (*recommendation*)] AND [(*trust*) OR (trustworthy)]

Then, to maximize the amount of returned documents, the search string was applied not only on titles but also on the abstract and whole body of the studies. We conducted this research in December 2018 and specified a time range from 2011 to the end of December 2018. Nonetheless, to further outreach preceding investigation on the aforementioned pilot, a Boolean OR of "*Internet of Things"*, "*IoT"*, "*recommender system"*, and "*trust"* was also applied from 2000 to 2011. Similarly, below string was spread on titles, abstract and body of the studies:

(Internet of Things) OR (*IoT*) OR (*recommender system)* OR (*recommendation*) OR (*trust)* OR (*trustworthy*)

In order to expand the scope (Research trends or specific technology evaluation question) as far as feasible, we developed the search strings for the academic database to all types academic documents, not just systematic reviews and mappings.

Selection of sources

The search process was a manual review of specific journal articles since 2011 in-depth and before to have an overall view of initiation point. Consequently, we extracted relevant result by categorizing publishers. In an indicated way, search process involved most reliable peer-reviewed articles in four electronic databases such as IEEE Xplore, Springer Link, Science Direct and Wiley Online Library. We picked journals since they were known to include either empirical studies and novel contribution, literature surveys, or utilized as sources for other SLRs.

Selection criteria

Once the potentially relevant study phenomena obtained, they need to be qualified for actual study criteria based on Kitchenham et al. [11] Quality Assessment Checklist (QAC) to provide articles from peer-reviewed journals with direct evidence about the research question. In order to alleviate the likelihood of bias, inclusion and exclusion criteria should be developed based on the following quality assessment question:

QA1. What are the objectives of this research study?
QA2. How proper the research methodology is for the studied subject?
QA3. What sources were constituted to investigate research study? Were there any restrictions?
QA4. Do the sufficient conclusions achieve from the synthesized evidence?

These patterns employ suitable methods and eliminate the possibility of synthesis or antithesis choice by researchers' expectation. If reviewers determine the validity and appropriateness of each study, it fills with 'yes'. We summarize the inclusion–exclusion criteria for this study in Table 2.

Quality assessment and data extraction

The phase of data withdrawal begins with practical screening. We picked 206 studies totally. In the first step, conference paper and book chapters were excluded. By adverting articles' title and the publisher, they were selected upon comprehensive criteria mentioned in Table 2. In order to understand the papers' contribution, we read the abstracts and search keywords. If not eliminated due to inappropriate abstract and concept, the full body of remain papers was reviewed to access their relevance. Due to this time-consuming process of filtering studies based on the relating application of specific topic, publication year, content and (QA1–QA4), and finally 59 articles were picked as a principal study.

While Table 2 carried out knowledge sharing in online databases by 59 articles, the selected papers' distribution over publication time is demonstrated in Fig. 2. A remarkable rise happens in the number of papers in the field of recommendation in IoT from 2011 to December 2018; also, during 2018 the amount of published articles is highest. In addition, Fig. 2b illustrates a pie chart of articles percentage over

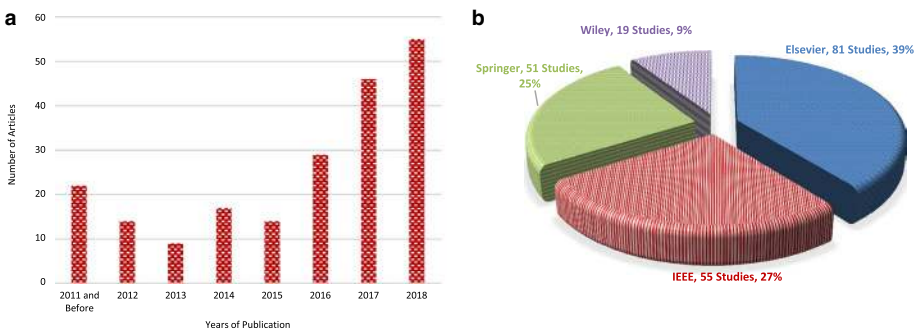

Fig. 2 **a** Number of primarily selected studies per year. **b** A pie chart of articles percentage on different publishers

the whole time in each investigated categories including Elsevier, Springer, IEEE, and Wily. Figure 2a shows the distribution of the circulated papers over each year which illustrates different publishers' contribution separately. However, as mentioned beforehand we excluded conference paper in Table 2, whereas academics oftentimes refer to journals for obtaining the valid document and disseminating their findings. Pertinent to matter introduced in the first formalization question (RQ1), the necessity of recommendation accuracy and utilization of trust management mechanisms in the IoT environment is significantly outlined.

Recommendation mechanisms based on IoT architecture

IoT recommendation is still infancy and as discussed further inadequate experience fulfilled in this field. In particular, already available articles have not scrutinized the whole dimension in the trusted recommendation. In this section, we classified them based on underlying techniques in distinguish layers which are developed by branches in Fig. 3. To this extent, experiments are distributed between three holistic and ambient platforms. The first subclass is *physical or hardware layer*; consists of primary hardware elements deployed in actuation, a communication network. Physical sub-branch here includes all responsibilities of transmission and reception of raw material of the physical layer as well as reliable transmission frames among nodes which are assigned to the data link layer in the ISO/OSI model. Therefore, it contributes to entities such as sensor networks which are adopted as information collection, RFIDs provide identification and information storage, embedded edge processors accomplish information to process and et cetera. The results of different methods' review on this layer are depicted in Table 3.

System on chip (SoC)

It is an integrated circuit that associate a microcontroller with peripherals components like Wi-Fi module or coprocessor. SoCs provide a solution to challenge design problems in embedded systems, multimedia, mobile and electronic domain due to their low power consumption [51]. The Raspberry PI is an instance of SoC with an Acorn RISC Machine architecture (ARM) compatible central processing unit (CPU) which does not contain data storage [52].

To drive security, a system-level requirement, several broad classes: software techniques (e.g. sandboxes, microkernels, and virtualizations) and hardware technologies (e.g. ARM TrustZone) have been applied. Pinto et al. [53] focused on TrustZone-based architecture that partially tackles the aforementioned need and promoted hardware as a trusted root, namely IIoTEED. Given technology, guarantee resource-constrained edge devices network connection while meeting trade-off between performance and security. To tackle any jeopardize, IIoTEED must be integrated with critical hardware-based security and acceleration techniques. As an advantage, the anti-counterfeit solution in edge device isolates fake spare parts and strengthens transport layer security and encryption, but coping with side-channel attacks are not included within the specification of ARM TrustZone. Therefore, authors will maintain practical implementing of proposed vision and security reinforcement as future work.

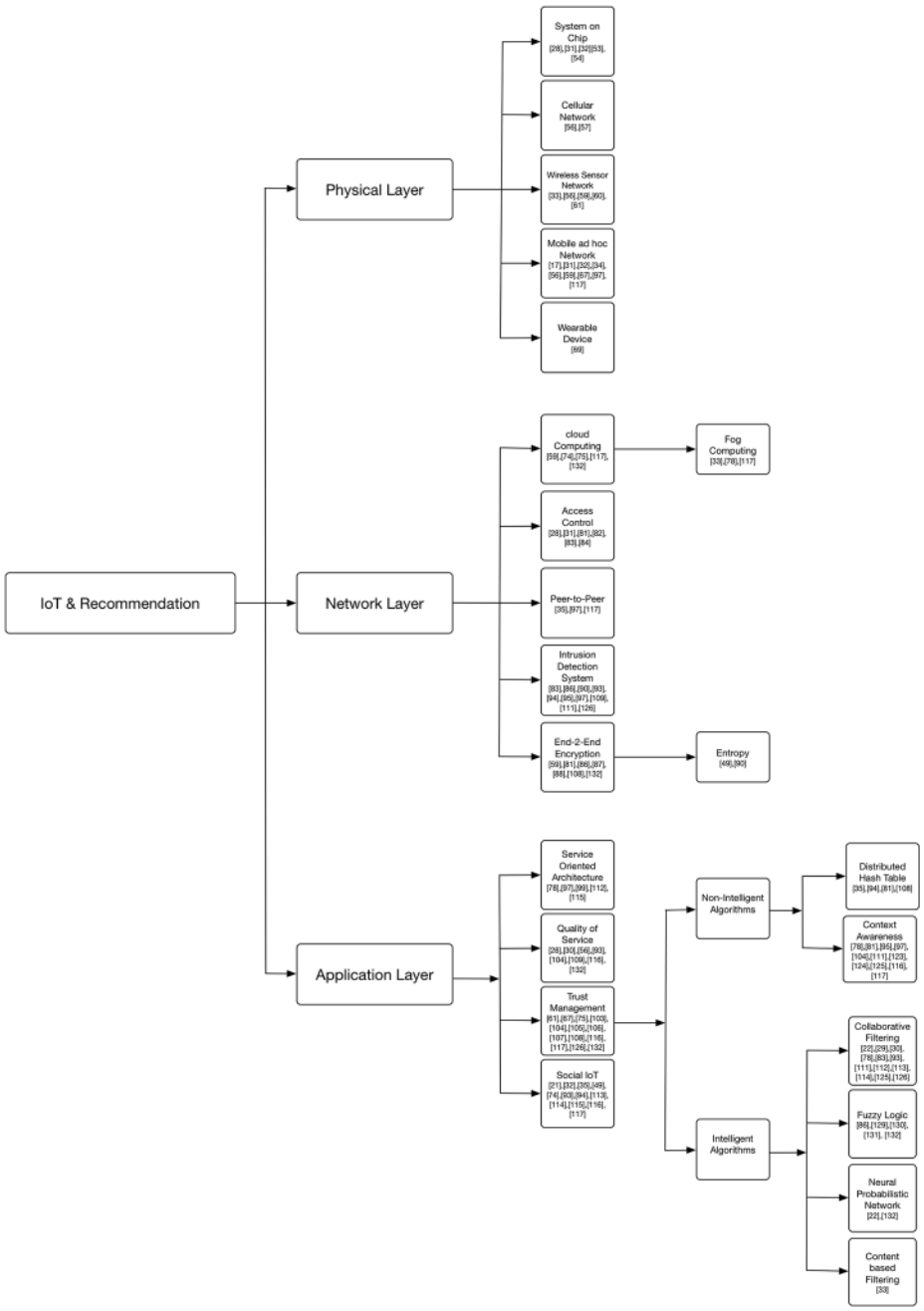

Fig. 3 Taxonomy of trust-based recommendation in IoT

Cao et al. [54] explored Usage control for the trustworthy data-sharing platform to make cities smarter. This is a policy-based data usage control (DUPO) model to hold different obligations and constraints that owners impose on data utilization. Further, this intermediation platform makes the supply chain more transparent and traceable. They took into account data usage requirements spatiotemporal granularity, abstraction/masking typical information. For the proof-of-concept, DUPO platform received data from the sensors, simulated by DPWS and CoAP. The Raspberry PI utilizes Ethernet

Table 3 An overview of trust strategies for a recommendation in the Physical layer of IoT

Reference	Advantages	Disadvantages	Evaluation technique	Evaluation environment
Pinto et al. [53]	Assure security and almost intact real-time properties Preempt Linux execution, even performing an IRQ	Applicability for resource-constrained edge devices not implemented Not integrated with hardware trust anchors to tighten security		On a ZedBoard targeting a dual ARM Cortex-A9 running at 600 MHz
Cao et al. [54]	Improve transparent and traceable data usage Ensure owners' obligations and constraints on data usage Provide data access as well as decision explanation Deal with rule conflict Policy composition	Lack of a concrete solution for trustworthy data sharing Not responding query on real-time Not involve end-users in evaluation to ensure usability Not share data on open standard APIs	DPWS and CoAP simulator	SPINdle-based jDUPO Visualiztion tool prototype
Nieto and Lopez [56]	Multi-hop communications reduce collisions risk while saving energy Convergence, reduce false positives, scalable QoS mechanisms and used in resource-constrained network	Protocol stack has an interface for technologies in MN Sensor's power consumption to connect to MANET interoperability problems, the complex path towards cooperation		g MATLAB and DOT files
Shirvanimoghaddam et al. [57]	Non-orthogonal multiple access techniques handle a huge number of Cellular devices 3GPP wide area solution on cellular low-power NOMA better throughput RA stage removal and same channel transition Radio resources utilization, and remove signaling overhead	No practical implementation challenges massive IoT in cellular networks: Device cost Battery life Coverage Scalability Diversity Challenges massive NOMA in cellular IoT: Traffic Power Code design SIC User fairness	Not mentioned	
Zafar et al. [59]	Identifies secure provenance for trust	Runtime overhead in dynamic instrumentation	No evaluation	

Table 3 (continued)

Reference	Advantages	Disadvantages	Evaluation technique	Evaluation environment
Litescu et al. [60]	Twenty percent of participants as optimal data sources Lower information precision to participants noise improves traffic situation with massive participants	Not implemented under realistic traffic network and human behavior Performance decreases with huge involvement as sources/consumers	Poisson process	
Ali et al. [61]	Central trust management lowered the sensors' energy cost, computation and storage overhead Variable forgetting factor protect against on–off attack High delivery ratios and good data aggregation at base station	Difficulty in contrasting this scheme's performance with others Trust is centrally handled in base station		Using C-Language
Tan et al. [17]	Effective secure routes Reasonable packet delivery rate, latency, and overhead	To hinder evil nodes, FPNT-OLSR creates longer paths and bigger average latency FPNT-OLSR(R) overhead is more than OLSR's	OLSR simulation	MoSim MATLAB
Kang et al. [34]	Protect user privacy and security in IAM	The linear empirical threshold for a tainted hit to IAM App graphics not convenient	TaintDroid	IAM prototype
Sicari et al. [32]	Secure mobile devices Communication integration in middleware security Collaborative interaction of smart devices	The lack of computing resources and ad hoc nature Indeterminate IoT taxonomy	No simulation or implementation	
Ali et al. [31]	Concurrently measures static and dynamic behaviors Detects deviations Supports multiple stakeholders' privacy Decreases log size and reduce network overhead Improves detection accuracy	Log size increases with window size	Trusted platform module (TPM) LSM in Linux Kernel Raspberry Pi	Machine learning WEKA
Køien [67]	Modeling human-to-device trust	TNA-SL was not feasible and practical Cannot cost-effectively mimic actual scenarios	No simulation	
Asthana et al. [69]	Consider budget and resource capacity Constraints When no tools exist, give feedback to technological developers	Limited samples Not evaluated with real data and condition such as an individual's mobility, background, personal preferences, financial factors		Evaluated in Weka library

gateway and Z-wave sensor devices to emit caught messages. raspberry locally processes data subscription from the intelligent parking application (IPA). However, added trust performance does not compel a negative impact on the system. While implicitly confessing on deficiency, they suggested uncovered aspect as future studies: (1) efficient real-time process while concerning scalability and trustworthy distribution in framework, (2) enhance open standard APIs to impel partners to share, manager and deliver correct meta-data on the platform and handle semantics variability and (3) to obtain end-users usability evaluation of information visualization.

Cellular networks

A cellular network is a radio communication network that is distributed over a wide geographic area called cells. Each cell is defined as the physical space served by at least one transceiver positioned in a fixed location, but typically at least three base transceiver stations required. These cell sites coverage voice or data packets transmitted between intracellular users. Various kinds of wireless devices such as smartphones, tablets, and laptops with portable modems, etc.) communicate among themselves and via base transceiver station, either move trough one fixed or more cells during transmission. In another word, the cellular networks are dependent on service providers and it's network infrastructure to achieve authentication and authorization of services. Imperatively, to avoid interference and guarantee the security of the network, data are transmitted with distinguishing frequencies among neighbor cells [55].

Nieto and Lopez [56] analyzed security and quality of service (QoS) mechanisms in the resource-constrained networks, called wireless sensor networks (WSN), cellular networks and mobile ad hoc networks (MANET) as a primary part of future internet (FI). Additionally, they depicted a taxonomy to identify technologies similarities plus the interconnection indications. Predominantly, they achieved parametric relation among security and QoS. Although user satisfaction and implementing QoS mechanisms through internet seem ever closer, but carrying such developments without taking into consideration the future network requirements, for instance, interoperability and secure cooperation among three representative networks is a vital threat. Shortly after networks' full operation, security and QoS problems will falsely-affect the inter-connection behavior. Therefore, future steps will focus on obtaining optimum security and QoS tradeoff in crucial systems and user-dependent infrastructure. Firstly, due to the WSN role in early warning system, security impact on critical infrastructure protection is of great value for future study. Secondly, although the user's impact on the composed environment is unpredictable this measurement considered as a key point for FI becoming a reality.

Shirvanimoghaddam et al. [57] presented massive non-orthogonal multiple access (NOMA) as a potential random access solution for cellular IoT to handle M2M communication and traffic. Traffic, load and channel estimation, power allocation, devices synchronization, channel code design, the complexity of successive interference cancellation and user fairness are some practical challenges of massive NOMA for massive cellular IoT, which are highlighted as a future direction. The benefit of the hybrid scheme for IoT is an aggregation of the RA procedure and the data transmission and send a message through the third message channel. Although this will solve the signaling overhead

in cellular systems as well as efficient use of radio resources, but is only applicable for delay-tolerant M2M. Besides, NOMA offered throughput efficiency in simple low power and cost IoT devices, and provide scalability and diversity on a large number of devices in the IoT cellular network. Authors claimed that by involving with 3GPP technologies, this solution will boost IoT cellular performance.

Wireless sensor networks (WSN)

They are composed of sensors, where most of them are autonomous, resource-constrained and specific purpose units used to monitor a region for obtaining environmental data. Then, data can either routed to a principal node called sink or be to collected and analyzed prior to sending to the sink node. Sensors are wirelessly connected and they, in case necessary can be replaced easily by other units should any of them stop operating. Two categories of WSNs exist: An unstructured WSN contains a dense collection of sensor nodes deployed randomly into the field and lead to uncovered regions and a structured WSN which all or some sensor nodes deployed in a pre-planned manner in a specific location and consequently fewer nodes deployment achieved with lower maintenance and cost [58].

Reliance of data plays a crucial role in decision making and risk assessment. In this regard provenance aids in data authentication by assuring properties of integrity, confidentiality, privacy, etc. However, its trustworthiness will only be achieved through secure provenance. Zafar et al. [59] analyzed underlying schemes that provide trust via secure provenance. They introduced a secure provenance taxonomy for analyzing privacy and integrity challenges and conducting a comparative review of the scheme in the cloud and wireless sensor network domain. Consequently, they highlighted future trends such as provenance-based access control, storage efficiency and mission miscellaneous domains for the research community, which could be considered as weak points of this work.

Due to advancements in Intelligent Transportation Systems which commuters simultaneously invested as real-time traffic recommendations consumer and data provider, Litescu et al. [60] investigated the effect of various type of inaccuracy in transportation. He acquired interesting observation: for data collection tiny fraction ($<20\%$) of the traffic participants is sufficient, and a massive number of participants drop performance, yet noise can compensate for this defect. In the future, practical experiment with real traffic network, pattern and human behavior are essential to demonstrate proposed scheme real-time prediction and accurate recommendation.

Ali et al. [61] drafted a trust scheme in WSN, where data aggregation is assigned to external mobile elements for disseminating the data toward the base station. MEs can either be common movable sensors or a smart mobile with a sensing power which represents the cluster heads' duty in IoT network. Authors referred to [62] for mobile element's selection procedure and utilized the cluster-based routing algorithms, Beta distribution, history window and a dynamic forgetting factor to eliminate trust manipulation by mischievous mobile elements. Although experimental simulation depicted the scheme's prosperity in keeping low data energy loss, whilst not negatively undermining delivery ratio and coverage, but no direct comparison with chosen trust schemes; lightweight and dependable trust system [63] and lightweight group-based trust management [64] revealed their findings.

Mobile ad hoc network (MANET)

It is a collection of self-organized wireless devices connected without the aid of any centralized management or fixed network infrastructure [65]. Ad hoc network is a dynamic topology—where (re)configured nodes enter and leave the network continuously and autonomously—nodes are free to move independently in any direction and heterogeneous—and some can be servers while others can only be clients. The ability of an ad hoc mobile device to act as a service provider depends on its computation, memory, storage, and battery life capacity. Hence, a mobile node should concern own "well-being"—before committing as a router to forward traffic on the behalf of others—for two reasons: If a node is damaged or lost, they can not easily be substituted, more importantly, these devices are close to the user (e.g., laptop and PDA) and include users' private data [66].

With the rapid development of the Internet of things (IoT) and ubiquitous computing, Tan et al. [17] presented a trust-based fuzzy Petri net model to estimate trust score in MANET and filter slander recommendation and malicious or compromised nodes. In addition, they proposed a routing algorithm with the maximum path trust ratio. Then, they extended the optimized link state routing protocol (OLSR) called FPNT-OLSR protocol, which generates no extra control messages during trust collection and aggregation method. MoSim program proved this mechanism efficiency in establishing secure routes and improvement in term of packet delivery ratio. However, to avoid mischievous nodes, FPNT-OLSR creates longer paths which slightly increases average overhead and latency. They suggested applying this model to other scenarios like VANET or cloud computing.

Kang et al. [34] proposed an interactive trust model (ITM) to preserve user privacy and security in the IoT application market (IAM). Application trustworthiness (AT) can be evaluated by assimilating the similarity of smartphone behavior and users' desired behavior in a mathematical format. A prototype system of rural areas in China with definite drawbacks was implemented. Future research needed to overcome deficiencies, for instance, linear function and the empirical threshold value for a tainted hit to IAM and agent customization for interactive trust model in the fundamental structure of work. This can be achieved by finding bottlenecks and customizing agent in the form of a widget.

Sicari et al. [32] published a survey where authors concerned open visions in IoT such as dissimilar paradigm, heterogeneous nature of objects, and diverse architectures. From one side, they analyzed the most applicable security (e.g. integrity, confidentiality, authentication, access control) related solution in the IoT environment and on the other side they employed privacy, and trust among users and things. They focused on the integration of IoT and communication technologies regarding security middleware to cope with protection constraints, as well as securing solutions for mobile device challenges under a legislative point of view. The main limitation of their work are indeterminate IoT taxonomy and eventually, the lack of rationale classification on reviewed activities.

In this research, Ali et al. [31] have designed and implemented a lightweight Linux Security Module (LSM) module for IoT devices that is scalable enough to achieve security goals and trustworthiness of remote entities. The proposed module of attestation, at one time, validates different application's static and dynamic behavior simultaneously in the kernel space. Behavior and attack verification fulfilled via machine learning tool, WEKA. Ultimately, the designed algorithm is capable of corporations in a solitary

Platform Configuration Registers (PCR) or Stored Measurement Log (SML) which overcome the privacy issues related to stakeholder(s) behavior log. Although the window's log size increased by its size growth, it stabilized after a specific period and ultimately reduced network transmission overhead.

With regard to complexities and dynamic nature of IoT environments ascertaining the real intent of the device is an inherent problem for a human. In order to oblige devices to associate correctly in IoT network, Køien [67] proposed subjective logic systems, TNA-SL for modeling human-to-device dynamic trust interaction (belief and uncertainty). He examined trust in an IoT device and services in multi-faceted software/hardware approaches transitivity, integrity, psychological view of risk and the human brain, distrust, deception, counter-attack, malevolence, and benevolence, reputations, confidentiality. Having in mind that human heuristic threat and opportunity handling is not applicable without least faults trusted proxy devices utilization and whereas feasibility and practical impact of the proposed model, in reality, was not demonstrated, he encouraged TNA-SL models behavior in an asymmetric network propagation as well as reputations/opinions broadcasting. Due to the lack of risk assessment in required trust level, he inspired investigation in this area to determine the frequency of the trust and belief.

Wearable device

Wearable technology is smart electronic devices with micro-controllers that can be implants or worn accessories such as activity tracker [68]. Wearable devices are an instance of the IoT, where "things" such as electronics, software, and sensors exchange data, via different wireless protocols, with a manufacturer and/or operator without human intervention.

Asthana et al. [69] addressed the proactive controlling of a given individual's health by a recommendation engine in wearables solutions. The demographic attributes like age, the location, gender and the Electronic Health Records (EHR) of residences are fed to a machine learning classification to predict disease. It utilized mathematical optimization to recommend optimal personalized wearable devices to individuals. This model was evaluated in a very tiny scale, therefore as future work, it is essential to perform a more comprehensive numerical study under a real circumstance by readings sensors, monitor person's health, and trigger measurement. Secondly, financial issues, personal preference, the mobility of individual are equally crucial in the analysis, that is neglected in this paper.

The second branch is a *network layer*, an interface layer located between the hardware layer and the application layer. This sub-branch assumes responsibilities of structuring, addressing, routing, traffic management which is dedicated to Network layer in ISO/OSI as well as reliable transmission includes activities of segmentation and sending an acknowledgment, tasks employed by transport layer in ISO/OSI model. The first step of communication such as subscription and message forwarding management occurs in this platform. Moreover, it handles critical issues such as data filtering, data propagation, data aggregation, access control, malicious node detection, cryptography, information discovery and etc. [70]. The results of different methods' review on this layer are depicted in Table 4.

Table 4 An overview of trust strategies for a recommendation in the network layer of IoT

Reference	Advantages	Disadvantages	Evaluation technique	Evaluation environment
Wang et al. [74]	Overcomes the DoS threats by selfish nodes Avoids DDoS threats by crowdsourcing	Non-cooperative parties reduce efficiency Non-malicious members received Lower may wrong results provide by honest participants	No simulation	
Fortino et al. [75]	Mutual benefit of single agent engagement in a group By group formation, the untrusted agents, gradually substituted with trusted ones Local reputation avoids global mechanism's overhead Good performance achieved with agents' small portion of involvement	Few statistical parameters were concerned With a minimum number of examined group, a few untrusted agents exit which lessened not totally removed with rising numbers	Poisson distribution	Not mentioned
Garcia-de-Prado et al. [78]	Facilitates communications and data delivery between C-IoT layers Avoids edge nodes waste resource Save expense in cloud real-time data processing	Not process many events per second in fog nodes Deter user profile and experience	Esper CEP	Mule open source ESB MQTT Mosquitto broker—Eclipse Case study: ir4HealthAdmin
Sfar et al. [81]	Adapted to any real environment to Improve productivity intensify issues of security and privacy	Theoretical rigor limitation Do not consider: auto-immunity, safety, reliability, and responsibility		Case study
Ouaddah et al. [82]	OM-AM access control solutions Considers centralized and decentralized approaches	Usability aspects are not extended No implementation on privacy-preserving access control framework	No simulation	
Roman et al. [83]	Cooperation diverse IoT entities despite lack of central systems Probability to pinpoint the problem origins Implements privacy and scalability Push/pulls data when needed	Key management between the limited device Overhead caused by incoming connections Concerns about internet protocols adaptability with context	No simulation	
Mahalle et al. [84]	Guarantees scalability, flexibility, and energy efficiency Devices proliferation does not degrade performance Avoids communication in low trust nodes More power conservation and high residual source	A mathematical model not implemented in real time RFID Not organized with capability-based access control	Mamdani logic	MATLAB 7.0. NS2

Table 4 (continued)

Reference	Advantages	Disadvantages	Evaluation technique	Evaluation environment
Sicari et al. [86]	Validated by real-time open data feeds NOS detects: Data confidentiality, source privacy, and integrity violations; Unauthorized access Robustness of key management Replay or routing attacks Without restarting the whole system add new modules, duplicate or remove available ones Independent of the data model and application domain	Low reliability regarding confidentiality, integrity, and privacy, weak accuracy and precision		Open-source Mosquitto Visualization service not mentioned
Hellaoui et al. [87]	Energy conservation and yet secure Vast participation by tracking entities' attributes Deterred adversaries to alternate between forwarding a (un)authenticated messages	Not consider untrustworthy recommendations Not evaluated in lossy networks	HMAC MD5	Cooja, the Contiki OS simulator
Azad et al. [88]	Assess nodes' reputation: (1) Independent of third-person and stay away of: Single point of failure Be in middle of threat Privacy destruction (2) Use aggregated behavior-based weights (3) Encryption/decryption promise privacy preservation (4) Avoid fraudulent response by NIZK proof Security is ensured by Decisional Diffie Hellman Trust value is concealed and could not abused to derive relations Bandwidth and storage capacity of RSU is sensible Free infrastructure of physical layer and performed in session layer	Delay occurs for database exploration and caused by wireless connection among objects	NIZK proof CPU 3.6 GHz core i7, 8 GB memory	Java program
Yu et al. [90]	Lowers the energy usage due to trust exchange among adjacent members Ensures accuracy and minimizes recommended trust Obtains more robustness and adaptability Security of packets forwarding and defeating attacks	Assumptions: Densely deployed sensors are prohibited to move freely Communicate under maximum power Attacker intercept any nodes has communication capabilities as normal nodes The communication channel is symmetric		Simulation in MATLAB

Table 4 (continued)

Reference	Advantages	Disadvantages	Evaluation technique	Evaluation environment
Khan et al. [93]	Explored trust management on SIoT Define SCIoT Propose an attack model Classifies probable threats Highlighted relevant challenges	The proposed issue remains unresolved	Not implemented	
Ing-Ray Chen [94]	Dynamic trust management Accurate trust assessment or minimizing trust bias Maximize application performance totally distributed without the need for centralized entities	Not consider the thing-to-thing autonomous Social relation Disregard the caching usage to relieve constraint storage After status changes recommendations do not improve trust convergence		ns3
Dwarakanath et al. [95]	In decentralized sources, privacy-aware collaboration consumes less than 0.5% battery for execution	On–off adversaries lengthen delay in gaining trust values Combats collusion and on–off threats of a mischievous minority Not practicable for single device data		Google Nexus 5 smartphones CEPsim
Wang et al. [97]	Screens dishonest nodes Desirable convergence, accuracy, and resiliency Compared with P2P gives more accurate trust prediction and resists against collusion Resilient to ballot-stuffing, bad-mouthing Applicability in a hostile and noisy environments	The overhead for SOANET with constraint memory capacity Trust prediction takes minutes rather than seconds for less powerful node	Random Waypoint mobility (RWM)	MATLAB

Cloud computing

Vaquero et al. [71] asserted "clouds are a large pool of easily accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized Service Level Agreements." The notable characteristics of cloud include: (i) pay-per-use; (ii) limitless resources capacity; (iii) self-service interface; (iv) abstracted or virtualized object and resources [72]. Cloud network offers ubiquitous, on-demand access to shared pools of customized resources (e.g. service, servers, storage, platform, infrastructure) that conveniently provisioned with the smallest amount of management effort, often over the Internet [73].

To achieve the mobile crowdsourcing network Wang et al. [74] introduced SIoT as a sensing entity. To handle DDoS attacks by participants and security issues, firstly presented a trustworthy crowdsourcing model in SIoT to act as a provider and make a bridge over end users and sensing objects. Then the concept of social awareness is introduced by message forwarding algorithm and determining social data links. Furthermore, by means of reputation-based auction mechanism and distinguishing reliability and unreliability of participants, winner selection and payment determination are performed. Although the proposed algorithm concerned the only particular type of attacks, and even no practical evaluation is fulfilled in this regard but authors plan to expand its trustworthiness by auction based social awareness mechanism in the future.

To deal with low-power IoT nodes, Fortino et al. [75] described a cloud of things (CoT); virtualized physical devices over the cloud environment and integrated them with some software agents to carry out their responsibilities. Although taking advantages of software social attitudes for recommendation in case of information insufficiency to handle situation independently, nevertheless, successful contribution highly relies on counterparts' reliability. In this regard, they proposed a distributed CoT Agent Grouping (CoTAG) algorithm to configure agents based on mutual trust (local reputation, reliability and usefulness) and suitable voting. In the light of proper parameters and adequate number of participants, they demonstrated this algorithm's rapid convergence to fight off untrusted agents and computation overhead. To advance this field, they will specifically enrich proposed algorithm with knowledge extraction techniques by exploit Big Data source in IoT and carry out more trustworthy decision via intelligent analytics.

Fog computing

We are a witness of acceleration in the amount of generated data in IoT and demand for the real-time process in cyber-physical and autonomous devices, to satisfy this need fog computing emerges in IoT. Fog Computing extends cloud network and deploys resources close to the end user clients by utilizing edge devices, for example, routers, and smartphones while playing a role of gateway to the Internet. Fog networking architecture benefit collaboration between end-user or near-user edge components to deal with [76]:

- Edge area, and small latency
- Spatial dispersal

- Large-scale of sensor nodes
- Mobility
- Real-time/predictable interactions
- The superiority of wireless access
- Heterogeneity
- Interoperability
- Configuration
- Support big data, online analytic.

Other advantages of fog computing in contrast to the cloud are; a substantial storage space versus kept in cloud centers, communication versus routing through the internet, and decentralized management versus centralized control mainly by gateways. Due to the above mentioned specification, fog computing can well- supports the Internet of Everything (IoE) [77].

Garcia-de-Prado et al. [78] introduced a collaborative context-aware service oriented architecture (COLLECT). Since context-awareness is key on recommender systems, this approach permits intelligent decision-making and facilitates real-time integration of IoT heterogeneous data. COLLECT was formed of cloud and fog nodes, which preserve confidential information in fogs and process IoT data without submission into the loud. Despite advantages, this architecture has la imitation to deal with an extremely large number of events per second in the fog. As future work, authors firstly suggested intelligent decision-making extension by real-time prediction. Secondly, to compensate current work drawback, incorporate user profile and experience for finding similarity in world wide web. Last but not least planned to integrate their work with previous ontological taxonomy for context-awareness to facilitate decision-making in a graphical way.

Access control

Access control refers to the edge between users and intelligent entities, which assigns permission for resource usage among nodes and retrieves person and/or objects illegitimate interference in restricted zone by the identifier. On the other hand, it specifies who (subject) can do what (operation or right) on which resource (object). When designing an access control system for IoT environments, contributed parameters on its performance are: delegation, access revocation, granularity, scalability, time efficiency, and security [79]. Identity management and access control issues are vital factors is trust satisfaction. Alcaide et al. [80] declared two participants as a data holder and data collector related in a private manner. Data holders only feed specific target information to data collectors and on contrast data collectors acquire information after authentication and identification of legitimated data holders in the group.

Sfar et al. [81] introduced a roadmap overview of a cognitive and systemic approach, to move IoT security toward autonomous objects capability in perceiving threats and attacks. Security concerns are mostly detailed from privacy, trust, identification, and access control points of view and other relevant interaction such as auto-immunity, reliability, and responsibility were just taken into account via the design phase and hence neglected. Then a case study of smart manufacturing, technological lock, and standardization is debated to ensure the security in IoT. They illustrated Evolution of IoT

security requirements in three axes: (1) effective security for tiny embedded devices, (2) context-aware, adaptive and user-centric security, (3) Finally, they concluded that by the cognitive and systemic approach, the evolution of more autonomous objects in their environment intensifies security and privacy-related issues.

In this paper, Ouaddah et al. [82] provided an objective, models, architecture, and mechanisms (OM-AM) analysis of IoT authorization. They extracted usability, advantages, and disadvantages of already existing access control solutions. Literature over the recent years (2011–2016) are both quantitatively and qualitatively evaluated on the basis of the fourteen security and privacy- preserving goals. By observing open issues such as counterbalancing between autonomous edge node control and access control, namely centralized and decentralized approaches, they identified key future research directions as, (1) intelligent shifts from center to the end device, (2) decentralized authorization and access control in unreliable environment, (3) hardware-level security, (4) open source security in order to obtain adequate access control framework for IoT.

Despite centralized architecture advantages, Roman et al. [83] pointed out challenges such as obtaining interoperability, business model, nodes' authorization/authentication and multiple strengths and alternatively proposed a distributed approach where edge nodes collaborate with each other in a dynamic way to exchange information. Nevertheless, this architecture encompasses benefits as well, since intelligence is not concentrated centralized in platforms and hence they obtained additional scalability. To achieve privacy, information is managed in a distributed manner, with sufficient processing and storage capacity of nodes. Authors claimed proposed architecture is applicable in the real world since trust and fault tolerance mechanisms are taken into account. Beside all rational advantages, we believe both centralized and distributed approaches are inevitable for foundations of a full-fledged IoT.

Mahalle et al. [84] proposed trust based decision making in dynamic access control by using a fuzzy approach. For the trust calculation, FTBAC framework used the linguistic values like experience (EX), knowledge (KN) and recommendation (RC). These fuzzy trust values are mapped to get access permissions in a loT network. Authors in this paper demonstrated flexibility and scalability of FTBAC scheme, although the rapidly increasing amount of devices do not deteriorate its efficiency. In other word, compare to access control without FTBAC average energy consumption is less and residual energy is higher in FTBAC. Although scalability and energy consumption is simulated, the proposed scheme is already a mathematical model and real-time RFID and sensor implementation and integration with an adequate access control model are still missing.

End-to-end encryption (E2EE)

It is a communication system where only participants have permission to read the messages. The data being communicated or stored are surveillance of any deciphering attempt by third parties. Eavesdroppers—such as telecom or Internet providers, and even communication service providers—access to cryptographic keys is prohibited [85]. End-to-end encryption has advantages over point-to-point which restricts information decryption between two endpoints.

Sicari et al. [86] presented a lightweight prototype of a distributed middleware layer, named NetwOrked Smart objects (NOS), able to deal with scalability issue in heterogeneous interconnected devices, security threats, data quality while minimizing data caching and inside memory processing. They implied various algorithms to evaluate registered/nonregistered source trust level. Despite a validated solution, poor accuracy and precision, weak reliability, confidentiality, privacy, and integrity are undeniable disadvantages of proposed NOS. Future extensions include (1) consistent assessment in various IoT domains, (2) key management implementation in the platform, (3) observe behavior in the duration of nodes joining/leaving and on the existence of sensitive data.

Hellaoui et al. [87] introduced an adaptive security model in the IoT based on trust management, which hindered on–off attacks by tracing node's behavior as well as adapting cryptographic measures. By employing three complementary modules of experiences, observations, and recommendations, this solution disappointed misbehaving node to alter between forwarding the authenticated and unauthenticated message. Although the proposed method alleviated resource consumption, yet kept its security. For further development, a study on untrustworthy recommendations and more advanced research on low power and lossy networks are suggested.

Azad et al. [88] studied on a decentralized TrustVote, a privacy preservation system which computed nodes reputation without leaning on third-parties' trust and hence prevented occurrence of the same shortcoming in their design. Proposed reputation protocol took profit of homomorphic encryption/decryption system to mask interacted objects' ratings and just disclosed aggregated weights to participants. As a result, banned deducing relationships for hostile targets. Whereas some misbehavior nodes manipulated system's accuracy by appointing high scores on poisonous activities, this scheme recognized them as mischievous if they provide out of norm response. Experimental result displayed some delays due to message transmission between vehicles and retrieving reputation value, however, the authors explained since most reputation evaluation was fulfilled in RSU and distributed via network, their model's delay was because of database exploration and affected by quality of wireless connection among objects. The authors claimed a sensible communication and storage overhead happened through implementation which was trivial in contrast to worthy achievements such as decentralized prototype and its privacy. These points are taken as challenges and will be studied as future work.

Information entropy

The concept of information entropy was introduced by Claude Shannon in 1948. Entropy refers to disorder or measure of the unpredictability of the state, or equivalently of its average information content in a random signal or accidental event [89].

Yu et al. [90] considered a quantitative model of trust estimation, wherein direct trust of nodes is calculated based on the transmission capacity, repetition ratio, the reliability of content, delay, integrity, etc. To annul the impact of subjective trust evaluation in the previous methods, trust factor weights are measured by information entropy theory. Since attributes are not covered equally in decision making, Dempster–Shafer (D–S) evidence theory is employed to get indirect trust. By obtaining D–S evidence theory and acquiring recommendations of several neighbor nodes, they dealt with subjective

uncertainty in the trust mechanism and improved the accuracy of anomaly detection. Hence, authors afford to tackle malicious nodes by adopting subjective and objective trust simultaneously. They aimed to conduct more practical research in the future on power-efficient, lightweight trust techniques.

Intrusion detection system (IDS)

It is a software or hardware monitors systems and decides whether a taken action is a malicious activity/policy violations or legitimate use of the environment. Detection methods are categorized based on analyzer's characteristics:

- Knowledge-based intrusion detection: contains information about system vulnerabilities, when any explicit attempt of abnormality is recognized, an alarm is triggered, otherwise it is normal.
- Behavior-based intrusion detection: any observed deviation from the expected normal behavior of the system/user assumed as an attack [91].

Whereas most systems are susceptible to penetration also finding all deficiencies is infeasible, and secure systems are vulnerable to be exploited by insiders' privileges, so a real-time IDS is developed. Therefore, security violations model is inferred from following abnormal pattern exploitation: Attempted, Masquerading or successful break-in; Penetration, Leakage, and inference occurs in legitimate data; Trojan; Virus; Denial-of-Service [92].

Khan et al. [93] explored trust management in Social Internet of Things (SIoT) and compared techniques by outlining features and drawbacks based on eight taxonomies: Trust properties, trust metrics, trust computational model, trust information collection, trust evaluation, trust dissemination and malicious attack resilient. Further, the autors proposed definition of SCIoT as *"A Social Collaborative Internet of Things is a new paradigm that has strong ties with Social Internet of Things and is defined as a platform of IoT where smart objects work together socially through recursive interactions of knowledge by establishing social relationships with their surrounding smart objects aiming to achieve common/shared goals in order to benefit humans." Then a hierarchical model of collaborating, cooperating, communicating, and the community in SIoT was represented. Besides, they reviewed pros and cons in available studies and distinguished fifteen attacks in SCIoT. Further, they highlighted some challenges such as trust vulnerabilities, resources limitation, protocols' scalability, friendship and social trust, protecting owner privacy, service finding, quality of service (QoS) to be resolved later.*

Chen et al. [94] developed their previous study by a trust protocol in Social IoT. In order to satisfy accuracy, convergence, and resiliency, they utilized trust propagation and trust aggregation mechanism to associate first-hand (direct observations and own experiences) and second-hand (recommendations) information. Furthermore, they analyzed the compromise between trust convergence and its fluctuation and achieved honesty, cooperativeness, and community-interest in SIoT changing environment. In such a manner they minimized trust bias (the difference between subjective and objective trust) and also maximized the application performance. They evaluated the feasibility of the proposed trust protocol based on ns3 simulation. Proposed adaptive trust management

protocol is distributed and does not require any centralized trusted entity. However, the disadvantages of this scheme are lacks concrete implementation or abstractions that is essential for information storage or retrieval. For future research areas, they will examine trust management protocol's properties in a dynamic environment and explore statistical methods to exclude inaccurate recommendations from malign nodes to further enhance trust convergence.

To tackle data privacy in collaborative scenarios, Dwarakanath et al. [95] introduced a trust-based approach for distributed complex event processing (CEP). In order to robust towards collusion and on–off attacks, they leveraged the trust between users based on communication interactions history as well as trust recommendations by cosine-based similarity check. However, proposed trust management model overcomes aforementioned hinder only while adversaries are in the minority. TrustCEP achieves privacy-aware collaboration amongst, in contrast to privacy-negligent approaches with a negligible rise of 2–6% in battery consumption. Nevertheless, apart from privacy constraint, dwindled crucial factors such as resource availability and device mobility patterns are awkwardly blatant in this paper. Therefore, as a future work proposed approach should be implemented in a dynamic and mobile environment to evaluate operators' mitigation. Then the usability and practicability of the model will be demonstrated.

Peer-to-peer (P2P)

This networking is an architecture of interconnected nodes ("peers") which share resources amongst each other without centralized administrative system and partition tasks between equally privileged participants. Schollmeier [96] defined Peer-to-peer as "A distributed network architecture may be called a Peer-to-peer (P-to-P, P2P, etc.) network, if the participants share a part of their own hardware resources (processing power, storage capacity, network link capacity, printers, etc.). These shared resources provide the service and content offered by the network (e.g. file sharing or shared workspaces for collaboration): They are accessible by other peers directly, without passing intermediary entities. The participants of such a network are thus resource (service and content) providers as well as resource (service and content) requestors (Servant-concept)".

Wang et al. [97] developed a context-aware trust management model, CATrust, for service-oriented ad hoc networks, P2P and IoT. This design employed logistic regression to predict service provider behavior pattern in a changing context, rather than judging truthfulness based on satisfactory/unsatisfactory history in networks. By taking into account recommendation filtering mechanism and isolating dishonest nodes, CATrust achieved accuracy against colluded attacks, as well as validated convergence, and resiliency. The proposed model performs better than Beta reputation scheme with belief discounting and also adaptive trust management with collaborative filtering in terms of False negative and False positive probability. To ascertain applicability, these future work is suggested: firstly, validate CATrust practicality with real geo-distributed data gathered by PlaneLab, secondly, demonstrate CATrust utility by integrating to social P2P/IoT characterized with QoS and social variables, last but not least, assess CATrust resiliency against sophisticated noisy environments and certain mobility application and malevolent behaviors such as opportunistic and collision attacks.

The last sub-branch is *the Application layer*. This layer employs various scenarios or circumstances of the session, presentation and application layers in the ISO/OSI model, to establish a trust relationship between entities. These mechanisms deal with sensitive information in heterogeneous IoT environment and verify trustworthily and legitimacy of connected devices in a rapid manner. In this sub-branch, we analyze activities of communication management, continuous information exchange, collaboration, data translation related algorithms, source sharing, different libraries, and APIs, etc.

Service-oriented architecture (SOA)

It is a logical way of software architecture to supply services to either end-user unit or other distributed services by integrating reusable functional applications via well-defined interfaces(contract). SOA based IoT systems elaborates the following challenges: First, trust management protocols in IoT have to be scalable to accommodate the huge amount of limited capacity heterogeneous entities. Second, trust protocols for SOA-based IoT establish the accurate degree of trust by addressing joining/leaving characteristic of nodes. Third, Trust management explode social relationships of IoT device owners to enhance performance. Lastly, it must be resilient to self-interest attack of malicious nodes [98].

Al-Hamadi and Chen [99] proposed a trust-based decision-making protocol for information sharing among IoT health devices. A collective knowledge would enable an IoT device to combine data and decide on behalf of its user whether or not to enter a given place/environment at a given time for health-related issues. Despite available trust management protocols for a general service-oriented IoT network which only takes service providers' trust scores into consideration for decision making, a health IoT system concerns a patient's risk classification (cost) and the probability of health loss (payoff) as well. They achieved a resilient protocol against noisy sensing information gathered by devices either intentionally or not. This success is a result of trust computation mechanism which includes not only the location rating trust but also the rater's as well as witness trust score. In this work, they leveraged a centralized cloud of mobile IoT devices to derive different sources' trust ratings. In the future, they need to advance the case with a distributed cloud of IoT devices for storage and processing. Moreover, to overcome poor accuracy due to disregarding social IoT properties, P2P trust evaluation should be employed, then a trustworthy decision in IoT health environment is achievable.

Trust management

It is an abstract concept of assessing symbolic representations of entities trust and process of automated decision-making without human participation. In this sense, Josang et al. [100] asserted "*The activity of creating systems and methods that allow relying parties to make assessments and decisions regarding the dependability of potential transactions involving risk, and that also allow players and system owners to increase and correctly represent the reliability of them and their systems*". However, trustworthiness, irrespective of the actual entities identification, is demonstrated by their cryptographic credentials. Blaze et al. [101] defined it as "*a unified approach to specifying and interpreting security policies, credentials, relationships which allow direct authorization of security-critical actions*". Further, this definition and perspective on trust management were

expanded to include honesty, truthfulness, competence, and reliability and implemented in information security, specifically in the context of access control policies [102].

Kounelis et al. [103] adopted a Model-based Security Toolkit called SecKit to enable collaboration approach between citizens with the definition of privacy, agency and data protection, and manage security-relevant aspects. Lack of evaluation of trust related metric to illustrate the proposed idea is a blatant drawback of this work. Moreover, the authors conceded that the usability aspect of implementation includes user expertise and previous knowledge remains for the future.

In this survey, Yan et al. [104] indicated the role of trust management in IoT for data fusion, context-awareness intelligence decision making, achieving trustworthy and improving user privacy and information security. Authors classified trust properties into five categories of Trustee/Trustor's objective and subjective properties, and context and then concerned part or all of them for holistic trust management. Additionally, they categorized available studies in eight taxonomies and compared papers' versatility based on ten objectives of trust management. Although reviewed papers are mostly represented in conference and symposium and not published in the journal, which would be considered as a defect point, however, they found out open issues, deduced challenges and anticipated future research on solving mentioned points in Table 5. More investigations should be oriented on a practical application such as lightweight security and privacy solutions, power-efficient technologies, risk management, SMC.

Wang and Zhang [105], conducted a literature review on trust management in IoT with regard to pre-defined trust criteria such as: trustworthiness, adaptability, usability, privacy, accuracy, efficiency, uniformity, comprehension and generality. They pointed out some noteworthy open issues and challenges. For instance, they believed it is vital to construct a fully integrated dynamic security framework which handles scalability and heterogeneity in IoT environment rather than a single layer. As a future trend, they suggested to enhance lightweight security solutions, privacy and anonymity preservation, as well as corruption and authenticated key exchange protocol in mobile devices to overcome security and privacy vulnerabilities in IoT scenario.

Suryani et al. [106] conducted a survey of researches on different trust assessment methods in IoT. They categorized studies based on three dynamic, private and hierarchy object characteristics, also asserted trust related metric, types, as well as attacks' resistance. However, there where no contrast between methods' applicability. We think that the credibility of some studied papers are shallow. As a future trend, they mentioned green energy aspect as a big constraint in low capability IoT devices for trust calculation and briefly pointed out on trust and privacy correlation to achieve security in IoT.

Mendoza and Kleinschmidt [107] presented an IoT distributed trust management by direct interaction (discover neighbor and request service) and indirect observation (exchange trust table, assess recommendation and update score). Local trust calculation mechanism divided in 6 mathematical phases initiated with assigning negative/positive value to honest/dishonest nodes. Some disadvantages are higher network traffic and energy consumption due to higher update interval, otherwise this method will suffer of long delayed false diagnosis. They asserted with 10% to 30% of abnormalities, the strategy not only detected implemented bad mouthing attack, but may also recognize

Table 5 An overview of trust strategies for a recommendation in the Application layer of IoT

Reference	Advantages	Disadvantages	Evaluation technique	Evaluation environment
Al-Hamadi and Chen [99]	Flexible to noisy data captured either intentionally or not Trust evaluation regarding location rating, rater and witness trust value For trustworthy decision takes data and source trust into account Customized information concerning user trust measures	There is a centralized cloud for trust rating and lacks a distributed cloud of IoT devices for storage and processing Poor decision accuracy due to disregarding SIoT attributes for P2P trust evaluation		NS3 simulation
Kounelis et al. [103]	Promoting trust in human–IoT relationship: enhancing agency through "Rights in Design"	No metric evaluation Usability (user expertise and previous knowledge) not implemented	SecKit: model-based security toolkit	(MQTT) message broker SecKit GUI
Yan et al. [104]	Find open issues: Trust assessment disregards context awareness and trustor's subjective approach Lacks a comprehensive trust management framework DPT for capability-constrained WSN Power efficiency makes trust management less energy-consuming	Not considered: Demands for trust in heterogeneous IoT Challenges on SMC and homomorphic encryption improvement Human privacy and processes confidentiality Hard to control cloud Difficult to achieve trustworthy data fusion Incomplete privacy preservation DTCT was not associated with other TM Immature SMC research HCTI is almost ignored	No simulation	
Wang and Zhang [105]	Address IoT challenges: Lack of fully distributed, applicable security solution Few studies on privacy and anonymity Scalable and secure mobile trust	Lack of empirical evidence	No implementation	
Suryani et al. [106]	Categorize trust metrics, types, methods, related attacks	No comparison to demonstrate methods applicability Lack of optimal resource utilization		No practical result on direct/indirect trust formulas

Table 5 (continued)

Reference	Advantages	Disadvantages	Evaluation technique	Evaluation environment
Mendoza and Kleinschmidt [107]	Despite 30% of malicious nodes, trust model's performance is well Besides bad mouthing attack, may detect other attack types	Higher interval of trust table update, lowers anomaly detection time Frequent update results in higher traffic and more resources consumption Average time for assigning nodes a distrust is lower than trust	Unit Disk Graph Medium (UDGM) as radio model, ContikiMAC as radio duty cycle (RDC) protocol CSMA/CA (Carrier Sensor Multiple Access with Collision Avoidance)	Cooja simulator of the Contiki operation system Tmote sky nodes
Chen et al. [108]	Assessing organizations' reputation does not cost heavy load due to smaller number than nodes Avoid modification, replay and message dropping attacks and protect the integrity, authenticity originality and non-repudiation ORES well detect attacks in both scattered or dense dispersion of nodes	No investigation on badly behaved user and organization Skip over other types of attacks	Software-defined networking (SDN) technology	Not mentioned
Margaris and Vassilakis [30]	Stop too cold or hot venues for the users' likings or marginal arrival times Improved satisfaction and recommendation accuracy Incorporates any IoT-sourced species to suit domain needs	Not consider recommendation with a lower score than 5 out of 10 or didn't pass with the highest rating No representative demographics A limited number of participants Not consider keywords and tags		Data extracted by Facebook Graph API and Tripadvisor
Guo et al. [109]	Aggregates trust according to belief theory or regression Combine social trust metrics validate the defense mechanism Applies scalability, mobility, the social interaction for trust evaluation Combines centralized cloud with trust propagation Real-world IoT applications	Deals between accuracy and energy consumption	No simulation	

Table 5 (continued)

Reference	Advantages	Disadvantages	Evaluation technique	Evaluation environment
Bernabe et al. [28]	Considering security evidence copes with information vagueness Multidimensional approach Uses resilient and lightweight mechanisms Combined with DCapBAC access control	Rise in memory requirement by the number of devices to handle trust management Lack of a fully distributed approach Miss well-defined interoperable negotiation language		Android SDK Android Platform 2.3.3 (API level 10)
Kowshalya and Valarmathi [21]	Defys on–off selective forwarding threats Inspects vulnerabilities to identify and isolate untrustworthy nodes	Lack of participation opportunity for low trust nodes undermines all types of attack identification		Dataset from CRAWDAD NS3 SocNetV 1.9
Mashal et al. [114]	Recommend third-party services SMHSR combination of SR, MPSO, and OBCF algorithms Servrank (SR): Solve sparsity with high accuracy and low assessment duration Independence of contextual information	No publicly available popular big database not depict sensor localization and mobility	TagRec	Lightweight RESTful platform
Mashal et al. [113]	A formal model for the service recommendation in IoT	Still in beginning and in the data collection phase Hard to find a large-scale dataset	No simulation	
Atzori et al. [49]	Guarantees the network navigability Associates things and social network Trustworthiness leverages degree of friends' interaction Social networks models reused to address IoT	requiring continuous communication detects CLOR, CWOL, and SOR Reduce efficiency in resource discovery		Simulation in SWIM mobility simulator
Chen et al. [115]	Identifies that inherent limitations affect security and stability Timeliness tackles dynamic behavior in a distributed scenario Recommendation based on reputation or past performance, social transaction and energy	Lack of actual unstable secure network Not achieved mutual boosting in social relationship and access service recommendation		CRAWDAD data set

Table 5 (continued)

Reference	Advantages	Disadvantages	Evaluation technique	Evaluation environment
Lin and Dong [116]	Bilateral trust evaluation Infers Trust from historical task. Trust transited via intermediate node Update Trust with delegation effects Adjust trust with dynamic environments	Despite obtaining more trust than conservative, aggressive transitivity suffers from complexity and communication overhead	Radio Frequency for Consumer Electronics (RF4CE) IEEE 802.15.4, Zigbee	Facebook, Google+ and Twitter Texas Instruments' Z-Stack (version 2.5.0) CC2530 chip social networks simulator not mentioned
Nitti et al. [35]	Isolate malicious nodes Cope with dynamic behaviors Immunity against malicious nodes mistreating	An increased network traffic due to feedback information swap Lower credibility and malicious behavior on strongly relation nodes	Theoretical analysis	SWIM Brightkite dataset
Fernandez-Gago et al. [123]	Consider trust, identity, and privacy Requirements Taking into account dynamicity and evolution	Lack of extension of a modeling language to represent trust requirements Disregard functional requirements in architecture	Not implemented	Scenario: Field Service Teams (FST)
Ben Saied et al. [111]	Identifies a group of threats against the trustworthiness Proposes a proper partnership for cooperativeness Offers fine-tunes trust for erroneous witnesses	Trust level decreases the first time bad-mouthing threat occurs		Simulation by the TRM
Chabridon et al. [124]	Privacy and QoC: middleware solutions for context managers Confidentiality and QoC Choose QoC level is not easy QoC (change) is sensitive information	Not consider dynamicity and spatio-temporal condition of context-aware management	No simulation	
Tang and Meersman [125]	Not limited in types of components (either software modules or physical smart object) Combine algorithms	Not evaluate usability Only recommends parts defined by domain ontologies	ORM/ORM2 OWL/RDF(s)	Java J2EE/Eclipse SDK SDT editor Collibra studio
Chen et al. [112]	Minimizes trust bias Optimizes application performance Minimizes convergence time Minimum computation in the capacity-limited node for trust update	Only considered persistent attackers Only considered self-interest incentives		NS-3 network simulator

Table 5 (continued)

Reference	Advantages	Disadvantages	Evaluation technique	Evaluation environment
Ko et al. [29]	Improves recommendation accuracy in average precision by 28.87% Accuracy does not decrease by increasing data sparsity Overcomes data-sparsity problem	The tested dataset has lower sparsity than the actual one MCMLI is not scalable matrix Completion takes a lot of time Processing time rises exponentially by increasing the number of user/item	PREA recommendation algorithm toolkit	TripAdvisor and Yahoo! Movies datasets Eclipse Indigo Java EE Indigo SR2 and JDK 1.7.0_03
Chen et al. [126]	Good performance under a large density of malicious nodes Early discover nodes attitude alteration, produce desirable result on time-dependent attacks	For faster data transmission will substitute 5G with current IEEE802.11p Vehicles speed acceleration, cause more packet loss and let to drop precision and recall Drop in recall and precision due to high proportion of adversaries	Dempster–Shafer (D–S) theory IEEE 802.11p	NS2 Citymob mobility model SUMO
Tormo et al. [129]	Quickly chooses proper trust and reputation The smooth and automatic transition between the reputation computation engines More accurate reputation values than traditional models of only one reputation computation engine	Reputation engines have weak accuracy for some time after activation Costly interchange among reputation engines regarding accuracy, without transition time		ROMEO: ReputatiOn Model Enhancing OpenID Simulator
Nguyen et al. [130]	Used for all situations without relying on historical experience or recommendations No dependency on third entities Trust values are consistent	Other pertinent factors environment-specific are not considered	Not mentioned	
Ali et al. [131]	An automatic recommendation process Prediction accuracy and a precision rate of recommendation	Lack of irrelevant data filtering mechanism Deplete information retrieval of social network		T2FSs in MATLAB Protégé OWL 4.3 package reasoners: Pellet, Fact ++, Hermit "SWRLTab"
Mahmud et al. [132]	Less AECR rate depicts TMM anomaly identification ability Less energy consumption In data transmission	With 10 to 50% of adversaries, the throughput dropped due to malicious nodes disassociation in packet forwarding	Adhoc On-demand Distance Vector (AODV) routing protocol	NS2

Table 5 (continued)

Reference	Advantages	Disadvantages	Evaluation technique	Evaluation environment
Asiri and Miri [22]	guarantees better availability, no SPOF Conserves energy, adds the life span of battery devices, decreases maintenance expense, immediate response Lessens computation overhead for information transmission Protect against bad/good mouthing attacks	No implementation in reality	No simulation	
Al-Turjman [33]	CCFF outperforms due to learning elements, searching data, fidelity increases data publisher by Decreasing loads puts services/resources close to users in the edge Replaces cached data according to fog and user obligation Substitutes unemployed data according utility task	Edge nodes security problems, susceptible to untrusted data		NS3: fog node implemented in Golang

other common IoT disruptions, such as on–off and selective forwarding attacks. Albeit, scheme promotion to defend other intrusions was devoted to the future.

As a matter of fact, traditional trust solutions are not applicable in IoT because of extremely large number of heterogonous entities, restricted computation resources, dynamic environment, in addition, they are special purpose application which do not fit other schemes. Hence, Chen et al. [108] introduced an IoT trust architecture by adopting a cross layer authorization protocol and soft defined networking. In order to establish trust, they presented nodes behavior-based and organization reputation mechanisms. Both theoretical analysis and simulation experiments demonstrated this technique's efficiency against modification, replay, and message dropping attacks and protect integrity and authenticity, originality and non-repudiation with high accuracy. In ongoing research, they intended to validate this scheme in the presence of remainder mischievous attacks. Further, they will inspect its behavior in contact of well or badly behaved nodes in a ubiquitous system. Disregarding vicious users was one of the drawbacks of proposed model which will cause irreparable damages in collision with ill-treated organization. They noted this point as a future direction to avoid spreading fake reputation.

Quality of IoT services (QIoTS)

It promises "Only here, only me and only now" and implies that IoT devices respond to service requests by personalized service at a precise time and place. This purpose is primarily satisfied in the application layer of IoT, but however, it is much better to be fulfilled in other layers too. The QIoTS concerns both IoT services' (the trustee) objective properties and users' (the trustor) objective and subjective properties. Although both trust mechanism and QoS are obligatory in IoT they are inherently contradictive features. Seeing that trust innately restricts resources' availability to other services, while QoS strives to optimized the same recourse consumption in the environment [104].

Margaris and Vassilakis [30] presented a recommendation algorithm (combination of the QoS and the CF-based algorithms) in which IoT-sourced information is exploited. This was obtained by added value to WS information by considering: IoT-sourced data respecting the venues and user contexts, qualitative aspects, the semantic similarity and the influencing factors which were extracted based on the user involvement in social networks. A significant increment in user satisfaction and compatibility with any specific domain needs due to the generic framework was the benefit of this method. Constrained number of participants who are not a representative of demography is a drawback of this work, therefore, it is rational to draw more generalization in already obtained results. Finally, as a future work authors intended to envision descriptions of keywords and tags, along with users' explicit evaluation attributes to achieve more accurate recommendations.

Since feeble attempt have been distinguished on trust evaluation in IoT, Guo et al. [109] developed a classification tree on available trust computation models for service management regarding five fundamental design dimensions called trust composition, trust propagation, trust aggregation, trust update, and trust formation. They disputed the efficiency of defense mechanism against badly-behaving owners who aim to disrupt services. They debated on the efficiency of defense mechanisms against abnormal attacks intruding the trust system. Besides, they summarized the most, least, and

little-visited trust models in previous approaches, then highlighted eight research gaps that deserve adoption more investigation to overcome drawbacks. The rationale behind this study was to suggest a future direction to overcome malicious attacks in IoT trust computation.

Bernabe et al. [28] delved a trust-aware access control mechanism (TACIoT) that extended DCapbac and implemented an ARM-compliant security framework for IoT. Contrary to previous models that just concern reputation and feedback, this multidimensional approach takes four dimensions, i.e., quality of service, reputation, security aspects, and social relationships into consideration to make an authorized decision. Accordingly, to tackle the information vagueness in pervasive scenarios, a fuzzy logic-based monitoring system is utilized, which relies on and quantified by historical trust property evidence. They instantiated TACIoT by implementing software in a real testbed for constrained and non-constrained devices. The shortcoming of this model is indispensable domain experts' assistance for adopting fuzzy rules and knowledge incorporation based on input and output parameters. Further, due to lack of evaluation on accuracy and privacy in trust quantification, they envisaged continuing further experiment on identity management system to assure secure interaction and shared data within communities and bubble in a trusted way.

SIoT

The convergence of "Internet of Things" and "Social Networks" flourished SIoT paradigm that denotes the intelligent entities interaction within a social framework. Indeed, adopting principles of the social network in IoT brings up several priorities [110]:

- Although the SIoT members are mostly human handled, autonomous objects create relationships with "friend" objects with regard to their owner's control settings;
- A SIoT structure designed in a demanded format to assure navigability and scalability, object discovery, service performance efficiency analogous to the human social network;
- establish trustworthiness to leverage interaction degree among friend things;
- the human social model is applied on ubiquitous IoT interconnected objects network.

With the pervasiveness of human to human, human to the thing and thing to thing relations, SIOT emerged where objects are both more intelligent and also socially conscious. In this regard, trust is as a vital aspect for establishing reliable autonomous communication. Kowshalya and Valarmathi [21] proposed a dynamic trust management model to evaluate trust on the basis of Direct observation (First hand or Direct Trust), Indirect Recommendation (Second hand or Indirect Trust), centrality, energy, and service score. This model is defendant against On–Off selective forwarding attacks. Simulation results depicted its surpass towards the fuzzy-based [46], Context-aware [111] and SOA-based [112] trust in terms of accurate detection and trustworthy communication. Authors calculated a victim node trust value by the cognizable equation, while fell down below the threshold, identified as untrustworthy nodes and isolated from the network.

Nevertheless, prohibited low trust value nodes will weaken attacks detection. To overcome this drawback, the authors proposed to elaborate further performance opportunities on the low trust value nodes. They Adhered their model's ability to learn the attacker's pattern and detect intrusions.

Mashal et al. [113] introduced a formal model for the concept of service recommender systems in IoT based on undirected weigh tripartite graph. Alongside, Mashal et al. [114] investigated the possibilities of correlation graph-based recommendation in IoT to connects users, objects, and services. They explored correlations between various algorithms on IoT Service Recommendation (IoTSRS) in terms of recall/precision metrics. Moreover, Simple Multiplication Hybrid Service Recommendation (SMHSR) combines three recommender algorithms SR, MPSO, and OBCF. Despite achieving higher performance, features such as sensor mobility and localization of sensor interaction were not taken into consideration.

Atzori et al. [49] demonstrated the possibility of creating a navigable social network of objects similar to the human network by employing the individual's behavior inspired approach as well as establishing and managing social relationships (POR, C-LOR, C-WOR, OOR, and SOR) under appropriate policies. Furthermore, they implemented a three-layer SIoT architecture of sensing, network, and application layers by relevant functionality such as objects, gateways, server, etc. They analyzed characteristics of SIoT statistically and asserted strength points, (e.g., integration with short distance communication technologies, interconnection separate networks and limited communication and/or computing) and weakness of architecture (e.g., in SIoT-enabled and lessening efficiency in resource discovery due to navigability over trusted zone). Thereafter, the objects' mobility traced through the SWIM simulator. To illustrate paths between nodes they proposed a comparison on achieved data mobility traces versus those stored in CRAWDAD, in addition, a further detailed investigation on relationship parameters and their maintenance procedure remains for future research.

Recently Social IoT (SIoT) Paradigm is flourished by imperceptible relations between human and devices. However, rapid growth in IoT service and necessity of heterogeneous objects' frequent collaboration has led Chen et al. [115] to present access service recommendation scheme for promoting service discovery and composition as well as resisting against malicious attacks in SIoT. Authors depicted the dynamic behavior of scheme in three environments: (1) malicious node population growth, (2) fast membership alteration, and (3) inconsistent behavior. The authors enhanced dynamic performance by integrating timeliness properties of transactions and energy-aware mechanism while addressing trust evaluation related issues in SIoT for instance, inherent resource constraints, vulnerability factors which affect the security and stability of IoT. Moreover, the recommendation was evaluated not only based on direct and indirect reputation but also on the basis of social relationship which reflects predictive validity of a given node by others, and current energy status of nodes. They demonstrated the benefit of object's social relationship in three-facet of accuracy, dynamic behavior, and network stability. However, the proposed scheme's advantages were not proven under secure manner in an actual distributed network, more importantly, promotion of both social relations and access service recommendation systems in SIoT cannot be achieved simultaneously.

Lin and Dong [116] put forward an SIoT tailored Dynamic trust consists of 6 fundamental factors i.e., the trustor and trustee, context, trustworthy estimation, object, resolution, and its consequences. Peculiar characteristics of SIoT trust designated to deal with currents models' difficulties: (1) bilateral protection of the trustor and trustee, which examine each other on four aspects of success rate, gain, damage, and cost. (2) infer trust by exploring historical features, (3) two schemes of conservative and aggressive transitivity, (4) update trust with delegation results of both positive and negative factors, and (5) modify with influence of dynamic environments. In spite of the enhancement in number of trustors' possible trustees in aggressive transitivity, this success burdens a cost of complexity and communication overhead for interrogating more nodes. Treating with vicious behavior in hostile environment will justify its relatively hard rational construction. Therefore, we can name it as a cost and gain strategy.

Butt et al. [117] made an effort to design a Social Internet of Vehicles (SIoV) paradigm on the basis of Restful web technology. Their intension was to take benefits of SIoT, intelligent transport system and VANET (Vehicular Ad hoc Network) technologies to develop semantic interoperability and scalability in their proposed layer architecture. In this respect, they emphasized some available and future challenges i.e. decentralization, security, safety, privacy, energy and resource management, quality of service, dynamicity and etc. and introduced use case scenarios to analyze its usability, however, no analytical experiment draw attentions in this paper.

Distributed hash table (DHT)

It is a class of a decentralized hash table that provides functionality i.e., insertion and retrieval of key-value pairs. Each participating node stores a part of the hash table and recovers the associated value of a given key. Responsibility for key delivery lookup and key insertion requests from the requestor to storing key node is distributed among the participants so that a change in the set of nodes results in minimum disruption. This allows a DHT to extend a massive number of nodes and deals with constant node's arrivals, departures, and failures [118].

Nitti et al. [35] inspected the social relationships of IoT device owners to obtain trust. They envisioned on trustworthiness management in SIoT by proposing two possible schemes, namely objective and subjective models, for improving networks scalability in information/service discovery based on the behavior of the object. Subjective trust model obtained from a social network, where each node evaluates its friends' trustworthiness according to its own experience and a chain of friends' opinion with potential providers. The objective model derived from P2P scenarios, where a DHT structure is deployed for storing and retrieving information about each peer. Although required information by the objective model is available to all nodes but is only run by pre-trusted nodes, which is questionable in IoT environments. The major con of subjective approach is a longer transient response due to dynamic behavior, but immunity against the risk of mistreating nodes based on relationships compensate this drawback. However, objective approach suffers this behavior, since it uses feedback from both malicious and benevolent nodes to calculate trust score. These methods inject a lot of throughput to the entire network due to storing the extreme amount of data, which burden on battery life due

and memory capacity. In addition to the above-mentioned notes, social relation promotion by improving trustworthiness will be considered for future works.

Context awareness

Dey [119] definition for context is well-known, where "Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves"; Context is unique information of each user or system and can not be generalized in a different thing.

Furthermore, Dey [119] depicted "*A system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task*". In fact, a context-aware system utilizes obtained information from its environment; that is, location, time, social attributes etc. to anticipate system's demand and adjusting its behavior to those specific requirements [120]. Context awareness is a fundamental aspect for making a decision generally and for real-time decision particularly [121].

Henricksen and Indulska [122] identified four imperfect types of context information:

- *unknown* when there is a lack of information about it.
- *ambiguous* when there are contradictory reports from different sources.
- *imprecise* when the reported information is true but the precision degree is inexact.
- *erroneous* when there is a conflict between the real and reflected states.

This context information is obtained from three principal sources: sensor devices, human and derived from other information types.

Fernandez-Gago et al. [123] proposed a dynamic framework to overcome the lack of certainty while focusing on trust, privacy, identity, and two main challenges includes interoperability and dynamicity/evolution which are functional requirements to derive holistic solution on trust and reputation management in the IoT scenario. A bottom-up approach manner architecture was exploited for building a framework comprises of different layers of scenarios, requirements, services, trust framework layers. Further, a field service team (FST) was utilized to depict the scenario and a use case to exemplify IoT applications. Ultimately, the implementation of framework concerning intermediate and services left to future work. However, authors already provided some initial hints namely privacy and identity of context which are substantial for trust management.

Saied et al. [111] addressed the weakness of prior approaches such as CONFIDANT and CORE which assess trustworthiness just based on single function and disregard past experiences of other functions, or other methods which derogate heterogeneity essence of an object by falsely re-arranging previous experiences into one metric. Therefore, the authors designed a context-aware and multiservice trust management system (TMS) for the IoT to alleviate deficiencies in the heterogeneity of objects, fault tolerance, service allocation, etc. Their model gave the node a dynamic trust value based on past behaviors to accomplish a required task in cooperative service and then induced most appropriate partners for assistant in sought cooperative service. Each simulated node was characterized and trust was updated by means of quality

of recommendation (QR), which was used to count the node's trustworthiness while rating others. Equally, by ending each interaction and during learning phase it was fine-tuned. Authors claimed that proposed system isolated common intrusions which targeted TMS.

Chabridon et al. [124] analyzed privacy techniques for context-aware management in IoT and highlighted three main hinders in IoT while managing privacy and quality of context (QoC), namely context data production and consumption decoupling, QoC-aware privacy, interdependency of QoC and privacy. Along with context data chain, authors indicated the necessity of policy languages to tackle anonymity and equally important to protect data. They discerned users' urgent demand for transparent privacy solutions in order to rely on IoT perspective. As future direction research on dynamicity, the spatiotemporal condition of knowledge and context management, security and privacy are inevitable.

Tang and Meersman [125] introduced DIY-CDR an ontology-based strategy to deliver recommendations which match users' preferences, needs, and hopes. Besides, authors developed the C-FOAM matching strategy with levels of string matching levels algorithm, a simple lexical matching algorithm using WordNet, and a graphical or conceptual matching called LexMA. Authors claimed that no constraint imposed on components which can be either software modules (e.g., web services and plug-ins) or physical object (e.g., sensors and chips), and restriction for plugging in a new hardware was solved by adding concepts in ontologies of domain, moreover, they comprised several algorithms to obtain matching results. However, SDT editor and DIY-CDR usability evaluation, as well as investigation on other modules in Onto-DIY with the capability of spontaneous annotation in accordance with the component description, remains for future.

Collaborative filtering (CF)

This method makes automatic predictions (filtering) about user preferences by capturing opinion or taste from other users (collaborating). CF constitute of (1) users' participation, (2) represent users' interests, (3) match people with similar tastes and (4) recommend highly rated items by similar users. Collaborative filtering approach is two types:

- *memory-based* two algorithms are used to calculate similarity:
  - *neighborhood-based CF* produces a prediction by weighted average ratings. Multiple measures, for instance, the Pearson correlation and vector cosine similarity is utilized;
  - *item-based/user-based Top-N recommendations* similarity vector is used the K most similar users' identification and provides a recommendation by user-item matrices. Locality-sensitive hashing employed in this regard;
- *model-based* uses different machine learning algorithms to predict users' rating of unrated items.

A key issue in collaborative filtering is how to add-up and weight the user neighbors' preferences and how immediate and accurate the ratings are.

Chen et al. [112] introduced an adaptive and scalable trust scheme for service composition applications in SOA-based IoT. They utilized a distributed collaborative filtering technique to get trust feedback using three social similarity level, i.e., friendship, social contact, and community of interest to weigh recommendation. Further, they adjusted node weight parameters for combining direct trust and indirect trust dynamically, Authors claimed that proposed method can cope with intrusions such as self-promoting, bad-mouthing, ballot-stuffing, and opportunistic attacks and lessen convergence time or trust bias. To achieve scalability, authors suggested a storage management strategy, whereas a limited capacity node needs to keep a subset of trust value and hence trust updated with minimum computation effort. In addition, the authors utilized a trust decay for removing outdated trust and further depicted the efficiency of proposed trust management protocol against Eigen Trust and Peer Trust. Nevertheless, a drawback of Bayesian probability based framework is that trust value is directly assessed on user satisfaction experiences and is not integrated with context.

Ko et al. [29] developed a multi-criteria matrix localization and integration (MCMLI) by CF-based algorithms to improve the accuracy of users' preferences prediction by mitigating the effects of data-sparsity. Firstly, MCMLI split a user-item matrix into submatrices (CUIS matrices), by clustering correlated users and items based on their similarity level. MCMLI then predicts user ratings on each item regarding the CUIS and aggregates the predicted ratings by assigning weights to criteria with respect to user's dependency. Whereas, matrix completion is a time-consuming process, equally increasing number of users and items enhances time complexity exponentially, so authors suggested Bayesian non-parametric matrix localization method, which does not oblige any advanced information for performance improvement. To overcome the scalability problem, investigating on MapReduce is proposed which enable processing on a cluster of numerous computing nodes concurrently.

In order to attain fundamental objectives of vehicular networks, such as, quick discovery of dishonest behaviours and information reliability, Chen et al. [126] developed an evidence based security scheme by employing local direct trust as well as indirect trustworthy recommendation of collaborative filtering. While highly accentuating on short time distinguish period, they took benefits of central IoV cloud, vehicular social relationship, user preference and geographical location to offer personalized application and more confident message propagation. They conducted theoretical test and simulation scenarios to illustrate better resistance of this methodology in presence of bad-mouth, selective-behavior and time-dependent attacks, particularly under large number of high speed adversaries. Even though, they confronted with some hardness in untrusted data proliferation as a reason of more packet loss. They aimed to study how internet of things can assist for inclusion of remote isolated vehicles into IoV society.

Fuzzy logic

Whereas Humans think rather in vague qualities terms, a quantitative measure like probability is often inadequate or misleading. To handle uncertainty and ensure information efficiency, the fuzzy inference was adopted [127]. The fuzzy approach benefits vague linguistic terms, i.e., low security or high reputation. Fuzzy represents of human knowledge about involved variables dependency and relations. in the following manner,

fuzzy logic perfectly comes up with aggregated subjective trust values about a given smart object [128]. Due to the fact that required computation resources for running a fuzzy system are small, fuzzy rules quantify final crispy trust value in the IoT world.

Despite old philosophy of rigid trust computation approaches, which hinder dynamic adaptation to the present conditions and oblige system administrators to choose the most suitable reputation model manually, Tormo et al. [129] designed a trust and reputation identification model on-the-fly, by taking both the current state (users, dedicated resources, etc.) and the expected performance values (accuracy, robustness, scalability, etc.) into consideration. This mechanism is able to substitute active reputation engine with idle one, whether to recognize its better outcomes than an active one. Additionally, the smooth transition among different computation engines is guaranteed, in order to avoid sudden changes in the reputation scores. OpenID Simulator demonstrated this solution outputted more accurate reputation measurements in contrast to the traditional model where merely one reputation computation engine is performing. As future work, they have foreseen research on making interoperability easier by standardization of reputation computation engines within the selection mechanism. Moreover, to prevent inefficiency of the framework, they work to help administrators in the process of defining the inference rules auto-adaptively.

Nguyen et al. [130] introduced a concept of personal space IoT and challenge-response trust assessment which evaluates the trust level of the device before admitting their participation in the space. In this model historical interaction, the previous encounter between two entities or existing trusted recommendations of third parties is not required, rather uncertainty of device behavior is measured via entropy to make trust/distrust decision. Authors demonstrated feasibility and consistency of the proposed scheme. Although, comprehensive exploration of various pertinent parameters is deprived, yet as future work, concurrent utilization of challenge-response trust assessment schemes with direct/indirect trust is advised to improve the accuracy and robust operational environments.

Ali et al. [131] automated patients' risk factor detection by type-2 fuzzy logic and fuzzy ontology-based semantic knowledge. In the presented system, health condition is extracted via wearable sensors. The authors enhanced prediction accuracy and a precision rate of recommendations by a combination of T2FL and the fuzzy ontology. To defeat encountered deficiency, authors planned to explore neural network with type-2 fuzzy ontology-based semantic knowledge and facilitate information retrieval from the social network, as well as filtering irrelevant data by support vector machine to intensify disease diagnosis.

Mahmud et al. [132] came up with a Brain-inspired trust management model to develop a reliable end-to-end (E2E) communication in cloud based IoT architecture. For this reason, they employed both data and node behavioral trust by applying adaptive neuro-fuzzy inference system (ANFIS) as well as a weighted additive technique and demonstrated trust model's productivity with Packet Forwarding Ratio, throughput, Average Energy Consumption Ratio and accuracy via simulation. In order to improve communication security in neuroscience applications, they suggested to advance with Bayesian statistics, Deep Learning, and Reinforcement optimization techniques in distributed block chain IoT architecture.

Probabilistic neural network (PNN)

It is a feedforward neural network often used in pattern recognition and classification problems [133]. A four-layer neural network i.e., input, hidden, pattern, and output layers can map the input pattern to any number of classifications by Bayesian network algorithm with highest posterior probability. PNN advantages are (1) easy and instantaneous training, (2) a significant speed enhancement in comparison to back-propagation, (3) decision boundary can become as complex or as simple as necessary and et cetera [134].

Asiri and Miri [22] proposed trust and reputation-based recommender system in IoT that utilized PNN. It was carried out on IoT edge devices and aimed to differentiate trustworthy and malicious nodes. By taking advantages of collaboration across IoT community devices, id est. rating prediction for newly joined devices on the basis of learning and their characteristics, it tackles cold start problems. The advantages of this model summarized as: (1) processing is handled by the nodes themselves, (2) there is no single point of failure and guarantee better availability, (3) fits any types of IoT devices and it is not designed for a certain context, (4) minimizes calculation overhead publicly available information, (5) provides a level of security in accordance with transmitted data sensitivity and consequently, (6) protects against bad mouthing and good mouthing attacks. However, the blatant defect of their job is the lack of practical implementation.

Content-based filtering (CBF)

This method uses discrete attributes of an item and a user preference profile to suggest extra items with equivalent properties [135]. In this method, items are described by keywords and content-based user profile are created regarding a weighted vector of item features, which indicates the importance of each feature for the user. Variety of techniques are involved to compute these weights. Consequently, it recommends best-matching items that are similar to those a user previously liked or is consuming now [136]. However, content-based approach suffers from the over-specification problem.

Al-Turjman [33] investigated a value exchanged based caching framework, called Cognitive Caching approach for the Future Fog (CCFF), used in fog and Information Centric Sensor Networks (ICSNs), where retrieved sensing data at the network edge. Discrete event simulations in NS3 and case studies examined to compare CCFF framework with other dominant management categories; for instance, node functionality-based caching (FC), content-based caching (CC), and location-based caching (LC) techniques under variety of parameters such as cache level, data publisher load, connectivity degree, and popularity. CCFF targeted the delay-tolerant caching requirement in the edge of Fog network. In addition, trust analysis and fidelity were as well addressed to accentuate the efficiency of CCFF in Fog, where edge nodes are under threat of improper data from the authorized entity in the cloud. In the end, proceeded in the matter of time required to retrieve data and experienced from publisher load.

Discussion and statistics

Papers published in a conference or national journals, textbooks, masters and doctoral dissertations, technical reports, editorial notes, web pages, and unpublished working papers were removed from consideration because practitioners and academics mostly refer to journals for obtaining information and spreading new findings.

In order to explore publication trend in recommender system from the advent of IoT and answer RQ1, an SLR of 206 articles till the end of December 2018 was adopted and extracted 59 articles among 206 journal article studies. However, in the period of investigation, we encountered some conference papers which embraced valuable contents in this regard. Hence, due to the novelty of this topic and fragmentary information as inference document, we made a note in initial selection provision and ultimately enfolded them in our database. This search process evolved four electronic databases, IEEE Xplore, Springer Link, Science Direct and Wiley Online Library, which we found them better-engaged pee-review and rich content articles. The mainstream in a published article is depicted in Fig. 4. This bar chart apparently reveals an upward rise in studied subject, especially in recent years.

To address second question RQ2, we had careful scrutiny on reviewed articles, and categorized all of the proposed or applied approaches, as mentioned in "Recommendation mechanisms based on IoT architecture" section, based on three fundamental layers in IoT. With respect to Fig. 3, the largest amount of researchers' attention focused on the application layer and its subcategories. This conspicuous difference has carried upon paramount importance of trust in recommendation; an IoT device relies on its socially connected devices (of the owner) over unrelated or unknown devices. This concept is visualized in two IoT scenarios: The first scenario is where objects actively cooperate with each other to achieve a common goal with human intervention; there, trust either derives from owners' social relationship and device trustworthiness is evaluated by its

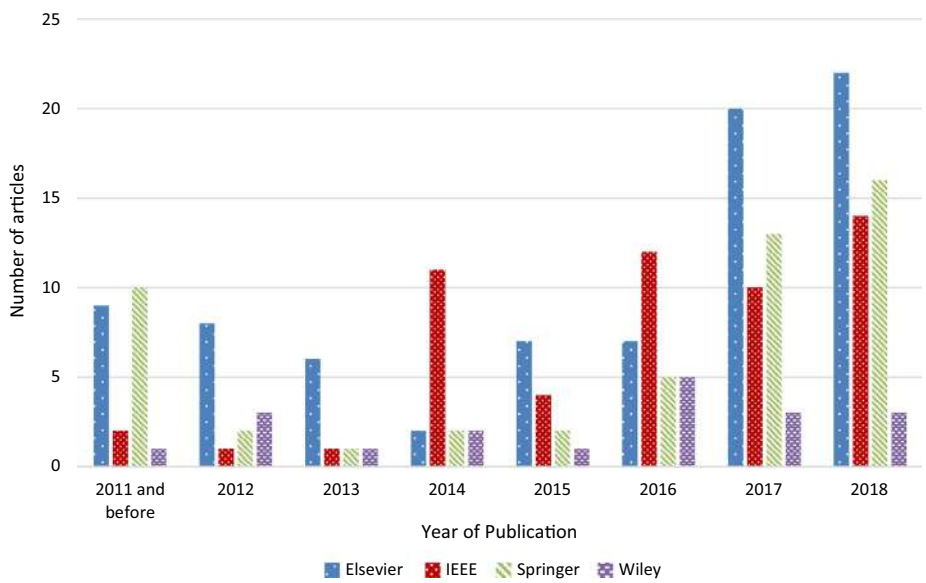

Fig. 4 Articles distribution over time including Elsevier, IEEE, Springer, and Wiley

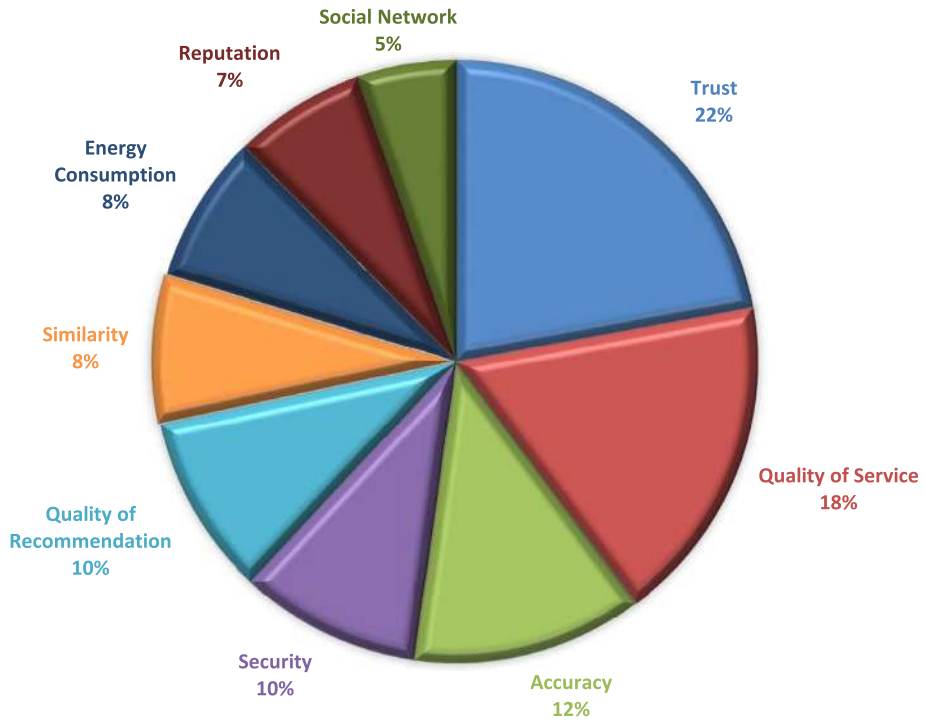

Fig. 5 Distribution of evaluation factors for a trustworthy recommendation in reviewed articles

capability to fulfill requested service or intention and goodwill to commit request service. The second scenario is where objects are autonomous and establish relationships among themselves in-network for collaboration and making a decision.

To answer the third question RQ3, and achieve a clear understanding of this research objective, the initiation step is to classify goals and policies in previous literature. Via rigorous attention to details, we acquired nine momentous parameters based on their number of occurrence in literature. Figure 5 which depicts the distribution of trust computation techniques among reviewed articles. It is as well asserted in Table 1 that with regard to researchers' predefined significance and priority, some parameters could be taken into account by some while simultaneously could be neglected by others. It can be inferred from Fig. 5 that the highest concern can be seen in trust convergence and accuracy of recommendation; the third most important attribute is quality of service (Interaction, Availability, Throughput, Delay, Bandwidth, Packet Loss, Overhead, reliability); the next place is allocated to prediction accuracy, then security (AuthN-AuthZ-System, Availability, Confidentiality, Integrity, Intelligence) and similarity (friendship-social contact-community of interest), respectively.

We survey the literature on current trustworthy recommendation techniques in IoT. In this respect, we reviewed quite a number of journals and conference proceedings to denote an exquisite their categorization. We classified the available mechanisms into twenty-four subcategories. Meanwhile, the result of the unbiased review on each studies' weakness and strength are summarized in Tables 3, 4 and 5. Unfortunately, the

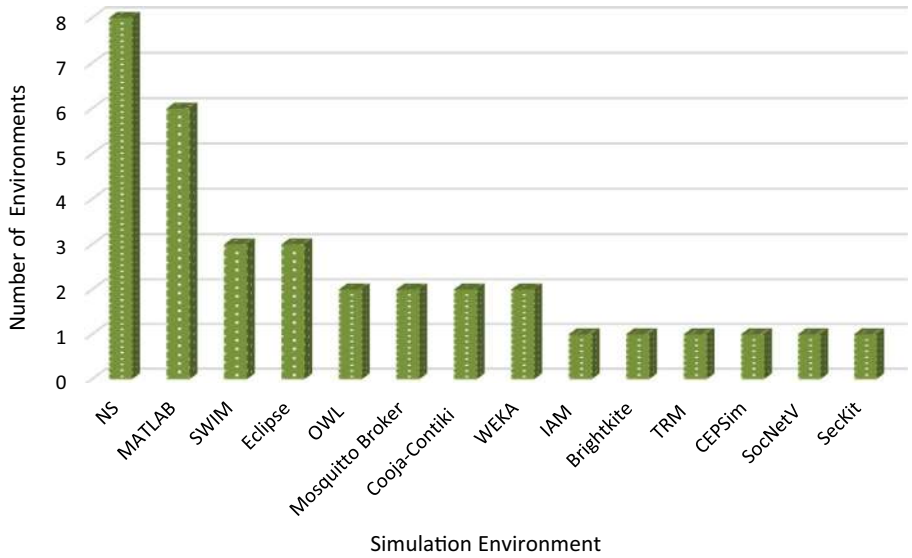

Fig. 6 Distribution of simulation environments over reviewed articles

number of available datasets to all in IoT domain is very low and hence, due to constraints in accessing realistic resources in IoT networks, simulation is the most convenient approach for evaluation hypothesis and validating their integrity. Researchers have occasionally utilized a synthetic generator. In this regard, Fig. 6 illustrated employed simulation environments in reviewed papers. By this way, we identify MATLAB and NS as the two most commonly utilized trust simulation environments in IoT. According to pertinent findings in Tables 3, 4, 5 and Fig. 6, reviewed articles rather exploited simulation environments to evaluate the proposed mechanism. Therefore, another fascinating future study would be an exploration in large-scale and resource-constraint IoT scenario with real data.

Albeit obtained responses for forth research question, RQ4 is not thoroughly promising. To debate forth question and the efficiency of synthesized evidence; corresponding literature review demonstrated priority of trust computation accuracy of recommendation. Moreover, by precisely concerning on the application layer of IoT and corresponding techniques such as service-oriented architecture, collaborating based or content-based filtering, fuzzy logic and social relationship between IoT entities, we can deduce that establishing more accurate and trustworthy recommender system in IoT virtual space is more feasible. Meanwhile, it is manifested that trust parameters and relevant factors have not yet been studied comprehensively in IoT scenario. To fill this gap, rigorous analysis of this field is of predominant importance.

Threats of validity

In spite of our attempt to assure quantitative or qualitative adequacy of this representation, it might still endure some indisputable bias and limitation. As an inference from this fact, any future interpretation or conclusion of this review should bear in mind below points:

1. Data extraction is performed based on search string and by manual inspection. Due to human mistakes, we could not guarantee to select all applicable studies or contradict any possibility of overlooking, however, our attempt is to lessen this impact by multi-review.
2. This research is a constraint to analysis the four most reliable electronic databases. Although statistics indicate on including the most credible and relevant articles, the possibility of escaping comprehensive content articles is disputable.
3. The recommendation in IoT environments covered in diverse domains, i.e., books, academic publications, editorial notes, etc. Our research scope only includes articles published in major international journals and omitted almost all conference proceedings papers. Also, articles that are more probable to study other IoT fields rather than recommendation or trust are not considered.
4. Although we have had a quick look at papers before 2011, due to lack of time, our dataset mostly encompasses papers from 2011 up to December 2018.
5. Non-English papers were not included.

In this paper, we attempt to present major recommendation issues in IoT which yet have not been thoroughly addressed from the trust aspect. By analyzing relevant studies, we observed that there is not an individual technique to involve entire recommendation metric, besides, some metrics cannot be seen mutually exclusive. For example, quality of recommendation and trust are both vital features in IoT, which inherently conflict. Trust evaluation mechanism innately entails operation that is recourse expensive and limits recourse availability, whereas the recommendation characteristic is to optimize those recourses utilization. We should seek a trade-off between optimal resource utilization and maintaining needful trustworthy recommendation.

Open research issues and future direction

Although pertinent findings in Tables 3, 4, 5 demonstrate significant developments in IoT trust evaluation, we identified several hardware and software challenges which remain unsolved due to heterogeneity essence and incremental growth in the number of IoT nodes. In Fig. 7 we illustrated some noteworthy direction for researchers to tackle current challenges in building trust-based recommendation in IoT and alleviate these demands in future architecture.

To answer RQ5 question, some challenges facing by previous researchers and studies [137] during recommendation in IoT are described below:

A. *Security and trust management*

It is unlikely to tackle IoT concerns, for instance, secure processing of heterogeneous data or avoiding malicious intrusion, unauthorized entry and negative hostile activities with a single security architecture. For this reason, a distributed among layers' solution should be introduced by monitoring behavior pattern of objects, encryption

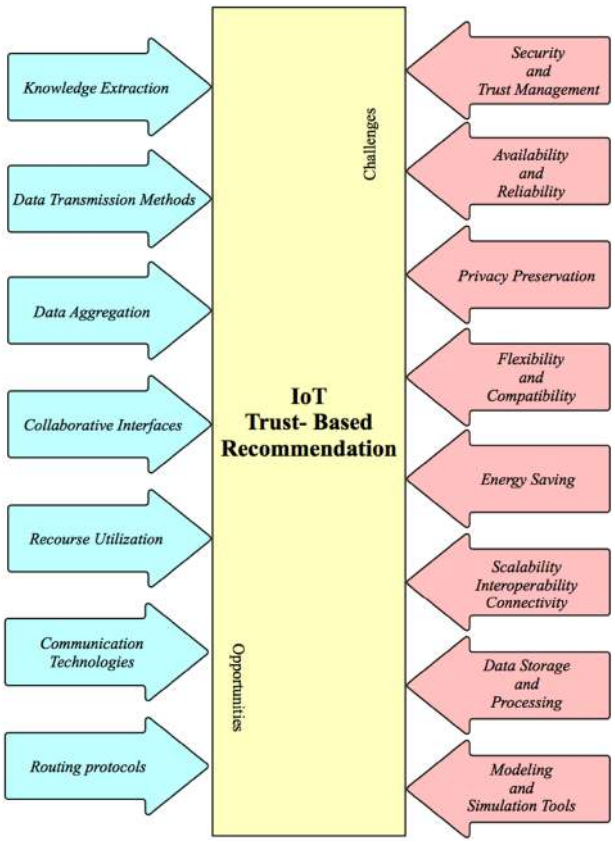

Fig. 7 Challenges and opportunities

algorithms and data mining methods, etc. Some future issues to deal with these challenges are:

1. Lightweight security:
   Due to small scale, low-capacity and context of IoT objects, lightweight solution would satisfy the authentication, access control, trust and key management requirements.
2. IoT mobile security:
   Based on mobility characteristic of mobile RFID system, maintaining a secure location update and probable vulnerabilities is of value. To come up with a solution, trust management, reads/tags corruption issues, multiple readers authentication and key exchange techniques should be included.

B. *Privacy preservation*

As a matter of fact, to enhance public confidence and promote privacy and anonymity requirements in dynamic IoT environment where vulnerable objects and sensors easily targeted of various threats like data exploitation, etc., using a pseudonym rather than plain ID for IoT objects and legitimate user communication allowance can mitigate probability of attacks. In addition, due to correlation of trust and privacy, trust evaluation mechanism will make a great assist in this respect.

C. *Energy saving*

Green energy in a major challenge for trust evaluation since most IoT objects are tiny wireless limited capacity devices. Low computational lightweight trust assessment model will be developed in this respect. By providing energy efficiency and maximizing resource utilization, we could alleviate node substitution requirement and optimal resources allocation.

D. *Flexibility and compatibility*

We rather concern compatibility issues of non-unified cloud or diversities in firmware rather than heterogeneity nature of devices in IoT environment. To deal with these barriers specialized hardware, storage and operating system might incur performance but will expand device capabilities with novel features and address interoperability and interdependency of the heterogeneous device without adding extra complexity.

E. *Scalability, interoperability and connectivity*

Scalability is a system property to handle increasing number of devices or resources while keeping their interoperability and avoid any performance degradation. To address this aim, firstly, a multi-layered IoT architecture must be sketched. Then, use cloud platforms as giant centralized storages and computation sources. Thirdly, a fog computing will carry out substantial amount of loads in edge nodes. Although distributed method is energy efficient, suffers from inaccurate content dissemination, limited capacity and deficiency in saving historical information. Another key challenge is supporting topology adoption for faultless connectivity of new components. Content-Centric Networking, a growing paradigm, will assist in this respect.

F. *Availability and reliability*

IoT availability implies seamless cooperation of authorized services through coverage space despite some current obstacles:

1. A major IoT concern is security; to defend system against attacks, unattended activities and unintended breakdowns. Some current solution like exploring vulnerability during software implementation or cryptography mechanism aid in system safety or avoiding extra cost.
2. Mobility and location awareness are other important points; a solution is adopting mobility management in IPV6 communication protocol and trust deployment among agents. Equally, proper routing protocol for low power lossy networks with simultaneous consideration of context, quality of service can support availability in IoT dynamic topology.
3. Last but not least limitation is swapping between reliability and power efficiency. Developing UPD transportation protocol for real-time data is a helpful key, although, persistence connection can be enabled on higher layers. Beyond that, IEEE 802.15.4 is a tackle for synchronization problem and intermittent access, even it is in its fancy stages.

G. *Data storage and processing*

Today we are witnessing of vast amount of data and rapid growth in interconnected objects in IoT. Hence the need for adequate storage spaces as well as effective ana-

lytic strategies for smart decision making is inevitable. To handle this aim, some artificial intelligence techniques i.e. data mining and machine leaning facilitate mathematical process. Furthermore, cloud infrastructure as a centralized repository and fog platform as distributed near field repository meet analytics data demands. At the same time, sending big data from cloud infrastructure to edges imposes extra cost of dissemination or accumulation.

H. *Modeling and simulation tools*

Although, there are some IoT reference models for example IoT-A, IIRA, RAMI, IEEE, etc. each supports certain features of prototype, absence of pervasive methodology for modeling such heterogeneous, complex network is tangible.

Despite available simulation tools such as NS, SWIM, cloudsim, contiki represented in Fig. 6, our findings about complication of IoT processes impose a need for multifaceted sophisticated simulation techniques able to integrate various protocols, privacy and security, power consumption in virtualized IoT infrastructure to obtain desired performance. Besides, massive amount of diverse loads discloses a fact that simulation defects are not confined to software applications and urge for hardware implementations, database, cpu, etc. as well. Constant development of simulation tools will satisfy real-time requirement of IoT scenario.

By surveying related papers in this field, follow there are some proposed opportunities and direction for above-mentioned hinders:

a. *Generality, validation*

Although some effort has made to preserve privacy in single piece of software or specific IoT layer, however, to achieve generality, more efficient protocols are needed through whole layers to keep entire IoT system integrated. In this respect, identification in data acquisition layer, data governance, access policy could to be addressed.

b. *Knowledge extraction*

This criterion goes beyond just creating or transforming information. It demands either the reuse of available knowledge and identifiers or applies a set of techniques like machine learning that allows a system to discover needed information from a large amount of raw data.

c. *Data transmission methods*

It is the transfer of data between point-to-point or multiple point communication channels. Below ISO/OSI model protocol layers typically occupied in data transmission, and deal with these responsibilities:

- Physical layer: channel coding or forward error correction, etc.
- Data link layer: error detection, synchronization, access control, etc.
- Presentation layer: source coding, cryptography, etc.

d. *Data aggregation*

The benefit of these criteria as described in "Conceptual methodology" section while proposing our trust-based recommendation mode. However, different types of data mining process can be employed to gather, summarized and reduce the dimension of data before dispatching them.

e. *Collaborative interfaces*
In a constantly shifting IoT environment special purpose interfaces (hardware or software) independent of programming languages, should collaborate to offer users functionality in a familiar IoT environment.

f. *Optimal resource utilization*
Predominant number of IoT objects are low power wireless sensors or embedded devices which are mostly associated by high computation demands. One of the solution for this shortcoming relies on IEEE 802.15.4 physical layer. Unlike WiFi and Bluetooth with high throughput and cost, this standard characterized by low energy, small data and less expense. To improve energy efficiency, devices spend majority of life in "sleep mode" and wake up for short interval to participate in communication. Additionally, identifying efficient resources and exploiting different hardware, software or overlaying virtual technology to maximize resource conservation is another alternative. One more recommendation is power transfer from distance, which entails promising future for IoT development.

g. *Communication technologies and protocols*
Depending on the application and factors like data range, battery life, security etc. one or a combination form of communication technologies (RFID, NFC, WiFi, Bluetooth, ZigBee and 2G/3G/4G/LTE, LoRaWAN, etc.), different format of message exchange as well as programming language (CoAP, RESTful, etc.) can be employed.

For instance, IPV6 is replaced for end-to-end communication, since IPV4 is already exhausted. UDP lightweight protocol is adopted due to available communication protocols e.g. TCP and HTTP deficiency for optimal transportation in IoT low powered devices. Nonetheless, UDP exposes unreliability, disorder and delay. In order to guarantee optimized data delivery in IoT, power-saving MAC or *Routing Protocol for Low Power and Lossy Networks are taken.*

Summary and conclusion

This survey provided a systematic review of recommendation techniques in IoT environment, which includes pertinent concepts definition and comprehensive analysis of mechanism and frameworks extracted from 59 authentic published literature among 206 primary selected papers from the search query, spanning 2011–2018. However, there was not comprehensive evidence on this matter and pros and cons are constrained to only one or two sources. This is happened due to publication bias towards the benefits which is common threat in literate review. We partially controlled it by choosing popular web domains with the most number of responses.

Secondly, through answering questions, we identified predominant metrics in recommendation techniques that should be comprehended in the future mechanism. Given that the systematic literature review is subject to question misunderstood, data synthesis or interpretation in all steps, understandability of inclusion and exclusion criteria for the review was examined in advance and only works with high level of agreement separated to become public. Despite each and every possible action, population or language bias, multiple or duplicate bias, reporting or citation bias and time bias might still present in the survey and could not be absolutely prevented.

Additionally, we classified literature based on three IoT layers, where, evidence recognized trust as a flourishing paradigm to ascend the accuracy of recommendation in IoT. We debated each approaches advantages and disadvantages and summarized the individual facts. In conclusion, trust computing mechanisms for recommender system still requires more investigation due to heterogeneity of IoT environment, to become more compatible with mobility instances and overcome its vulnerability as well. As future works, we suggest to extend the generality of this study by taking a deeper search associated with SLRs in trust techniques for a recommendation and evaluate different metrics in mathematical format or in a simulation toolkit while contrasting them by new ones. In this respect, one can launch either manual or automated searcher to trace the systematic literature reviews' progress or whether restricted analysis results are more reliable. We sincerely hope this review's outcome shed light on the research grounds for a further contribution to a trustworthy recommendation in IoT.

Acknowledgements
Not applicable.

Authors' contributions
All authors contributed equally to this manuscript. All authors read and apporved the final manuscript.

Funding
No funding was received.

Availability of data and materials
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Author details
[1] Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran. [2] Computer Science, University of Human Development, Sulaimanyah, Iraq. [3] Department of Computer Engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran.

Received: 17 February 2019 Accepted: 9 May 2019
Published online: 03 June 2019

References

1. Ashton K (2009) That 'internet of things' thing. RFID J 22(7):97–114
2. Kobayashi G, Quilici-Gonzalez JA, Broens MA, Quilici- Gonzalez ME (2011) Ubiquity of virtual disguisers and potential impact on ethical behavior. In: 2011 fourth international conference on Ubi-media computing. IEEE, Piscataway
3. Kobayashi G, Quilici-Gonzalez ME, Broens MC, Quilici-Gonzalez JA (2016) The ethical impact of the Internet of Things in social relationships: technological mediation and mutual trust. IEEE Consumer Electron Mag 5(3):85–89
4. Zheng S, Jiang T, Baras J (2011) Exploiting trust relations for nash equilibrium efficiency in ad hoc networks. In: IEEE international conference on communications (ICC), 2011. IEEE, Piscataway
5. Ricci F, Rokach L, Shapira B (2015) Recommender systems: introduction and challenges. In: Recommender systems handbook. Springer, Berlin, pp 1–34
6. Kalaï A, Zayani CA, Amous I, Abdelghani W, Sèdes F (2017) Social collaborative service recommendation approach based on user's trust and domain-specific expertise. Future Gen Comput Syst 80:355–367
7. Celdrán AH, Pérez MG, Clemente FJG, Pérez GM (2016) Design of a recommender system based on users' behavior and collaborative location and tracking. J Comput Sci 12:83–94
8. Lucas JP, Segrera S, Moreno MN (2012) Making use of associative classifiers in order to alleviate typical drawbacks in recommender systems. Expert Syst Appl 39(1):1273–1283
9. Staab S, Bhargava B, Leszek L, Rosenthal A, Winslett M, Sloman M, Dillon TS, Chang E, Hussain F, Nejdl W, Olmedilla D, Kashyap V (2004) The pudding of trust. IEEE Intell Syst 19(5):74–88
10. Roman R, Najera P, Lopez J (2011) Securing the internet of things. Computer 44(9):51–58
11. Kitchenham B, Brereton OP, Budgen D, Turner M, Bailey J, Linkman S (2009) Systematic literature reviews in software engineering—a systematic literature review. Inf Softw Technol 51(1):7–15
12. Yuan W, Guan D, Lee YK, Lee S, Hur SJ (2010) Improved trust-aware recommender system using small-worldness of trust networks. Knowl-Based Syst 23(3):232–238

13. Yuan W, Guan D, Shu L, Niu J (2012) Efficient searching mechanism for trust-aware recommender systems based on scale-freeness of trust networks. In: IEEE 11th international conference on trust, security and privacy in computing and communications (TrustCom), 2012. IEEE, Piscataway
14. Yuan W, Guan D, Lee YK, Lee S (2011) The small-world trust network. Appl Intell 35(3):399–410
15. Massa P, Avesani P (2009) Trust metrics in recommender systems. In: Computing with social trust. Springer, London, pp 259–285
16. Walter FE, Battistion S, Schweitzer F (2008) A model of a trust-based recommendation system on a social network. Autonomous Agents Multi-Agent Syst 16(1):57–74
17. Tan S, Li X, Dong Q (2015) Trust based routing mechanism for securing OSLR-based MANET. Ad Hoc Netw 30:84–98
18. Zhao D, Ma Z, Zhang D (2016) A distributed and adaptive trust evaluation algorithm for MANET. In: Proceedings of the 12th ACM symposium on QoS and security for wireless and mobile networks. ACM, New York, pp 47–54
19. Liu Y, Gong X, Xing C (2014) A novel trust-based secure data aggregation for internet of things. In: 9th international conference on computer science & education (ICCSE), 2014. IEEE, Piscataway, pp 435–439
20. Yao L, Man Y, Huang Z, Deng J, Wang X (2016) Secure routing based on social similarity in opportunistic networks. IEEE Trans Wireless Commun 15(1):594–605
21. Kowshalya AM, Valarmathi ML (2017) Trust management in the social Internet of Things. Wireless Pers Commun 96(2):2681–2691
22. Asiri S, Miri A (2016) An IoT trust and reputation model based on recommender systems. In: 14th annual conference on privacy, security and trust (PST), 2016. IEEE, Piscataway, pp 561–568
23. Victor P, De Cock M, Cornelis C (2011) Trust and recommendations. In: Recommender systems handbook. Springer, Boston, pp 645–675
24. Noh S (2007) Calculating trust using aggregation rules in social networks. In: International conference on autonomic and trusted computing. Springer, Berlin, Heidelberg, pp 361–371
25. Ning H, Liu H, Yang L (2013) Cyber-entity security in the Internet of Things. Computer 46(4):46–53
26. Abdmeziem MR, Tandjaoui D, Romdhani I (2016) Architecting the internet of things: state of the art. Robots Sens Clouds, Springer, Cham, pp 55–75
27. Li N, Das SK (2013) A trust-based framework for data forwarding in opportunistic networks. Ad Hoc Netw 11(4):1497–1509
28. Bernabe JB, Ramos JLH, Gomez AFS (2016) TACIoT: multidimensional trust-aware access control system for the Internet of Things. Soft Comput 20(5):1763–1779
29. Ko HG, Ko IY, Lee D (2018) Multi-criteria matrix localization and integration for personalized collaborative filtering in IoT environments. Multimedia Tools Appl 77(4):4697–4730
30. Margaris D, Vassilakis C (2017) Exploiting Internet of Things information to enhance venues' recommendation accuracy. SOCA 11(4):393–409
31. Ali T, Nauman M, Jan S (2017) Trust in IoT: dynamic remote attestation through efficient behavior capture. Cluster Comput 21(1):409–421
32. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A (2015) Security, privacy and trust in Internet of Things: the road ahead. Comput Netw 76:146–164
33. Al-Turjman F (2017) Cognitive caching for the future sensors in Fog networking. Pervasive Mobile Comput 42:317–334
34. Kang K, Pang Z, Da Xu L, Ma L, Wang C (2014) An interactive trust model for application market of the Internet of Things. IEEE Trans Industr Inf 10(2):1516–1526
35. Nitti M, Girau R, Atzori L (2014) Trustworthiness management in the social Internet of Things. IEEE Trans Knowl Data Eng 26(5):1253–1266
36. Grandison T, Sloman M (2000) A survey of trust in internet applications. IEEE Commun Surv Tutorials 3(4):2–16
37. Gambetta D (2000) Can we trust. Trust: making and breaking cooperative relations. 13, pp 213–237
38. Taylor J (1997) Introduction to error analysis, the study of uncertainties in physical measurements
39. Li L, Li S, Zhao S (2014) QoS-aware scheduling of services-oriented Internet of Things. IEEE Trans Ind Inf 10(2):1497–1505
40. Flexner SB, Hauck LC (1993) Random house unabridged dictionary. Random House, New York
41. Chen S, Wang G, Jia W (2013) A trust model using implicit call behavioral graph for mobile cloud computing. In: Cyberspace Safety and Security. Springer, Cham, pp 387–402
42. Anderson JM (2003) Why we need a new definition of information security. Comput Secur 22(4):308–313
43. Li YM, Chen CW (2009) A synthetical approach for blog recommendation: combining trust, social relation, and semantic analysis. Expert Syst Appl 36(3):6536–6547
44. Li Z, Chen R, Liu L, Min G (2016) Dynamic resource discovery based on preference and movement pattern similarity for large-scale social internet of things. IEEE Internet of Things J 3(4):581–589
45. Martinez B, Montón M, Vilajosana I, Prades JD (2015) The power of models: modeling power consumption for IoT devices. IEEE Sens J 15(10):5777–5789
46. Chen D, Chang G, Sun D, Li J, Jia J, Wang X (2011) TRM-IoT: a trust management model based on fuzzy reputation for internet of things". Comput Sci Inf Syst 8(4):1207–1228
47. 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
48. Atzori L, Iera A, Morabito G (2011) SIoT: giving a social structure to the internet of things. IEEE Commun Lett 15(11):1193–1195
49. 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
50. Valentine S (2010) Human resource management, ethical context, and personnel consequences: a commentary essay. J Bus Res 63(8):908–910

51. Flynn D, Aitken R, Gibbons A, Shi K (2007) Low power methodology manual: for system-on-chip design. Springer Science & Business Media, Berlin
52. Goodeve DM, Taylor RW (1990) Communications coprocessor for the Acorn RISC machine. Microprocessors Microsyst 14(5):301–305
53. Pinto S, Gomes T, Pereira J, Cabral J, Tavares A (2017) IIoTEED: an enhanced, trusted execution environment for industrial IoT edge devices. IEEE Internet Comput 21(1):40–47
54. Cao QH, Giyyarpuram M, Farahbakhsh R, Crespi N (2017) Policy-based usage control for a trustworthy data sharing platform in smart cities. Future Gen Comput Syst. https://doi.org/10.1016/j.future.2017.05.039
55. Miao G, Zander J, Sung KW, Slimane SB (2016) Fundamentals of mobile data networks. Cambridge University Press, Cambridge
56. Nieto A, Lopez J (2014) Analysis and taxonomy of security/QoS tradeoff solutions for the future internet. Secur Commun Netw 7(12):2778–2803
57. Shirvanimoghaddam M, Dohler M, Johnson SJ (2017) Massive non-orthogonal multiple access for cellular IoT: potentials and limitations. IEEE Commun Mag 55(9):55–61
58. Yick J, Mukherjee B, Ghosal D (2008) Wireless sensor network survey. Comput Netw 52(12):2292–2330
59. Zafar F, Khan A, Suhail S, Ahmed I, Hameed K, Khan HM, Jabeen F, Anjum A (2017) Trustworthy data: a survey, taxonomy and future trends of secure provenance schemes. J Netw Comput Appl 94:50–68
60. Litescu SC, Viswanathan V, Aydt H, Knoll A (2016) The effect of information uncertainty in road transportation systems. J Comput Sci 16:170–176
61. Ali BA, Abdulsalam HM, AlGhemlas A (2018) Trust based scheme for IoT enabled wireless sensor networks. Wireless Pers Commun 99(2):1061–1080
62. Abdulsalam HM, Ali BA, AlRoumi E (2017) Usage of mobile elements in internet of things environment for data aggregation in wireless sensor networks. Comput Electrical Eng 72:789–807
63. Li X, Zhou F, Du J (2013) LDTS: a lightweight and dependable trust system for clustered wireless sensor networks. IEEE Trans Inf Forensics Secur 8(6):924–935
64. Shaikh RA, Jameel H, d'Auriol BJ, Lee H, Lee S, Song Y-J (2009) Group-based trust management scheme for clustered wireless sensor networks. IEEE Trans Parallel Distrib Syst 20(11):1698–1712
65. Toh CK (2002) Ad hoc mobile wireless networks: protocols and systems, vol 11104. Springer, Berlin
66. Zanjireh MM, Shahrabi A, Larijani H (2013) ANCH: A new clustering algorithm for wireless sensor networks. In: 2013 27th international conference on advanced information networking and applications workshops (WAINA). IEEE, Piscataway, pp 450–455
67. Køien GM (2011) Reflections on trust in devices: an informal survey of human trust in an Internet-of-Things context. Wireless Pers Commun 61(3):495–510
68. O'Donovan T, O'Donoghue J, Sreenan C, Sammon D, O'Reilly P, O'Connor KA (2009) A context aware wireless body area network (BAN). In: 3rd international conference on pervasive computing technologies for healthcare, pervasive health 2009. IEEE, Piscataway
69. Asthana S, Megahed A, Strong R (2017) A recommendation system for proactive health monitoring using IoT and wearable technologies. In: IEEE international conference on AI & mobile services (AIMS), 2017. IEEE, Piscataway
70. Bandyopadhyay D, Sen J (2011) Internet of things: applications and challenges in technology and standardization. Wireless Pers Commun 58(1):49–69
71. Vaquero LM, Rodero-Merino L, Caceres J, Lindner M (2008) A break in the clouds: towards a cloud definition. ACM SIGCOMM Comput Commun Rev 39(1):50–55
72. Voorsluys W, Broberg J (2011) Buyya R (2011) Introduction to cloud computing. In: Buyya R, Broberg J, Goscinski AM (eds) Cloud computing: principles and paradigms. Wiley, Hoboken, pp 1–41
73. Mell P, Grance T (2009) The NIST definition of cloud computing. National Institute of Standards and Technology. Technical Report Version 53(6):50
74. Wang K, Qi X, Shu L, Deng DJ, Rodrigues JJPC (2016) Toward trustworthy crowdsourcing in the social internet of things. IEEE Wireless Commun 23(5):30–36
75. Fortino G, Messina F, Rosaci D, Sarné GML (2018) Using trust and local reputation for group formation in the Cloud of Things. Future Gen Comput Syst 89:804–815
76. Bonomi F, Milito R, Zhu J, Addepalli S (2012) Fog computing and its role in the internet of things. In: Proceedings of the first edition of the MCC workshop on Mobile cloud computing (MCC '12). ACM, New York, pp 13–16
77. Bonomi F, Milito R, Natarajan P, Zhu J (2014) Fog computing: a platform for internet of things and analytics. In: Big data and Internet of Things: a roadmap for smart environments. Springer, Cham, pp 169–186
78. Garcia-de-Prado A, Ortiz G, Boubeta-Puig J (2017) COLLECT: COLLaborativE ConText-aware service oriented architecture for intelligent decision-making in the Internet of Things. Expert Syst Appl 85:231–248
79. Gusmeroli S, Piccione S, Rotondi D (2013) A capability- based security approach to manage access control in the internet of things. Math Comput Model 58(5–6):1189–1205
80. Alcaide A, Palomar E, Montero-Castillo J, Ribagorda A (2013) Anonymous authentication for privacy-preserving IoT target-driven applications. Comput Secur 37:111–123
81. Sfar AR, Natalizio E, Challal Y, Chtourou Z (2018) A roadmap for security challenges in Internet of Things. Digital Commun Netw 4(2):118–137
82. Ouaddah A, Mousannif H, Elkalam AA, Ouahman AA (2017) Access control in the Internet of Things: big challenges and new opportunities. Comput Netw 112:237–262
83. 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
84. Mahalle PN, Thakre PA, Prasad NR, Prasad R (2013) A fuzzy approach to trust based access control in internet of things. In: 3rd international conference on wireless communications, vehicular technology, information theory, and aerospace & electronic systems (VITAE), 2013. IEEE, Piscataway, pp 1–5
85. Padlipsky MA, Snow DW, Karger PA (1978) Limitations of end-to-end encryption in secure computer networks. No. MTR-3592-VOL-1. MITRE CORP BEDFORD MA

86. Sicari S, Rizzardi A, Miorandi D, Cappiello C, Coen-Porisini A (2016) A secure and quality-aware prototypical architecture for the Internet of Things. Inf Syst 58:43–55
87. Hellaoui H, Bouabdallah A, Koudil M (2016) TAS-IoT: Trust-based adaptive security in the IoT. In: IEEE 41st conference on local computer networks (LCN), 2016. IEEE, Piscataway, pp 599–602
88. Azad MA, Bag S, Parkinson S, Hao F (2018) TrustVote: privacy-preserving node ranking in vehicular networks. IEEE Internet Things J
89. Shannon CE (1948) A mathematical theory of communication. Bell Syst Tech J 27(3):379–423
90. Yu Y, Jia Z, Tao W, Xue B, Lee C (2017) An Efficient trust evaluation scheme for node behavior detection in the Internet of Things. Wireless Pers Commun 93(2):571–587
91. Debar H, Dacier M, Wespi A (2000) A revised taxonomy for intrusion-detection systems. Annales des télécommunications 55(7–8):361–378
92. Denning DE (1987) An intrusion-detection model. IEEE Trans Softw Eng 13(2):222–232
93. Khan WZ, Aalsalem MY, Khan MK, Arshad Q (2017) When social objects collaborate: concepts, processing elements, attacks and challenges. Comput Electr Eng 58:397–411
94. Chen R, Bao F, Guo J (2016) Trust-based service management for social Internet of Things Systems. IEEE Trans Depend Secure Comput 13(6):684–696
95. 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) 2017. IEEE, Piscataway, pp 30–39
96. Schollmeier R (2001) A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In: Proceedings First International Conference on Peer-to-Peer Computing. pp 101–102
97. Wang Y, Chen R, Cho JH, Swami A, Lu YC, Lu CT, Tsai J (2016) CATrust: Context-Aware Trust management for service-oriented ad hoc networks. IEEE Trans Serv Comput 11(6):908–921
98. Papazoglou M (2012) Web services and SOA: principles and technology, 2nd edn. Pearson Education Limited, Harlow, Essex, England; New York
99. Al-Hamadi H, Chen R (2017) Trust-based decision making for health IoT Systems. IEEE Internet Things J 4(5):1408–1419
100. Jøsang A, Keser C, Dimitrakos T (2005) Can we manage trust? In: International conference on trust management. Springer, Berlin, Heidelberg, pp 93–107
101. Blaze M, Feigenbaum J, Lacy J (1996) Decentralized trust management. In: Proceedings IEEE symposium on security and privacy, 1996. IEEE, Piscataway
102. Blaze M, Ioannidis J, Keromytis AD (2003) Experience with the keynote trust management system: applications and future directions. In: International conference on trust management. Springer, Berlin, Heidelberg
103. Kounelis I, Baldini G, Neisse R, Steri G, Tallacchini M, Pereira AG (2014) Building trust in the human? Internet of Things relationship. IEEE Technol Soc Mag 33(4):73–80
104. Yan Z, Zhang P, Vasilakos AV (2014) A survey on trust management for Internet of Things. J Netw Comput Appl 42:120–134
105. Wang PU, Zhang P (2016) A review on trust evaluation for internet of things. In: Proceedings of the 9th EAI international conference on mobile multimedia communications. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering)
106. Suryani V, Widyawan S (2016) A survey on trust in Internet of Things. In: 2016 8th international conference on information technology and electrical engineering (ICITEE), IEEE, Piscataway, pp 1–6
107. Mendoza CVL, Kleinschmidt JH (2018) A distributed trust management mechanism for the Internet of Things using a multi-service approach. Wireless Pers Commun 103(3):2501–2513
108. Chen J, Tian Z, Cui X, Yin L, Wang X (2018) Trust architecture and reputation evaluation for internet of things. J Ambient Intell Hum Comput. https://doi.org/10.1007/s12652-018-0887-z
109. Guo J, Chen R, Tsai JJP (2017) A survey of trust computation models for service management in Internet of Things systems. Comput Commun 97:1–14
110. Atzori L, Iera A, Morabito G (2010) The Internet of Things: a survey. Comput Netw 54(15):2787–2805
111. 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
112. Chen R, Guo J, Bao F (2016) Trust management for SOA-based IoT and its application to service composition. IEEE Trans Serv Comput 9(3):482–495
113. Mashal I, Chung TY, Alsaryrah O (2015) Toward service recommendation in Internet of Things. In: seventh international conference on ubiquitous and future networks (ICUFN), 2015. IEEE, Piscataway
114. Mashal I, Alsaryrah O, Chung TY (2016) Analysis of recommendation algorithms for Internet of Things. In: IEEE wireless communications and networking conference workshops (WCNCW). IEEE, Piscataway, pp 1–6
115. Chen Z, Ling R, Huang CM, Zhu X (2016) A scheme of access service recommendation for the Social Internet of Things. Int J Commun Syst 29(4):694–706
116. Lin Z, Dong L (2018) Clarifying trust in social internet of things. IEEE Trans Knowl Data Eng 30(2):234–248
117. Butt TA, Iqbal R, Shah SC, Umar T (2018) Social Internet of Vehicles: architecture and enabling technologies. Comput Electr Eng 69:68–84
118. Galuba W, Girdzijauskas S (2009) Distributed hash table. Springer, Encyclopedia of database systems, pp 903–904
119. Dey AK (2001) Understanding and using context. Pers Ubiquit Comput 5(1):4–7
120. Abowd GD, Dey AK, Brown PJ, Davies N, Smith M, Steggles P (1999) Towards a better understanding of context and context-awareness. In: International symposium on handheld and ubiquitous computing. Springer, Berlin, Heidelberg, pp 304–307
121. Burstein F, Brézillon P, Zaslavsky A (2010) In: Burstein F, Brézillon P, Zaslavsky A, editors. Supporting real time decision-making: The role of context in decision support on the move. Vol. 13. Springer Science & Business Media, Berlin

122. Henricksen K, Indulska J (2004) Modelling and using imperfect context information. Proceedings of the second IEEE annual conference on pervasive computing and communications workshops, 2004. IEEE, Piscataway
123. Fernandez-Gago C, Moyano F, Lopez J (2017) Modelling trust dynamics in the Internet of Things. Inf Sci 396:72–82
124. Chabridon S, Laborde R, Desprats T, Oglaza A, Marie P, Marquez SM (2014) A survey on addressing privacy together with quality of context for context management in the Internet of Things. Ann Telecommun 69(1–2):47–62
125. Tang Y, Meersman R (2012) DIY-CDR: an ontology-based, Do-It-Yourself component discoverer and recommender. Pers Ubiquit Comput 16(5):581–595
126. Chen JM, Li T, Panneerselvam J. (2018) TMEC: a trust management based on evidence combination on attack-resistant and collaborative internet of vehicles. IEEE Access
127. Zadeh LA (1965) Fuzzy sets. Inf Control 8(3):338–353
128. Özkan I, Türkşen IB (2014) Uncertainty and fuzzy decisions. In: Banerjee S, Erçetin Ş, Tekin A (eds) Chaos theory in politics. Understanding complex systems. Springer, Dordrecht, pp 17–27
129. Tormo GD, Mármol FG, Pérez GM (2015) Dynamic and flexible selection of a reputation mechanism for heterogeneous environments. Future Gen Comput Syst 49:113–124
130. Nguyen T, Hoang D, Seneviratne A (2016) Challenge-response trust assessment model for personal space IoT. In: IEEE international conference on pervasive computing and communication workshops (PerCom Workshops), 2016. IEEE, Piscataway
131. Ali F, Khan P, Islam SR, Kwak, Ullah N, Yoo SJ, Kwak KS (2017) Type-2 fuzzy ontology–aided recommendation systems for IoT–based healthcare. Comput Commun 119:138–155
132. Mahmud M, Kaiser MS, Rahman MM, Rahman MA, Shabut A, Al-Mamun S, Hussain A (2018) A brain-inspired trust management model to assure security in a cloud based IoT framework for neuroscience applications. Cognit Comput 10(5):864–873
133. Zeinali Y, Story BA (2017) Competitive probabilistic neural network. Integr Comput Aided Eng 24(2):105–118
134. Specht DF (1990) Probabilistic neural networks. Neural networks 3(1):109–118
135. Aggarwal CC (2016) Content-based recommender systems. Recommender systems, Springer, Cham, pp 139–166
136. Mooney RJ, Roy L (2000) Content-based book recommendation using learning for text categorization. In: Proceedings of the fifth ACM conference on Digital libraries. ACM, New York
137. Čolaković A, Hadžialić M (2018) Internet of Things (IoT): a review of enabling technologies, challenges, and open research issues. Comput Netw 144:17–39

Publisher's Note