IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 21 November 2022, accepted 16 January 2023, date of publication 31 January 2023, date of current version 7 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3240990

SURVEY

Trust Evaluation Model in IoT Environment: A Comprehensive Survey

SOMYA ABDULKARIM ALHANDI, HAZALILA KAMALUDIN, AND NAYEF ABDULWAHAB MOHAMMED ALDUAIS
Faculty of Computer Science and Information Technology (FSKTM), Universiti Tun Hussein Onn Malaysia (UTHM), Batu Pahat, Johor 86400, Malaysia

Corresponding authors: Somya Abdulkarim Alhandi (somya.abdulkarim@gmail.com), Hazalila Kamaludin (hazalila@uthm.edu.my), and Nayef Abdulwahab Mohammed Alduais (nayef@uthm.edu.my)

This work was supported in part by Universiti Tun Hussein Onn Malaysia (UTHM) through Tier—1 (vot H789), and in part by the Ministry of Higher Education of Malaysia (MOHE) through Fundamental Research Grant Scheme under Grant Vot K216 and Reference Code: FRGS/1/2019/ICT04/UTHM/03/2.

ABSTRACT The Internet of Things (IoT) is a rapidly evolving field that provides seamless connections to a physical object, making it part of a smart environment. To fully realize the potential power of the connections between these objects in IoT, trust between them is critical. Conventional security measures are not sufficient to provide comprehensive security for this smart world. Trust is used to reduce the risk of insecurity when nodes are connected to the Internet. In an IoT environment, various trust models have been proposed for Wireless Sensor Networks (WSNs) and Radio Frequency Identification (RFID). Nevertheless, these are not fully adapted to the dynamic and uncertain environment of the intelligent IoT. Therefore, this article reviews the characteristics of recent works in IoT trust models. A comprehensive study has been conducted on the classification of trust models. A set of factors are discussed, such as trust characteristics, trust architecture, trust distribution, trust aggregation technique, trust model type, and attack type. In addition, this paper provides readers with an understanding of the current existing trust model and directs future works to propose new models that satisfy all characteristics that should be considered when developing a trust model. Finally, some research challenges and directions are identified.

INDEX TERMS Internet of Things, wireless sensor network, radio frequency identification, trust model.

I. INTRODUCTION

The IoT is a technology that allows massive of intelligent communication nodes to be connected to the Internet. These nodes are actuators or/and sensors that can process and restore data from other systems without or with personal interference. The growth of IoT has brought a huge impact on several fields, and many IoT applications have been implemented to enhance system performance and quality of life in manufacturing, transportation, healthcare, etc., [1], [2], [3].

IoT technology involves multiple tasks to obtain the goals developed through smart services. The smart activities allow devices to interact with the physical world to provide users with the right service anytime, anywhere.

Its architecture consists of three layers, which are the perception, network, and application layers [4], as shown in Figure 1. At the perception layer, the actuator/sensor node performs sensing, processing, storage and transmission of data to the network layer. The network layer performs routing and delivery of data over the internet to multiple IoT hubs and computers using a variety of new technologies. While, the application layer ensures the authenticity, integrity, and confidentiality of data, and connects the physical world with the ubiquitous cyberspace through millions of smart things, which provided high economic benefits in different fields.

Significant advances in this technology have increased the number and mechanisms of attacks. Attackers often exploit the heterogeneity of IoT to raise trust issues and manipulate behavior to deceive the reliability of devices and the services provided through it. Furthermore, the heterogeneity and

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

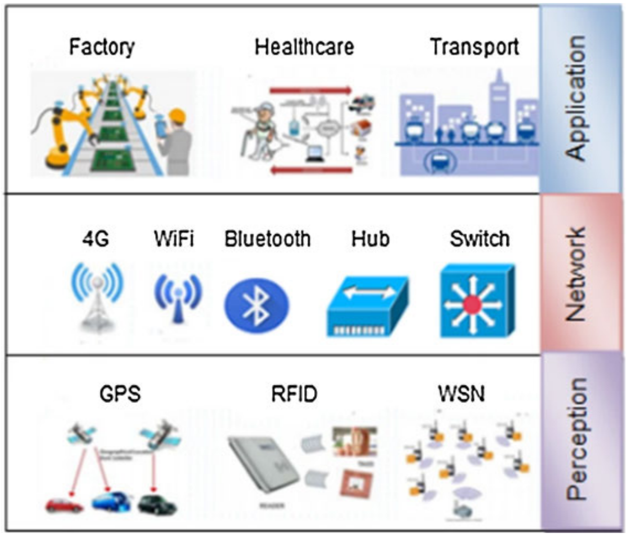


FIGURE 1. IoT architecture layers [4].

dynamics of IoT applications and the scarcity of resources have created huge challenges in terms of trust, security, and privacy, which play an essential role in the accomplishment of IoT implementation [5]. Therefore, the trust evaluation model uses to identify untrusted behaviors and isolate untrusted objects. It also helps to overcome the perception of uncertainty and reduce potential risks before making any decisions, which can help IoT infrastructure operate in a controlled manner and avoid unpredictable conditions and service failures [4], [5], [6].

IoT applications are unlikely to achieve widespread adoption if they do not have a robust security foundation, which will prohibit the development of malicious models, or at least alleviate their influence [6], [7]. Therefore, authentication and encryption mechanisms are utilized for IoT security. Providing robust authentication and encryption mechanisms helps mitigate several IoT security issues. The authentication and encryption mechanisms used to securely exchange messages between nodes, and thus represent the first line of defense against external attacks [8]. These mechanisms can prevent and detect external attacks but cannot handle internal attacks and adversarial nodes in the network. In fact, internal attackers can bypass these mechanisms by accessing the shared key and triggering multiple attacks on the IoT network. For this reason, the concept of trust has been introduced to deal with internal attacks in the IoT [7].

In the literature, privacy and security have been discussed in many research and they are explained in more detail. However, the trust model in IoT research has not been comprehensively investigated in a holistic manner. Therefore, in this paper, we will emphasize the trust evaluation model, which is considered to be more complex than the security itself as described in [9] and [10]. This is because trust is evaluated based on several factors such as strength, merit, reliability, usability, ability or other characteristics related to the object [11]. The contributions of this survey paper can be summarized as follows:

- A comprehensive literature review of the trust evaluation model.
- Emphasized and suggest the most common characteristics that can be considered in any trust evaluation model.
- Study the existing classifications of trust models deployed to current WSN and RFID technology in IoT.
- Point out the challenges and direction of research.

The rest of this article is organized as follows: In section II trust definition is described, and section III elaborates on the characteristics of trust in IoT. The classification of trust models is discussed in section IV. In section V overview of the suggested trust model is discussed, and the trust in WSN and RFID is described in section VI. In section VII we defined research directions within the trust model in IoT. Finally, section VIII presents the conclusion of this paper.

II. TRUST DEFINITION

Trust in IoT is a term that involves analysis of the behavior of the devices connected to the same network. The trust relationship between two devices helps in influencing the future behaviors of their interactions. When devices trust each other, they prefer to share services and resources to a certain extent. Trust management allows the computation and analysis of trust among devices to make a suitable decision in order to establish efficient and reliable communication among devices.

Trust is very important in autonomous sensor networks and self-configuration because it helps nodes determine whether another member of the network is a malicious node or a non-cooperative node [8]. Therefore, it is necessary to ensure that the object is trustworthy when it interacts with other objects [12]. Objects in the IoT cannot perceive other objects around, such as humans, so it is much more difficult to establish trust in the IoT environment. Moreover, it is difficult to measure the actual credibility value of an object with high accuracy. This is even more difficult when each subject has different perceptions and interpretations of the word ''trustworthy''. Therefore, the definition of trust includes more than a few concepts, such as lack of control, risk attitude, context specificity, utility, comfort, reliability, vulnerability, confidence, expectation and dependency [12].

There is no typical description of trust, so the researchers defined it from their perspective. In [13], they defined it as the level of belief in other objects according to direct and indirect observation. In [8], they defined it from a sociological domain as the behavior of one person trusting another person in the presence of ambiguous paths. In this term, trust is used to reduce the risk of dealing with others. In [14], trust is defined as a quantitative or qualitative attribute of a trustee, which is assessed as measurable confidence in an objective or subjective method by the trustee and used for a specific task, context, and period. While in [15], the trust is defined as an estimated subjective probability that an object shows reliable behavior for specific processes under a condition with possible hazards.

TABLE 1. Comparison in this survey and the previous surveys.

Ref. No	Trust Attribute		Trust Architecture			Trust Distributed		Trust Aggregation		Trust Type		Trust attack	Trust model in WSN	Trust model in RFID
	Social	Nonsocial	Centralized	Decentralized	Distributed	Direct	Indirect	Detail	Undetailed	Node Data	Node behavior			
[13]	√	√	√	√	X	√	√	X	√	X	X	X	X	X
[9]	√	√	√	√	√	√	√	X	√	√	X	X	X	X
[16]	√	√	√	X	√	X	X	X	√	X	X	X	X	X
[17]	√	√	√	X	√	X	X	√	X	X	X	√	X	X
[18]	X	X	√	√	√	√	√	X	X	X	X	X	X	X
[19]	√	X	√	X	√	X	√	X	X	X	√	X	X	X
Our survey	√	√	√	√	√	√	√	√	X	√	√	√	√	√
Annotation: √ -Discussed, X-Not discussed														

The researchers have evaluated the trust model either based on node data or node behavior, where the node data trust and node behavior trust should be seriously considered and stringently supported. Besides that, there is no survey has elaborated on the trust model in WSN and RFID in the IoT environment, where WSN/RFID is the two main technology in IoT. The comparison in this survey and the previous surveys is tabulated in Table 1.

III. CHARACTERISTIC OF TRUST

The characteristics of trust evaluation have been driven based on the researcher's perspective view and there are no common characteristics that have been followed. In [5], [7], [20], and [21] authors have classified the trust as follows:

- Context attributes: the trust relationship is based on the context, and the context point to all the information that defines the condition of the relevant participant.
- Subjectivity: A trust factor that is hard to measure and monitor. These attributes are more related to cognition or social trust.
- Objectivity: a trust factor that can be measured and monitored. These attributes are more about computing trust.

While authors in [4], [8], [22], and [23] have defined the trust characteristics into several attributes (see Figure 2) as follows:

- Trust is subjective: Trust can differ from the trustee in the same confidence and sense of trust, for example, if node X trust on node Y, that does not mean, node T has the same confidence on node Y.
- Trust is asymmetric: The trust does not apply in both directions between trustee and trustor. For example, if node X trusts node Y, this does not mean that node Y also trusts node X.
- Trust is dynamic: It can exist for a while. Over time, the level of confidence will change.
- Trust depends on the context: The level of trust in oneself may vary greatly in different environments.
- There is no complete trust: Trust that one object holds over another object is never 100%.
- Trust is transferable: in the case where node X trusts node Y and node Y trusts node T, the transitivity is related to the degree to which node X trusts node T. This attribute is important and can be used for reasoning in another context, which may be a more complex relationship.

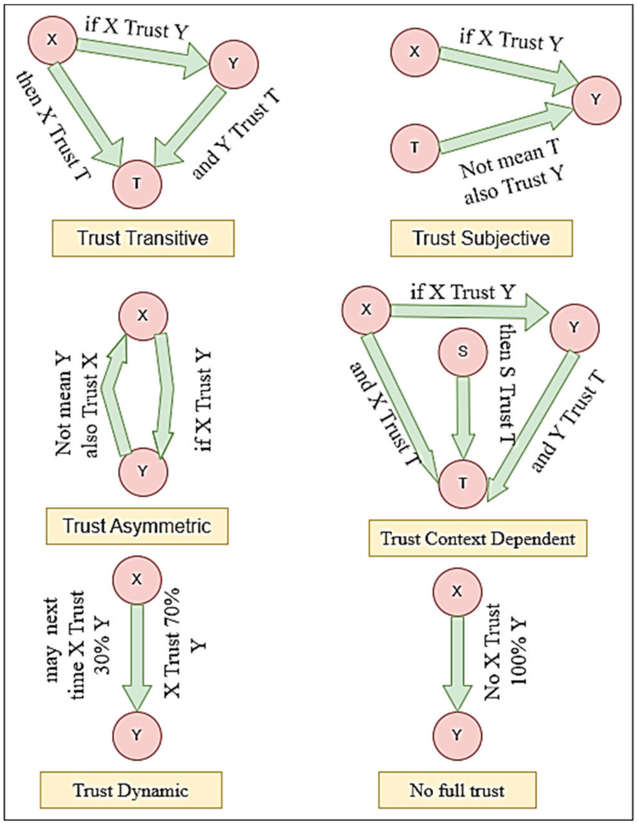


FIGURE 2. Explanation of each trust characteristics.

IV. CLASSIFICATION OF TRUST MODEL

The main concern is to evaluate the trust value of the node before the actual data communication. The trust computing model is a model that provides the trust value of nodes in the network. Based on the different characteristics of trust, several trust models have been classified in [8], [13], [14], [24], [25], [26], [27], [28], and [29].

In [25], researchers discussed the challenges and existing solutions of the trust model, which are divided into eight categories; identity, verification, confidentiality, mobile security, middleware, policy enforcement, trust, privacy, and access control. In [8], the authors divided the trust model into two categories; node trust model and data trust model. The node trust model is based on corresponding characteristics of node behavior such as:

(i) data repetition rate of the sample that can reflect the abnormal behavior of the node, and
(ii) packet size that reflects the abnormal node

If the packet size is too large, it means denial of service attack, and, if it is too small, it means selfish node. The data trust model is based on the data collected by sensor nodes such as the data's reliability, accuracy, consistency, correctness, and competence.

In [14], authors developed a trust model based on the three trust metrics which are reputation, experience and knowledge as illustrated in Figure 3. As can be seen from Figure 3, the trust evaluation model is divided into direct and indirect trust. Direct trust is represented by the knowledge trust metric, which directly provides the perception of trustees during the interaction between objects. There are two attributes in the knowledge trust metric, namely social attribute and non-social attribute. The social attribute is used to determine whether a trustor can rely on other social objects such as (confidence, relationship, and willingness). Whereas the non-social attribute is used to determine whether the trustor can rely on physical or cyber objects for example (competence, dependence). On the other hand, indirect trust is represented by experience and reputation trust metrics. The experience trust metric is a personal observation considering only interactions from a trustor to a trustee for example (feedback), whereas the reputation trust metric reflects the global opinion of the trustee such as (recommendations and ratings) [14].

In [24], the authors proposed two categories; decision model and evaluation model. The decision model includes strategy models and negotiation models, while the evaluation model comprises communication (flow) models, reputation models, and behavior models. The two proposed categories are displayed in Figure 4.

Different types of trust models have been proposed in [26] to assess the trust such as Markov chain, arithmetic/weighted, directed/undirected graph, swarm intelligence, neural network, probability, fuzzy, entropy, game theory, and Bayesian statistics. These methods are used to evaluate the trust of secure routing. As shown in Figure 5, the authors have divided the trust model based on related methods that have been used. Each method has different characteristics from the others, and is only suitable for specific purposes, e.g., fuzzy logic technique is appropriate for the case of uncertain or inaccurate data.

A classification of trust models has been developed in [27] based on five characteristics which are trust composition, trust propagation, trust update, trust formation, and trust aggregation. They also pointed out the challenges related to each category. The classification of the trust model is illustrated in Figure 6.

Indeed, most current trust models utilize analytical methods to assess trust values. However, other techniques such as social networks, machine learning, ant colony-based algorithms, and evolutionary algorithms have also been used. Therefore, the authors in [28] introduced a new category of trust models according to biologically inspired and socially based trust techniques. Therefore, the author classifies the trust model into; social inspiration, biological inspiration, and analysis as shown in Figure 7.

In [29], they proposed various indicators of trust computing in the IoT environment which are trust, security, energy, accuracy, service quality, social network, reputation, and recommendation quality. While the author in [13] defined the trust model into five components trust which are metrics, propagation, architecture, algorithm, and source. The trust model is illustrated in Figure 8.

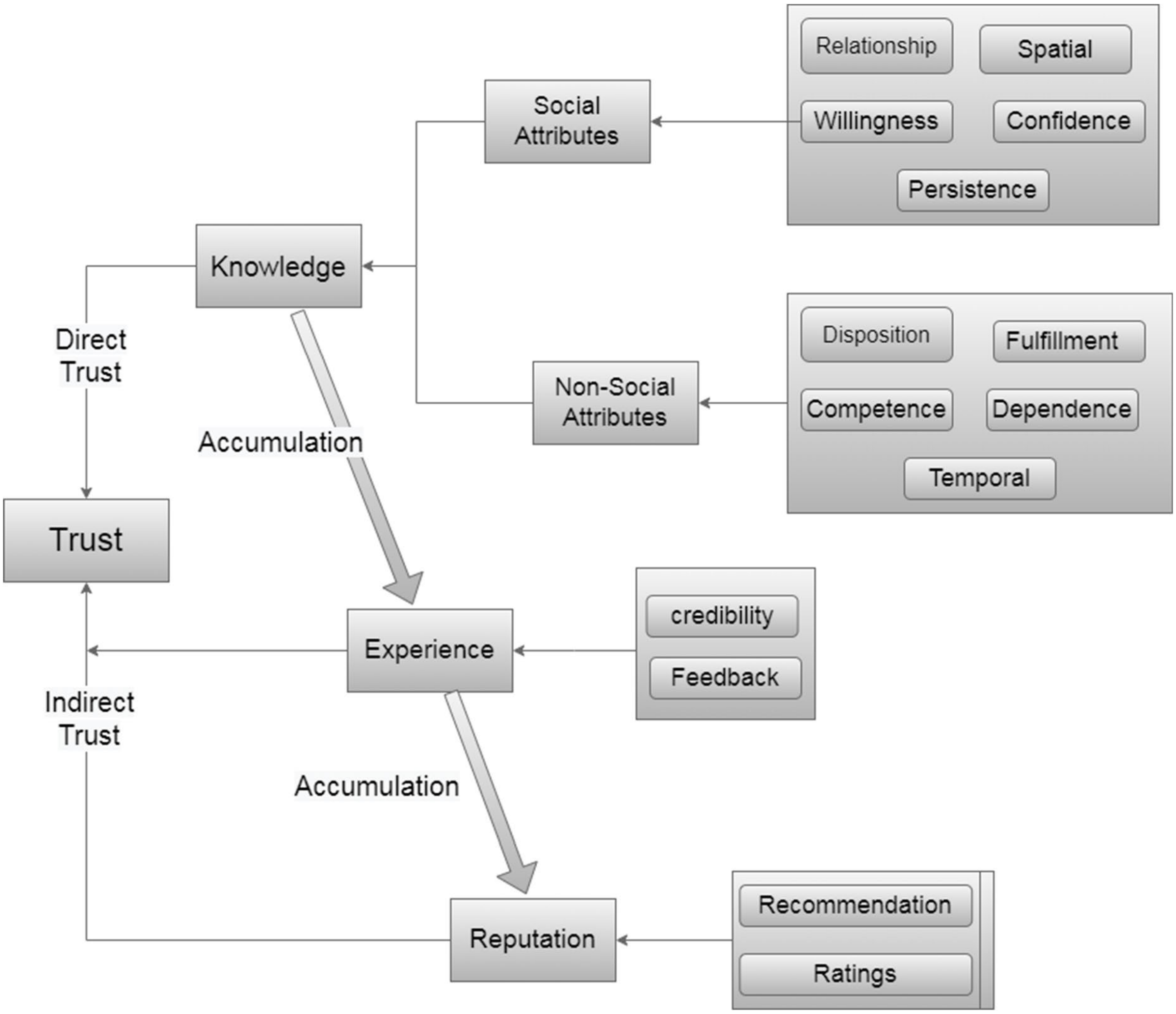


FIGURE 3. Trust evaluation model [14].

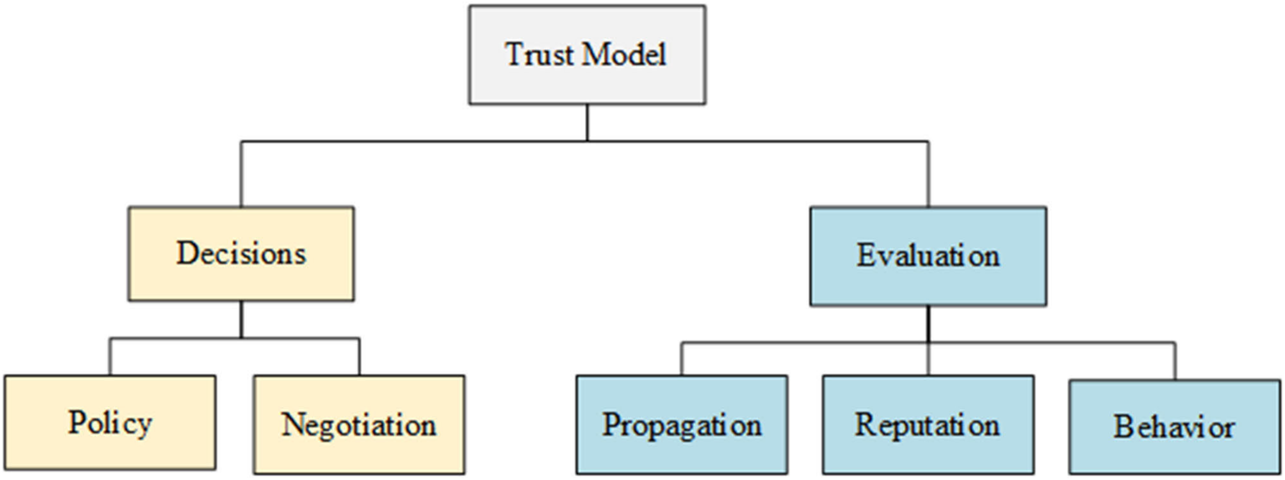


FIGURE 4. Trust evaluation model [24].

V. OVERVIEW OF THE SUGGESTED TRUST MODEL

Based on the aforementioned, we emphasized the most common characteristics that can be considered in each trust evaluation model. Therefore, we classified the trust model into six categories. They are (i) trust attributes, (ii) trust architecture, (iii) trust aggregation, (iv) trust source, (v) type of

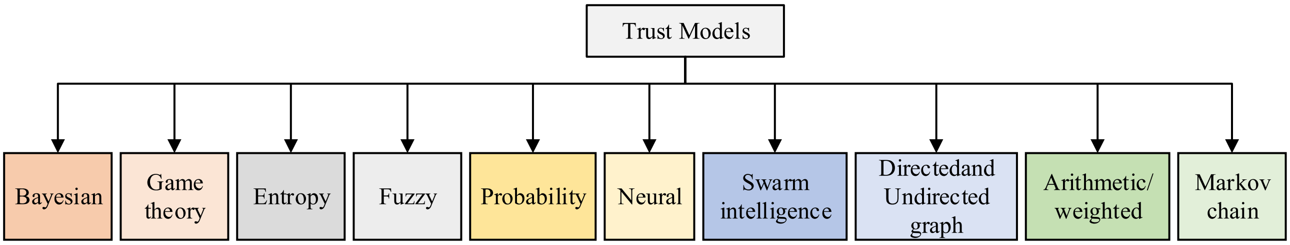


FIGURE 5. Trust evaluation model [26].

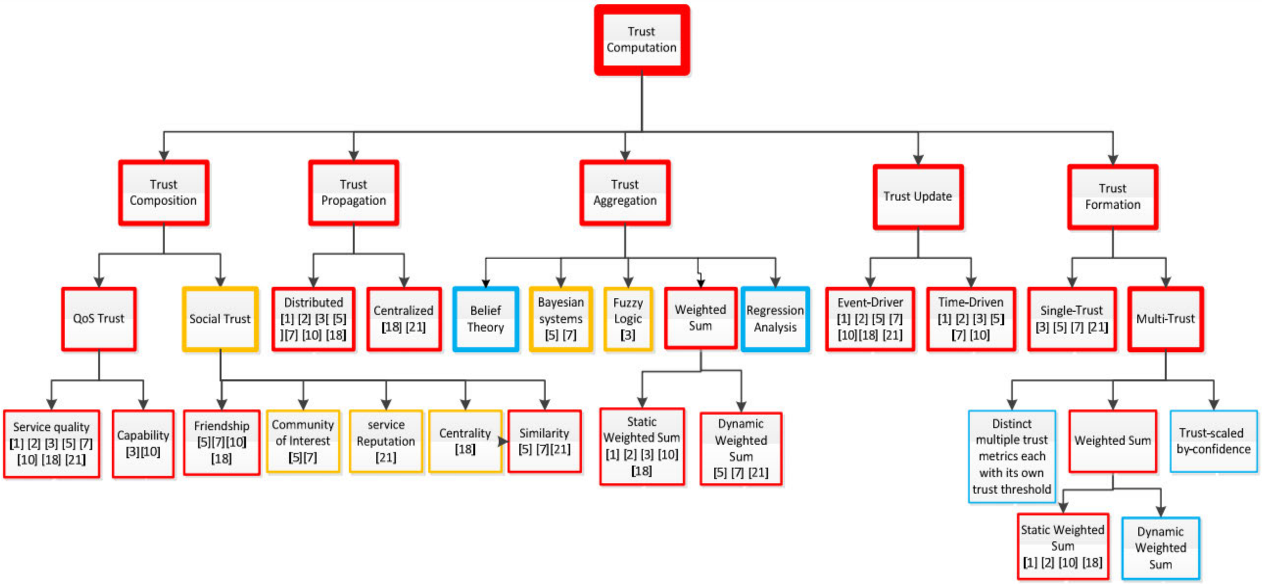

Trust Computation
Trust Composition
Trust Propagation
Trust Aggregation
Trust Update
Trust Formation
QoS Trust
Social Trust
Distributed [1] [2] [3[[5]][7] [10] [18]
Centralized [18] [21]
Belief Theory
Bayesian systems [5] [7]
Fuzzy Logic [3]
Weighted Sum
Regression Analysis
Event-Driver [1] [2] [5] [7] [10][18] [21]
Time-Driven [1] [2] [3] [5] [7] [10]
Single-Trust [3] [5] [7] [21]
Multi-Trust
Service quality [1] [2] [3] [5] [7] [10] [18] [21]
Capability [3][10]
Friendship [5][7][10] [18]
Community of Interest [5][7]
service Reputation [21]
Centrality [18]
Similarity [5] [7][21]
Static Weighted Sum [1] [2] [3] [10] [18]
Dynamic Weighted Sum [5] [7] [21]
Distinct multiple trust metrics each with its own trust threshold
Weighted Sum
Trust-scaled by-confidence
Static Weighted Sum [1] [2] [10] [18]
Dynamic Weighted Sum

FIGURE 6. Trust classification tree [27].

trust model (vi) type of attack. These parameters can be used as common terms for discussing IoT trust. Figure 9 shows our proposed classification of trust models. In summary, the most common trust models aforementioned are tabulated in Table 2.

As depicted in Figure 9, we elaborate our proposed classification of trust models as following:

A. TRUST ATTRIBUTES

In the IoT environment, there are two types of trust based on the relationship [16]. The first is the trust between a person and its device which is known as non-social trust, also known as quality of service (QoS) trust, and the second is the trust between a person and another person, known as social trust. Non-social trust indicates the confidence that IoT systems can offer high-quality services in response to service requests. QoS trust generally indicates performance, which is measured by task completion ability, reliability, collaboration, and ability [29], [30], [31]. Social trust originates from the social relationship between owners of IoT devices, measured by connectivity, centrality, privacy, honesty, and intimacy. Social trust is particularly common in IoT devices that must be in social IoT systems. Evaluation is not only according to QoS trust but also based on the level of trust of its owner [13], [27].

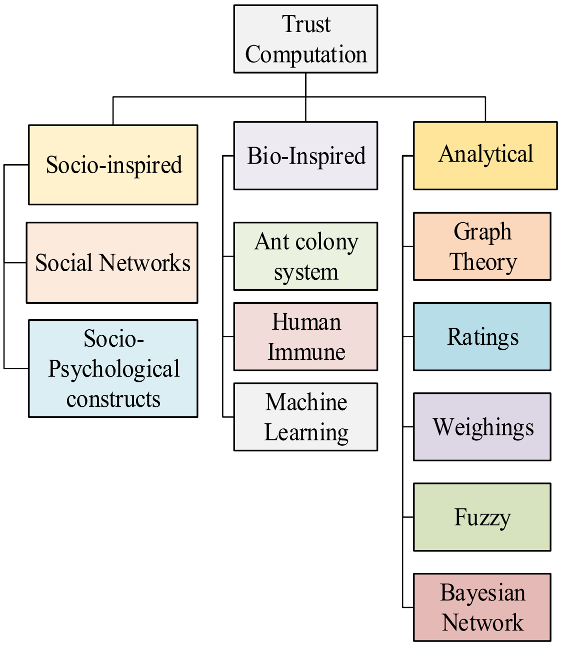


FIGURE 7. Trust models according to [28].

B. TRUST ARCHITECTURE

For heterogeneous applications and services on the IoT, special attention must be paid to the architecture of the trust

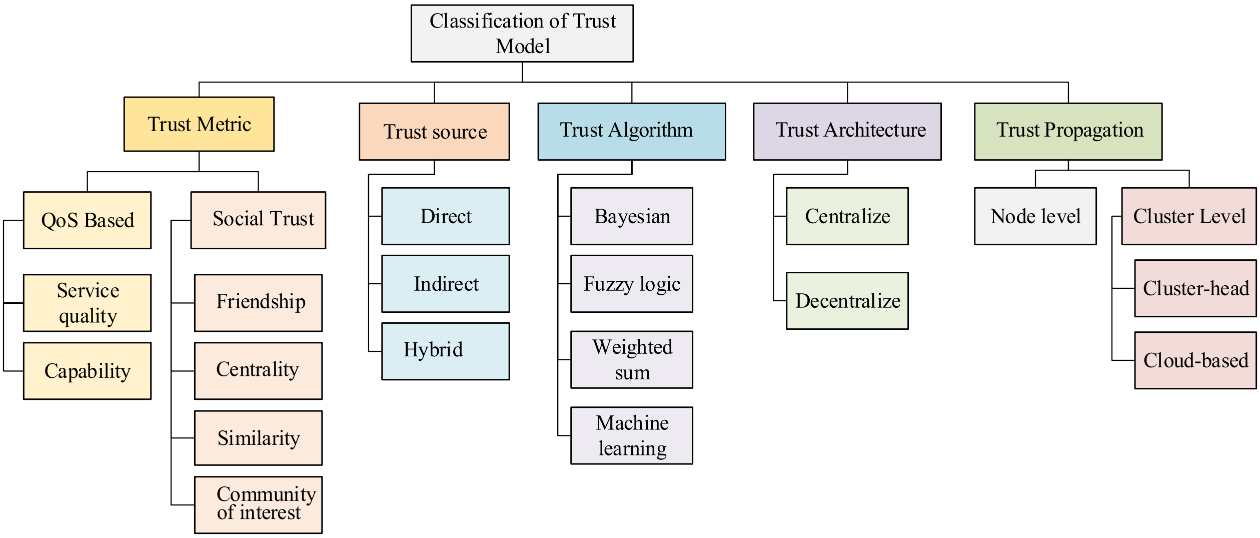
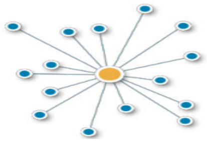
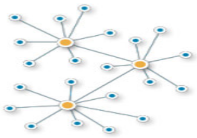
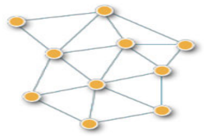


FIGURE 8. Trust Models according to [13].

TABLE 2. Summary of most common trust model.

Trust model	Description
Trust model 1 [14]	This trust model is developed based on direct and indirect trust. Each of them has attribute namely social and non-social. This model is focused more on social and non-social attributes while is not considering other attributes such as type of trust and type attack.
Trust model 2 [24]	This trust model classified into, decision model and evaluation model. The decision model includes strategy and negotiation models, while the evaluation model comprises communication (flow), reputation, and behaviour models.
Trust model 3 [26]	This trust model is developed based on trust aggregation method such as (fuzzy, entropy, game theory). Each method has different characteristics from others and is only suitable for specific purposes.
Trust model 4 [27]	This trust model is developed based on five characteristics which are trust composition, trust propagation, trust aggregation, trust formation and trust update this model consider some characteristics but still there are other characteristics need to consider such as distributed trust either direct or indirect trust and type of trust that is define either trust evaluation is based on behaviour node or data of the node.
Trust model 5 [28]	This model is introduced a new category of trust model according to biologically inspired and socially based trust techniques. So, the author classifies the trust model into; social inspiration, biological inspiration, and analysis.
Trust model 6 [13]	This model is defined the trust model into five components trust which are metrics, propagation, architecture, algorithm, and source trust. But still need to define type of trust evaluation (either based on the behaviour node or based on data of node) and type of attacks.
Trust model 7 Suggested	The suggested model used the most common characteristics which are (i) trust attributes, (ii) trust architecture, (iii) trust aggregation, (iv) trust distributed, (v) type of trust model (vi) type of attack. The previous models are not considering as an optimum model for the trust model because they consider some attributes while ignore other. However, the suggested model has considered all attributes that are required in each model.

TABLE 3. Trust architecture approaches.

Characteristic	**Centralized**	**Decentralized**	**Distributed**
Network Topology			
Trust Propagation	Cluster level (Path is direct from node to base station)	Cluster level (Path is from Member Cluster MC to Head Cluster HC to Base Station BS)	Node level (Path is distributed from node to neighbour node until reach to Base Station BS)
Maintenance	Low	Moderate	High
Fault Tolerance:	Low	Moderate	High
Stability	Unstable	Recovery potential	Quite stable
Development	Less complex	Moderate	Complex
Diversity	Low	High	High
Scalability	Low	Moderate	High
Evolution	Low	High	High

model related to trust propagation. Trust propagation refers to how to propagate trust information to other objects within the network. Generally, there are three types of trust propagation methods: centralized, distributed, and decentralized.

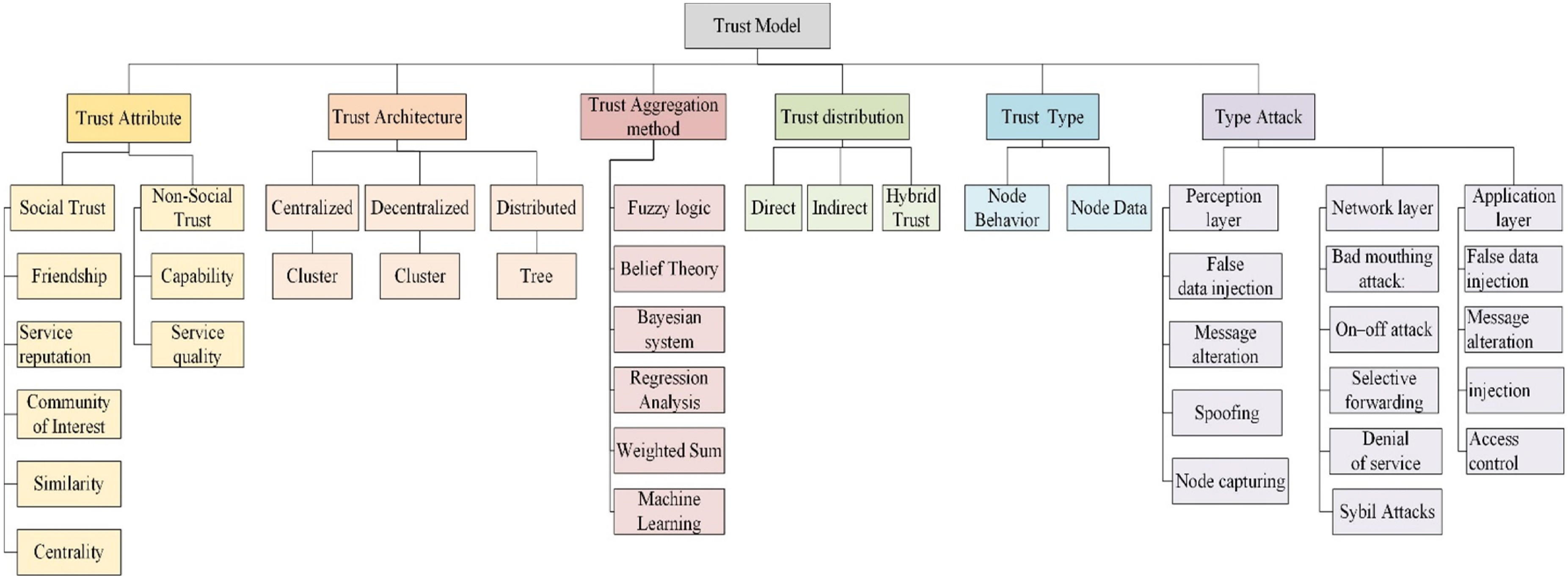


FIGURE 9. The proposed classification of trust models.

In the centralized method, a centralized entity manages all aspects of the trust model including the information about trust metrics, trust attributes, decision-making mathematical models, trust negotiation, algorithms, protocols, and provides the service on demand. Every trust service and request will pass via a central node that can be accessed by all other nodes in its domain [32].

On the other hand, in distributed trust evaluation method, each node should compute all aspects of the trust model locally by observing and exchanging trust reports with neighboring nodes.

In a distributed approach, the IoT users independently exchange trust matrices with neighbouring users without the interference of a centralized entity, which means the trust agents complete all necessary calculations locally.

For IoT applications, however, it is not enough to stick to one method, because sometimes the computation has to be done remotely and some needs to be done locally, based on the accessibility of resources. Therefore, a fully centralized model or a fully distributed model will not give satisfactory results, so alternatives between distributed and centralized methods should be considered. In this respect, the decentralized model, it can be considered as an optimum model for the trust evaluation. It is considered an alternative model to both distributed and centralized architecture, which combines the positive points of both [13], [27], [32].

In line with the literature, the author in [27] divided trust propagation into centralized and distributed, while the authors in [13] divided the trust architecture into centralized and decentralized. Based on this division, the trust architecture can be divided into centralized, distributed, and decentralized [32]. Table 3 demonstrates a comparison between the trust architectures.

C. TRUST AGGREGATION METHODS

Previous research efforts have tried to combine multiple models to take benefit of their advantages and at the same time try to alleviate their shortcomings. This clue has lately become more famous in the context of the IoT, where trust is more complicated due to a lot of aspects engaged in trust evaluation and trust establishment. Therefore, trust aggregation techniques can be used as approaches to inspect a trust level or trust score once all trust attributes (TAs) and trust metrics (TMs) are already collected and calculated [33]. It also indicates the assessment of trust assurance attained via reputation or self-observation feedback of other IoT objects [17]. The key algorithms and methods used to assess trust include particle swarm, fuzzy logic, Bayesian inference, and so on. Some researchers [28], [34], and [35], have proposed algorithms inspired by biologists, namely particle swarm optimization (PSO) and ant colony. Recently, a new algorithm for calculating the trustworthiness of the IoT has emerged, which is according to machine learning [14], [36], and [37]. Table 4 shows the comparison between these types of recent aggregation algorithms.

D. TRUST DISTRIBUTION

The trust distribution has been divided into direct trust, indirect trust, and hybrid trust. Direct trust is computed according to the interface between IoT devices and other systems. It represents a quantifiable value of the device's ability to finish the demanded task. It also depends on the historical record of the interaction between the two systems [33]. Indirect trust is the trust value achieved by an object from another object based on previous interaction experience. Other scientists and researchers utilized different terms to denote indirect trust, including feedback, rating, recommendation, and reputation [38]. The most commonly utilized source of trust is hybrid trust that combines direct trust and indirect trust [12]. Figure 10 points to these three types of trust sources utilized by current scientists and researchers [33] to employ a trust model in IoT devices.

E. TYPE OF TRUST MODEL

Through our research, we can observe that trust has been conceptualized based on node behaviour or node data [39], [40]. Most researchers develop their trust model according to the node behaviour [10], [11], [39], [41], [42] and few of them considered the node data [43], [44].

- **Node Behaviour Trust Model**: Most trust evaluation models build their trust based on characteristics of node behaviour such as forwarding packet, delay transmission packet, size packet. Moreover, these systems utilize a certain set of metrics like length/frequency of the transaction, certificate validity, reputation, community interest, cooperativeness, honesty to assess the trustworthiness of the end node and then to determine the trust relationship between the trustees and trustors [39]. The other general misunderstanding is that assuming the existence of node trust will ensure trust in data. This is undoubtedly different in several aspects, such as timeliness, the validity of data and other unique attributes to data which are often ignored in computing trust for end nodes [39].
- **Data Trust Model**: Current research identifies the key role of accurate data in the current era of the IoT. Data accuracy and quality directly affect model results and decision-making [43]. The rise in the number of linked systems on the IoT lets it difficult to establish data trust using conventional evaluation approaches [44]. In the IoT based on wireless sensor network applications, the functions of WSN are reporting, processing and data sensing, rather than learning information of nodes. Nevertheless, as the weakness of the wireless communication channel, an attacker can easily attack the transmission of information through the wireless link, eavesdrop, forge, tamper, and even initiate a denial-of-service attack. The spread of false data will cause serious damage and waste a lot of system energy [8], [45]. As mentioned above (node trust model), data trusted is ignored by many researchers. Therefore, it is very

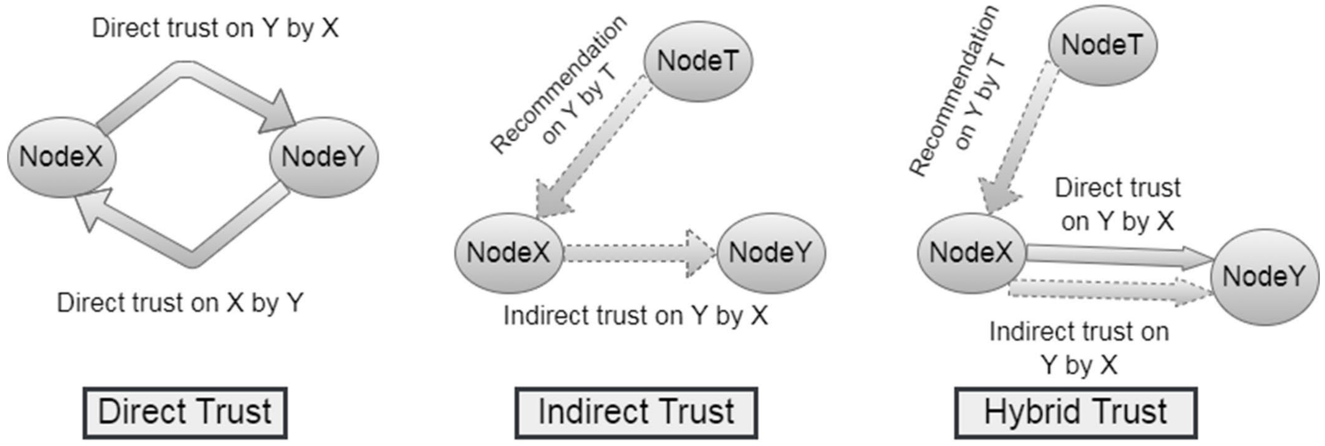


FIGURE 10. Trust distribution [33].

important to assess the trust value of data. The traditional data trust model used MAC (Message Authentication Code) to evaluate information in WSN. MAC can protect data integrity. However, once an attacker initiates fake data, these trust models will become invalid. Therefore, it needs a new trust model that can consider the trust model of nodes data and nodes behaviour at the same time [8].

F. TYPE ATTACK OF TRUST MODEL

In the IoT, sensors are distributed in all places to monitor the environment. Nevertheless, these entities are susceptible to a lot of security threats, which may cause serious issues in numerous fields, such as the medical field, where minor safety issues may threaten the lives of patients [46]. In this review, we are focusing on entities that misbehave, and these entities essentially intend to impact the quality of the information and efficiency of the communication in the IoT architecture layers (perception layer, application layer and network layer). Table 5 shows the description of the attack types.

VI. TRUST IN WSN AND RFID

WSN and RFID are two technologies that are mainly used in IoT and became the fundamental pillars of the IoT [47]. Both technologies focus on sensing and wireless communication, which are the two key requirements of the IoT [48].

WSN is composed of a group of dedicated autonomous sensors and actuators with wireless communication infrastructure. It is designed to control and monitor the physical or environmental conditions in different locations, coordinate data to the main location, and transmit control commands back to the desired through the network actuator location [49]. The WSN architecture consists of four components, namely the sensor node, the sink node, the transmission medium, and the control terminal. The data is collected from each sensor node and routed back to the sink node. These sink or receiver nodes can be connected to the Internet. Figure 11 shows the structure of a typical WSN [47].

RFID is an automatic identification technology that utilizes two essential kinds of equipment: a reader as the main body of communication, and a tag with a unique electronic code. The reader utilizes radio frequency (RF) signals to interrogate these tags, and the tags respond with their identification code (ID). The tag can also contain a sensor, in which case the tag will also backscatter the data from the sensor. The tag can be active (powered by a battery) or passive (harvesting energy from the RF signal of the reader) [49]. An RFID tag consists of an antenna, a chip, and every tag have a unique electronic code. Furthermore, RFID can store some information in the RFID tag according to the size of its storage space. RFID communication process includes signal encoding or decoding and modulation or demodulation [60].

A. TRUST EVALUATION MODEL IN WIRELESS SENSOR NETWORKS

Recently, WSN has become one of the largest benefit technologies and has attracted the attention of more and more researchers. Due to their functions of data gathering, transmission, and processing, sensor nodes can be installed in a lot of fields, such as health care, industrial security monitoring, battlefield detection, and environmental monitoring [61]. Nevertheless, because of the open environment and restricted energy, these sensors are exposed to several attacks, for example, an attacker capturing some normal nodes and trying to modify its behaviour by entering wrong data or decisions to mislead the entire network's decisions. Besides that, the sensor nodes might be procumbent to non-malicious faults, like insufficient residual energy and failure of wireless transceivers or elements, producing untrustworthy data generation [45]. Therefore, data aggregation is required in sensor networks to enhance the energy ratio. When the node is taken the erroneous or forged data transmitted by the faulty node, it will influence the results. Thus, the security and the trust of WSN is an important issue that needs to be resolved.

TABLE 4. Summary trust aggregation methods.

Reference	Aggregation Techniques	Main Features	Advantages	Limitation
[50], [51], [52], [8], [11], [53]	Fuzzy Logic-based	• Fuzzy logic: the trust is computed based on the past interaction of sensor nodes.	• Use fuzzy logic to quantify uncertain or inaccurate data. • The structure of the fuzzy logic system is simple and easy to understand.	• Fuzzy logic gives trust levels in the form of fuzzy terms such as "acceptable-unacceptable", good-bad", and "low-high" rather than providing accurate trust values.
[54], [55], [5]	Bayesian Methods	• Trust can be considered as Bayesian inference and be able to model as random variables in range [0, 1] after Beta distribution, which Belief discounting applied to define against malicious nodes such as bad-mouthing attack and ballot- stuffing attacks.	• The trust calculation in Bayesian inference is accurate and has no single point of failure.	• The calculation of Bayesian demands high memory and complex computations. • It can improve the security of every node but cannot improve the robustness of the system.
[31], [56], [27]	Weighted Sum	• Higher weights are assigned to nodes with higher transaction or reputation relevance. Therefore, objects that are closely related to the trustee have a higher weight. • Use similarity or credibility as the weight of indirect trust collection.	• Energy efficiency can limit the effects of malicious node attacks, such as bad-mouthing attacks, On/Off attacks, and conflict behaviour attacks. • There is no memory or computational complexity on ordinary sensor nodes.	• The trust evaluation is subjective. It is not appropriate to establish a recommended trust value through weighted average. • The computational cost of calculating the weighting factor is very high, and because the possibilities are unlimited, it is impractical.
[57], [10], [41], [38]	Belief Theory	• Belief theory (Evidence Theory or Dempster-Shafer Theory (DST)) is dealing with the logic of utilizing uncertainty and is associated with other methods such as imprecise probability theory.	• Dempster-Shafer (D-S) evidence theory can briefly express "uncertainty" and other significant concepts and make correct judgments by effectively incorporating various uncertain data.	• Due to the cooperation and communication with nodes, the trust evaluation process requires additional energy and time costs, and the memory cost also increases with the number of parameters, algorithm accuracy and network density. • The use of complex algorithms for the calculation process will lead to greater energy consumption.
[36], [37], [14]	Machine Learning	• The trust valuation is formalized as a classification issue and demonstrates a new method using machine learning technique. Firstly, the trust features vector is building based on the trust related factors. Then, the trust classifier is built by collecting sample data containing trust feature vectors and trust ratings.	• Identification of trends and patterns. • No human interference is required. • To deal with the multidimensional and huge amount of data	• In the process of machine learning, a large amount of data acquisition is required for the learning and training process. • Time and resources: The algorithm management data that helps manage all functions in the machine learning process and the use of certain data will take a long time if there are any errors in the correction process.
[58], [59]	Regression Analysis	• Regression analysis is a statistical operation to estimate the relationship between variables. It can be used to approximate the relationship between trust and a set of variables that characterize node behaviour.	• Regression analysis offers an estimation of the value of the dependent variable based on the value of the independent variable. • Regression analysis also assists to get a measurement of fault when utilizing the regression line as the basis for estimation. • Regression analysis assists to gain the measurement of the degree of correlation or association between two variables	• The regression relationship will change over time, which is called the parameter instability problem. The use of regressions specific to the investment environment results in the return of public information of relations that might negate their future usefulness. If regression assumption is infringed, hypothesis testing and prediction based on linear regression will be invalid.

Asymmetric encryption technology is broadly applied to deal with external attacks in the IoT [14]. However, due to complexity in the calculations and huge computational memory requirements, the restricted processing power, and resource constraints are not useful for WSN. In recent years, trust mechanisms have been regarded as an effective supplementary mechanism to guarantee the reliability of sensor networks [14]. According to historical behaviour, the trust value of the node can be estimated depending on the performance of a specific task to evaluate the node reliability. At present, numerous typical trust models have been presented for WSNs, which can originate from fuzzy logic, Dempster-Shaffer (D-S) evidence, Bayesian estimation, game theory, etc [62]. These models have detected malicious nodes via trust evaluation to a certain extent, providing a theoretical basis for more research.

In [50], a trust evaluation model based on entropy method was proposed to detect malicious nodes. They evaluated the direct and indirect trust values based on the attributes of the corresponding behavior nodes and they used the entropy method to define appropriate weight values. Their model can identify malicious nodes and effectively reduce the impact of malicious nodes, however, when the rate of malicious nodes increases, the efficiency of the model decreases.

In order to precisely evaluate the trust relationship between sensor nodes, it is necessary to design an appropriate trust estimation model to effectively resist attacks and bad behaviours [10]. A quantitative model of trust value was proposed to detect node behaviour in the WSN. A number of trust factors related to the behaviour of sensor nodes are selected. Each trust factor is found by the entropy method to avoid the influence of subjective settings. Moreover, the D-S theory is used to derive and synthesize trust, and the statistical factors of node behaviour are presented to modify the comprehensive results. The model has the ability to resist attacks and detect malicious nodes. The data packet forwarding security is achieved by the combination of the entropy method and D-S theory. However, this model uses a complex algorithm for computing processes which leads to greater energy consumption.

In [63], a trust model scheme based on Dumpster-Shafer Dempster-Shaffer (D-S) evidence theory is proposed. They consider the spatiotemporal correlation of data gathered by sensor nodes in neighbouring areas and approximate the trustworthiness of nodes. Based on the D-S theory, the trust model is established to count the number of interactive behaviours of trust, uncertainty, or distrust. It is also used to estimate the direct and indirect trust values and a flexible synthesis technique that accepts to compute the whole trust to classify the malicious nodes. This scheme has benefits over the conventional approaches in the identification of malicious nodes and data fusion accuracy. However, a better balance is needed to enhance energy efficiency, diminish redundant information, and guarantee the objectivity of credibility assessment.

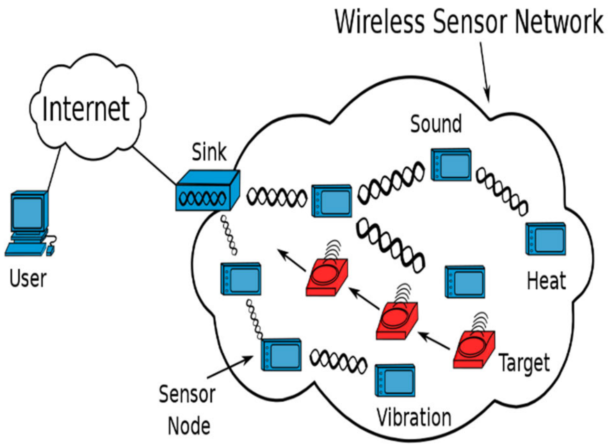


FIGURE 11. WSN components [47].

In [67], a group-based clustered wireless sensor network trust management scheme (GTMS) is proposed. This method is mainly used to decrease the cost of trust evaluation. GTMS requests less energy, memory, and communication overhead, and is considered more proper for large-scale sensor networks. The model has the ability to prevent and detect abnormal, selfish, and malicious nodes. GTMS used security flexibility analysis, which analyses the flexibility of GTMS protocol against trust management attacks. However, GTMS uses more than a few mechanisms to enhance the resource efficiency of clustered WSNs. This method depends on a broadcast-based strategy to gather feedback between cluster members (CMs), which needs a lot of resources and power consumption.

The Agent-Based Trust and Reputation management scheme (ATRM) is proposed to administer the trust and reputation of the node with the least overhead in terms of extra messages and delay time. The major contribution of ATRM is the notability of localized trust and reputation management strategies that can reduce acquisition and communication cost delays [68]. However, the ATRM needs each node to have a locally held mobile agent which is in charge of administering the trust and reputation of its hosting node.

In [52], a dependable and lightweight trust system (LDTS) is proposed for clustered WSN based on the nodes' identities (roles) in the clusters. The authors developed a trust evaluation scheme for cooperation between cluster members and cluster heads, which uses an adaptive weighting method for trust aggregation. This scheme reduces communication overhead by cancelling feedback between cluster members or cluster- heads, which leads to reducing the effect of malicious nodes.

A data fusion mechanism and a trust evaluation model based on trust is proposed in [40]. In this model, the trust value is computed by the simple average of the weight of the comprehensive trust degree. The comprehensive trust includes data trust, behaviour trust, and historical trust. Data trust can be computed by processing sensor data, while behaviour trust can be obtained based on the behaviour of nodes during perception and forwarding packets. The initial value of the historical trust is set to the maximum and is updated with the comprehensive trust. Comprehensive trust is attained through the weighted calculation for historical trust, behaviour trust and data trust. Then the trust value is recorded in the list and the data fusion process is implemented based on this trust list. This trust model can be better to control the status of nodes and can enhance the survival time of the node. Moreover, the trust model has a better anomaly detection rate than the other models, because this model includes three factors: data, behaviour, and historical inertia.

In [38], dynamic trust evaluation is realized by dynamically adjusting the weights of direct trust and indirect trust and updating mechanism parameters. Direct trust is computed based on energy trust, data trust and communication trust, as well as punishment factors and adjustment functions. Indirect trust is recommended and assessed by a third-party trust. Moreover, comprehensive trust is measured by assigning dynamic weights to direct trust and indirect trust and combining them. They also proposed an update mechanism based on sliding windows and induced ordered weighted average operators to improve flexibility.

Recently, WSN data aggregation technology using external mobile elements (ME) has been presented. A trust scheme was introduced in [53] to assign the task of aggregating data to the most reliable external ME in the WSN to diminish data loss. The program accomplishes well in decreasing data and energy loss. Figure 12 shows that the WSN is divided into fixed grid clusters, and the passing mobile elements act as the cluster head ME.

In [34], an ant colony optimization algorithm for secure routing (ACOSR) based on the WSN trust-aware model was proposed. The authors considered internal attacks such as black hole attacks, ACOSR uses a trust evaluation model to effectively isolate malicious nodes based on node behaviour, reduce packet loss rates, and establish secure routes. Furthermore, by using the remaining energy of the node as the main factor of the chosen probability, the average energy of the node is considered when updating the pheromone, which can effectively balance the energy consumption between all nodes and decrease the average energy consumption of the entire node.

B. TRUST EVALUATION MODEL IN RFID

The term IoT originates from the requirement to establish a heterogeneous environment in which systems with different processing abilities can communicate and cooperate in a smart environment that is transparent to users [69]. In the context of the IoT and current research, RFID technology is considered to be the basic technology of the IoT. RFID has been broadly utilized in a lot of different fields, such as supply chain management, retailing, pharmaceutical production, and logistics [49]. The utilization of RFID technology in a distributed and challenging environment usually results in a multi-domain RFID device, where security problems such as reader revocation, data access permissions,

TABLE 5. Description of attack types.

Reference	Attack Type	Trust Type	Affected Layer	Description
[5]	Bad/good mouthing	Communication trust	Network Layer	Bad nodes might give unfair good or bad opinions to create false compliments and deface good nodes respectively.
[3], [29]	False data injection	Data fusion trust, Communication trust and Data perception trust	Application layer, Network layer and Perception layer	It might insert incorrect reports to damage the results of data fusion.
[3]	Message alteration	Data fusion trust, Communication trust and Data perception trust	Application layer, Network layer and Perception layer	It might change messages to fool legal entities.
[27]	Bush telegraph	Data fusion trust, Communication trust and Data perception trust	Application layer, Network layer and Perception layer	It is a particular case of a message change attack, where malicious entities might perform little tolerable changes in each round.
[36], [64]	Message suppression	Data fusion trust, Communication trust and Data perception trust	Application layer, Network layer and Perception layer	It might drop messages to block other parties from receiving consistent information at the right time. It operates in an alternative way to preserve a certain level of trust.
[5], [30]	Selective forwarding	Communication trust	Network layer	It only sends low-cost or low-importance messages
[36], [64]	On-off attack	Communication trust	Network layer	It acts in an alternative way to keep a certain level of trust.
[36], [42]	Newcomer	Data fusion trust And Communication trust	Network layer and Application layer	The entities can delete all their bad records to accede to the network as a new node.
[39], [17]	Impersonation	Data fusion trust and Communication trust	Network layer and Application layer	It might pretend to be another entity to use its features.
[5], [3], [65]	Denial of service	Communication trust	Network layer	It sends continuous messages to block communication channels and disrupt network performance.
[3], [5], [66], [12]	Sybil	Communication trust	Network layer	The same entity might transmit several messages from different locations with various identities.

tags, and reader authentication, have become management challenges.

A common case is the enabled aircraft scenario, where on board RFID tags and readers will be linked to different ground systems across several management domains for logistics and access control. The maintenance history of the part included in the on-board RFID tag is the airline's proprietary information, and access must be kept prohibiting deliberate or random access by unlawful RFID readers in other administrative domains.

Several data protection and encrypted authentication methods have been presented to overcome the security issues in [70]. Despite the traditional encryption mechanism that can offer data integrity, node authentication, and data confidentiality for exchanged messages, and protect the system from external attacks, they cannot deal with internal attackers [71]. An example of an internal attacker, a reader owning legitimate encryption keys which can effortlessly launch an internal attack inside the system by changing data or injecting false information without being recognized.

An open RFID system can only be effective when the system can trust and collaborate with each other. The open system environment is also evolving. Therefore, trust and cooperation are essential to be regularly maintained to respond to alerts. RFID is becoming an everywhere computing technology, bringing privacy and security threats. Moreover, the use of RFID technology in a challenging and distributed environment usually leads to a multi-domain RFID system, where there is no past interaction between entities from heterogeneous domains or the establishment of trust between pre-agreed strategies is a challenge. The following sections describe the previous work of the trust model in the RFID system.

In [64], the authors proposed Computational Trust Management (CTM), which provides unqualified security in preventing and detecting cloning and fake attacks by focusing on supply chain business information transactions between partners. Taking RFID label wine as an example, their trust framework consists of seven layers of authenticity, privacy, prevention, detection, monitoring and auditing, detection-hard trust, experience, and soft trust. This work offers a good integration, detection and prevention, and soft trust model to improve data sharing and implement a secure authorization model between supply chain trading partners.

Research in [70] proposed an overall approach that takes into account privacy, trust, and security (PTS) together. This model deployed a lightweight-based encryption subsystem to deal with trusted computing, a security-based subsystem to offer integrity and trust confirmations, and a privacy improved system (anonymizer) to solve privacy matters for RFID systems. The authors have studied earlier RFID protocols to highlight the significance of privacy, trust, and security in RFID systems. It is recommended to use security solutions such as encryption technology to protect the data in the communication channel. It is also recommended to verify the integrity of the platform to protect the RFID system from data hijacking and masquerading attacks. Privacy protection solutions are also emphasized and recommended to offer intractability for the RFID system. On the whole, the RFID system with privacy, trust, and security will protect

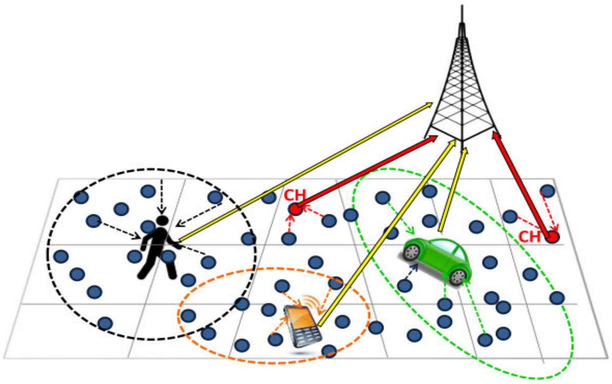


FIGURE 12. WSN divided into fixed grid clusters [53].

the RFID system via trusted computing, anonymization, and encryption.

The importance of data anonymity must be strengthened through integrity verification to prevent any untrusted platform from becoming a threat to others. The integrity verification utilized for the trust establishment of the system is very important in the RFID system. Authors in [72] proposed a combination approach for trust and privacy of future integrated RFID systems. They highlighted the safeguard of data at all layers in the RFID system. Their method in this hybrid RFID model is unique due to its considering potential subjects and efforts to tackle them in a unified and incorporated manner. They emphasized the integration of a trusted platform module (TPM) for trust and an anonymizer for privacy preservation. This solution is appropriate to be utilized for defensive the near field communication (NFC-based) mobile phones and future RFID systems. This model can resist being attacked or hijacked by an adversary.

System integrity verification of RFID components, readers, back-end servers, and tags must be implemented to improve system trust. Authors in [73], presented a back-end server and RFID reader with embedded trusted computing technology to improve the measurement and verification of system integrity. They also introduced a trusted platform module (TPM) and Advanced Encryption Standard (AES) encryption used to encrypt the data transmission in the trusted RFID system, and mutual certification for the trusted RFID protocol.

In [74], two RFID authentication phases, namely the initialization (IA) and termination (TA) phases were proposed, which are used to pass the tag's value without using the real tag's values (key and identifier). They performed identity verification with the server to enhance RFID privacy and security. The IA stage technology decides earlier whether to admit or terminate the authentication session. After the tags and servers successfully pass the IA stage, they use the authentication based on [75] to send and receive the tag's identification value. The TA stage is to ensure that the server knows the authenticity and update status of the tag. Adding the IA and TA phases between the server and the tag improves the RFID privacy and security authentication protocol.

In [41], they proposed a hybrid method (group-based method and collaboration method) and security check switching (SCH)-based identification technology for mobile RFID systems. The presented protocol offers customization and flexibility, to ensure the secure and scalable deployment of RFID systems to support powerful distributed structures, such as the IoT. The protocol uses integrated malware detection technology to provide additional protection against malware.

Research in [71] proposed a multi-domain trust model. The presented trust model offers a hierarchical trust framework, which includes multiple trust evaluation and establishment methods. There are two layers of trust in the framework: the RFID reader trust layer and the authentication center trust layer. In the RFID reader trust layer, they use two schemes to assess the trustworthiness of the reader: the scheme based on D-S evidence theory (D-S scheme) and verification interaction proof (VIP scheme). In the certification center, the trust layer is used for the management center to centrally manage the trust level of the certification center. This model compared their schemes with the Bayes-based scheme. The model shows that the VIP scheme is superior to all other mechanisms because it detects earlier misbehaviours of nodes, while the Bayes-based scheme has the lowest detection rate for malicious events.

Trust evaluation model of the previous works in WSN and RFID technologies have been summarised in Table 6 based on several characteristics including evaluating trust based on characteristics of (node behaviour, node data and energy consideration), trust metrics, trust architecture, aggregation method/methodology, trust source, type of attack, percentage of malicious node detection, and analysis energy consumption.

VII. RESEARCH CHALLENGES AND DIRECTIONS

Based on the studies presented in Table 6, we summarised the research challenges and directions of the trust evaluation model.

(a) Energy efficiency is a major research challenge, especially in trust computing where IoT nodes have limited energy to compute goals. From Table 4, few researchers have considered the energy efficiency of trust evolution models. However, due to the current progress of IoT, energy efficiency needs to be further improved to adapt to the rapid growth of heterogeneous IoT devices.

(b) The trust evaluation model is primarily based on node behaviour or data, and thus is unreliable because it only considering one side of the trust type. On the other hand, consider both types of trust, node behaviour, and node data, when developing a trust evaluation model, the credibility of the trust evaluation model will be improved.

(c) Most of the current trust models used complex algorithms to compute the trust value. Therefore, a lightweight and simple trust model should be developed to maintain minimal resource consumption such as low memory, low processor, and low power supply.

TABLE 6. Trust evaluation model of the previous works (*note: (√) consider, (X) not consider).

Ref	Type of technology	Evaluating trust based on characteristics of			Trust metrics	Trust Architecture	Aggregation method/ Methodology	Trust source	Type of attack	Percentage of Malicious node detection	Analysis Energy consumption
		Node Behaviour	Node Data	Energy consideration							
[42]	WSN	√	X	X	Data repetition rate, Packet size abnormality, Data correlation, The, Volatility of transmission delay	Distributed (Node level)	Weighted sum method and entropy-based weight assignment	Hybrid (direct and indirect trust)	on/off attack, DoS attack, data forgery attack and forwarding attack	About 70% when malicious nodes are 40%	X
[10]	WSN	√	X	X	Integrity Factor, Delay Factor, Consistency, Repetition Rate Factor, and Packet Forwarding Capacity	Distributed (node)	Dempster–Shafer evidence theory and Entropy theory	Hybrid (direct and indirect trust)	good and bad-mouthing attack, on/off attack, DoS attack, data forgery attack, and selective forwarding attack	About 0.8% when malicious nodes are 40%	The average energy consumption(0.5J) Number node500
[40]	WSN	√	√	X	Behaviour trust, data trust, and historical trust.	Centralized (cluster)	Weighted sum method	Hybrid (direct and indirect trust)	malicious, selfish, and faulty Attacks	About 0.9% when malicious nodes more 0.7%	The average of the energy saving ratio
[52]	WSN	√	X	X	resource efficiency and dependability of a trust system	Decentralized (cluster)	self-adaptive weighted method	Hybrid (direct and indirect trust)	malicious, selfish, and faulty Attacks	X	Improve efficient of system less memory and communication overhead as m
[38]	WSN	√	√	X	Sensing Data, behaviour of node and residual energy factor	Distributed (node)	Dynamic Weighted sum method	Hybrid (direct and indirect trust)	On-off attack, attack on information and Black hole attack	About 85% when malicious nodes are 40%	X
[63]	WSN	√	X	X	spatiotemporal correlation of the data collected by sensor nodes	hierarchical topology	Dempster–Shafer evidence theory and a flexible synthesis method	Hybrid (direct and indirect trust)	detection of malicious nodes, bad mouthing attack, and on–off attack	About 89%when malicious nodes are 30%	the energy-exhausted node is relatively slow with the increase in the node density
[61]	WSN	X	√	√	Reducing number of transmitted packet for normal and error data. Reducing the size of transmitted data	Centralized (data transmitted direct from sensor node to base station)	Simple linear regression. adaptive threshold and Multiple Linear Regression model	Direct trust	Injected error data	About 97% of error data injection detected	The average of the energy saving is 98%
[53]	WSN	X	√	X	Network Energy Loss, Network Coverage, and Data delivery ratio represents	Centralized (cluster External Element proposed as Cluster Head (CH))	Beta distribution model which	Hybrid (direct and indirect trust)	Detect misbehaviour of Cluster Head (CH))	X	minimize the energy loss in the network about 5j at the end of round
[41]	WSN	√	X	X	Availability, consistency, delivery, strictness, Packet receives and send	Distributed (node)	fuzzy theory, D-S evidence theory	Hybrid (direct and indirect trust)	Selfish and malicious nodes.	When the increasing of malicious nodes, the trust value increase because the proposed scheme takes fuzziness and subjectivity of trust in consideration.	X
[34]	WSN	X	X	√	Residual energy of sensor node	Distributed (node)	Bayesian Statistical theory formation entropy theory Ant colony optimization algorithm (ACO)	Hybrid (direct and indirect trust)	Black hole attack	X	balance the energy expenditure among all sensor nodes and reduce the average energy consumption of
[71]	RFID	√	X	X	Relationships between RFID components security, and accuracy.	Hierarchy	-D-S (Dempster-Shafer) theory verification of interaction proofs (VIP)	Hybrid (direct and indirect trust)	Malicious behaviours of node(Reader)	The malicious behavior detection increases as the time increases	X
[70]	RFID	X	√	X	Data trust , privacy, and security	X	-lightweight Encryption (AES). -Privacy-preserving protection via Anonymizer technique. -Integrity verification and attestation.	Direct Trust	Man in the middle attacks. Replaying or forging data. Traceability.	X	X
[54]	RFID	X	√	X	Data trust and privacy information.	X	-lightweight Encryption (ECC). -Privacy preserving protection via Anonymizer. -Integrity verification and attestation.	Direct Trust	Malicious codes. Eavesdropping attack Traceability. Man in the middle attacks.	X	X
[55]	RFID	√	X	X	Reliability Data	X	A mutual attestation by using (TPM), and AES encryption.	Direct Trust	Relay attack. Traceability. Man in the middle attacks.	X	X
[74]	RFID	X	√	X	Security and privacy.	X	Initialization of Authentication Stage. Authentication protocol (Kaul and Awasthi's) Termination of Authentication (TA). Update stage	X	Denial of Service Attack (DoS). Replay and Parallel Session Attack. Man-in-the-Middle Attack. Cloning Attack. Tag Anonymity and Intractability.	X	X

(d) IoT devices are always exposed to several types of attacks in the IoT layers. Therefore, the trust model should consider the development of trust computation methods to detect different types of attacks in the IoT layers.

(e) From Table 6, the most popular and simplest trust aggregation and trust reasoning is to apply the use of static weighted sums to form trust. However, due to the complexity of the IoT environment, this solution is not smart enough. Therefore, new research is needed to use more effective trust formation methods, including dynamic weighted summation, machine learning, and regression analysis.

VIII. CONCLUSION

The purpose of this paper is to provide researchers with an overview of the existing trust evaluation models for WSN and RFID in the IoT environment. The main features of trust are elaborated. The classification of trust models has been discussed in detail and a combination classification for trust models is suggested. The suggested classification is based on the trust characteristics including trust attributes, trust architecture, trust distribution, trust aggregation method, trust model type, and attack type. A comparison of trust architecture approaches in the form of centralized, distributed and decentralized approaches are highlighted. Since neither centralized nor distributed models yield satisfactory results, decentralized models are introduced as an alternative to distributed and centralized approaches, which combines the positive points of both. The aggregation methods which are Fuzzy Logic, Bayesian Methods, Weighted Sum, Belief Theory, Machine Learning, and Regression Analysis methods have been explained and summarised in terms of techniques, main features, advantages, and limitations. The Weighted Sum method is the most common method used because it considers as lightweight technique. A description of the different types of attacks are presented in terms of the nature of the attacks, the type of trust, the layers involved, and the attack descriptions. The trust evaluation models in WSN and RFID are selected to discuss because these two technologies are mainly used in IoT applications. The summary of recent work on the trust evaluation model of WSN and RFID is tabulated. Finally, the paper concluded with a discussion of the current work's challenges as well as some future research possibilities.

REFERENCES

[1] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Data collection and wireless communication in Internet of Things (IoT) using economic analysis and pricing models: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2546–2590, 4th Quart., 2016, doi: 10.1109/COMST.2016.2582841.

[2] E. Oriwoh and M. Conrad, "'Things' in the Internet of Things: Towards a definition," *Int. J. Internet Things*, vol. 4, no. 1, pp. 1–5, 2015.

[3] I. U. Din, M. Guizani, B.-S. Kim, S. Hassan, and M. K. Khan, "Trust management techniques for the Internet of Things: A survey," *IEEE Access*, vol. 7, pp. 29763–29787, 2019, doi: 10.1109/ACCESS.2018.2880838.

[4] S. F. A. Mon, S. G. Winster, and R. Ramesh, "Trust model for IoT using cluster analysis: A centralized approach," *Wireless Pers. Commun.*, vol. 127, no. 1, pp. 715–736, Nov. 2022, doi: 10.1007/s11277-021-08401-7.

[5] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, Jun. 2014, doi: 10.1016/j.jnca.2014.01.014.

[6] M. Eisenhauer, P. Rosengren, and P. Antolin, *The Internet of Things*. New York, NY, USA: Springer, 2010.

[7] N. Djedjig, D. Tandjaoui, I. Romdhani, and F. Medjek, "Trust management in the Internet of Things," in *Security and Privacy in Smart Sensor Networks*. Hershey, PA, USA: IGI Global, 2018, pp. 122–146, doi: 10.4018/978-1-5225-5736-4.ch007.

[8] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, "Management and applications of trust in wireless sensor networks: A survey," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 602–617, May 2014, doi: 10.1016/j.jcss.2013.06.014.

[9] F. Azzedin and M. Ghaleb, "Internet-of-Things and information fusion: Trust perspective survey," *Sensors*, vol. 19, no. 8, p. 1929, Apr. 2019, doi: 10.3390/s19081929.

[10] Y. Yu, Z. Jia, W. Tao, B. Xue, and C. Lee, "An efficient trust evaluation scheme for node behavior detection in the Internet of Things," *Wireless Pers. Commun.*, vol. 93, no. 2, pp. 571–587, Mar. 2017, doi: 10.1007/s11277-016-3802-y.

[11] A. Khalil, N. Mbarek, and O. Togni, "Fuzzy logic based security trust evaluation for IoT environments," in *Proc. IEEE/ACS 16th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2019, pp. 1–8, doi: 10.1109/AICCSA47632.2019.9035294.

[12] Z. M. Aljazzaf, M. Perry, and M. A. M. Capretz, "Online trust: Definition and principles," in *Proc. 5th Int. Multi-Conf. Comput. Global Inf. Technol.*, Sep. 2010, pp. 163–168, doi: 10.1109/ICCGI.2010.17.

[13] W. Najib and S. Sulistyo, "Survey on trust calculation methods in Internet of Things," *Proc. Comput. Sci.*, vol. 161, pp. 1300–1307, Jan. 2019, doi: 10.1016/j.procs.2019.11.245.

[14] U. U. K. Jayasinghe, "Trust evaluation in the IoT environment," Ph.D. dissertation, Dept. Comput. Sci., Liverpool John Moores Univ., Liverpool, U.K., 2018.

[15] P. Das and S. Debnath, "A trust computing model for future generation networks," in *Proc. 11th Int. Conf. Comput., Commun. Netw. Technol.*, Jul. 2020, pp. 1–4, doi: 10.1109/ICCCNT49239.2020.9225462.

[16] W. Abdelghani, C. A. Zayani, and I. Amous, "Social media: The good, the bad, and the ugly," *Inf. Syst. Frontiers*, vol. 20, pp. 419–423 Mar. 2018.

[17] J. Guo, I.-R. Chen, and J. J. P. Tsai, "A survey of trust computation models for service management in Internet of Things systems," *Comput. Commun.*, vol. 97, pp. 1–14, Jan. 2017, doi: 10.1016/j.comcom.2016.10.012.

[18] A. Altaf, H. Abbas, F. Iqbal, and A. Derhab, "Trust models of Internet of Smart Things: A survey, open issues, and future directions," *J. Netw. Comput. Appl.*, vol. 137, pp. 93–111, Jul. 2019, doi: 10.1016/j.jnca.2019.02.024.

[19] G. Fortino, L. Fotia, F. Messina, D. Rosaci, and G. M. Sarné, "Trust and reputation in the Internet of Things: State-of-the-art and research challenges," *IEEE Access*, vol. 8, pp. 60117–60125, 2020, doi: 10.1109/ACCESS.2020.2982318.

[20] Z. Yan and S. Holtmanns, "Trust modeling and management: From social trust to digital trust," in *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions*, R. Subramanian, Ed. Hershey, PA, USA: IGI Global, 2008.

[21] Z. Yan and C. Prehofer, "Autonomic trust management for a component-based software system," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 6, pp. 810–823, Nov. 2011, doi: 10.1109/TDSC.2010.47.

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

[23] I. Pranata, G. Skinner, and R. Athauda, "A holistic review on trust and reputation management systems for digital environments," *Int. J. Comput. Inf. Technol.*, vol. 1, no. 1, pp. 44–53, 2012. [Online]. Available: http://ijcit.com/archives/volume1/issue1/Paper010106.pdf

[24] F. Moyano, C. Fernandez-Gago, and J. Lopez, "A framework for enabling trust requirements in social cloud applications," *Requirements Eng.*, vol. 18, no. 4, pp. 321–341, Nov. 2013, doi: 10.1007/s00766-013-0171-x.

[25] C. Kolias, W. Meng, G. Kambourakis, and J. Chen, "Security, privacy, and trust on Internet of Things," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 10–13, Feb. 2019, doi: 10.1155/2019/6452157.

[26] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for Internet of Things: A survey," *J. Netw. Comput. Appl.*, vol. 66, pp. 198–213, May 2016, doi: 10.1016/j.jnca.2016.03.006.

[27] J. Guo and I.-R. Chen, ''A classification of trust computation models for service-oriented Internet of Things systems,'' in *Proc. IEEE Int. Conf. Services Comput.*, Jun. 2015, pp. 324–331, doi: 10.1109/SCC.2015.52.

[28] H. Nunoo-Mensah, K. O. Boateng, and J. D. Gadze, ''The adoption of socio- and bio-inspired algorithms for trust models in wireless sensor networks: A survey,'' *Int. J. Commun. Syst.*, vol. 31, no. 7, p. e3444, May 2018, doi: 10.1002/dac.3444.

[29] N. Djedjig, D. Tandjaoui, I. Romdhani, and F. Medjek, ''Trust management in the Internet of Things,'' in *Human-Centric Computing and Information Sciences*, vol. 9, no. 1. Berlin, Germany: Springer, 2018, pp. 122–146.

[30] B. R. Ray, J. Abawajy, and M. Chowdhury, ''Scalable RFID security framework and protocol supporting Internet of Things,'' *Comput. Netw.*, vol. 67, pp. 89–103, Jul. 2014, doi: 10.1016/j.comnet.2014.03.023.

[31] F. Bao and I.-R. Chen, ''Trust management for the Internet of Things and its application to service composition,'' in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2012, pp. 1–6, doi: 10.1109/WoWMoM.2012.6263792.

[32] C. Ye, W. Cao, and S. Chen, ''Security challenges of blockchain in Internet of Things: Systematic literature review,'' *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 8, p. e4177, Aug. 2021, doi: 10.1002/ett.4177.

[33] V. Suryani and S. Widyawan, ''A survey on trust in Internet of Things,'' in *Proc. 8th Int. Conf. Inf. Technol. Electr. Eng. (ICITEE)*, Oct. 2016, pp. 1–6, doi: 10.1109/ICITEED.2016.7863238.

[34] Y. Wang, M. Zhang, and W. Shu, ''An emerging intelligent optimization algorithm based on trust sensing model for wireless sensor networks,'' *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, p. 145, Dec. 2018, doi: 10.1186/s13638-018-1174-6.

[35] R. R. Sahoo, A. R. Sardar, M. Singh, S. Ray, and S. K. Sarkar, ''A bio inspired and trust based approach for clustering in WSN,'' *Natural Comput.*, vol. 15, no. 3, pp. 423–434, Sep. 2016, doi: 10.1007/s11047-015-9491-8.

[36] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, ''IoT security techniques based on machine learning,'' 2018, *arXiv:1801.06275*.

[37] U. Jayasinghe, G. M. Lee, T.-W. Um, and Q. Shi, ''Machine learning based trust computational model for IoT services,'' *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 39–52, Jan. 2019, doi: 10.1109/TSUSC.2018.2839623.

[38] Z. Ye, T. Wen, Z. Liu, X. Song, and C. Fu, ''An efficient dynamic trust evaluation model for wireless sensor networks,'' *J. Sensors*, vol. 2017, pp. 1–16, Jan. 2017, doi: 10.1155/2017/7864671.

[39] U. Jayasinghe, A. Otebolaku, T.-W. Um, and G. M. Lee, ''Data centric trust evaluation and prediction framework for IoT,'' in *Proc. ITU Kaleidoscope, Challenges Data-Driven Soc.*, Apr. 2018, pp. 1–7, doi: 10.23919/ITU-WT.2017.8246999.

[40] Z. Chen, L. Tian, and C. Lin, ''Trust model of wireless sensor networks and its application in data fusion,'' *Sensors*, vol. 17, no. 4, p. 703, Mar. 2017, doi: 10.3390/s17040703.

[41] R. Feng, X. Xu, X. Zhou, and J. Wan, ''A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory,'' *Sensors*, vol. 11, no. 2, pp. 1345–1360, Feb. 2011, doi: 10.3390/s110201345.

[42] X. Yin and S. Li, ''Trust evaluation model with entropy-based weight assignment for malicious node's detection in wireless sensor networks,'' *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, p. 198, Dec. 2019, doi: 10.1186/s13638-019-1524-z.

[43] N. A. M. Alduais, J. Abdullah, A. Jamil, L. Audah, and R. Alias, ''Sensor node data validation techniques for realtime IoT/WSN application,'' in *Proc. 14th Int. Multi-Conf. Syst., Signals Devices (SSD)*, Mar. 2017, pp. 760–765, doi: 10.1109/SSD.2017.8166984.

[44] J. Byabazaire, G. O'Hare, and D. Delaney, ''Data quality and trust: Review of challenges and opportunities for data sharing in IoT,'' *Electronics*, vol. 9, no. 12, p. 2083, Dec. 2020, doi: 10.3390/electronics9122083.

[45] N. A. M. Alduais, J. Abdullah, A. Jamil, L. Audah, and R. Alias, ''Effect of data validation schemes on the energy consumptions of edge device in IoT/WSN,'' in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 77–81, doi: 10.1109/IWCMC.2018.8450460.

[46] D. Airehrour, ''A trust based routing framework for the Internet of Things,'' Ph.D. dissertation, Dept. IT SE, AUT, Auckland, New Zealand, 2017.

[47] W. Ji, L. Li, and W. Zhou, ''Design and implementation of a RFID reader/router in RFID-WSN hybrid system,'' *Futur. Internet*, vol. 10, no. 11, pp. 1–12, 2018, doi: 10.3390/fi10110106.

[48] H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, ''A review of IoT sensing applications and challenges using RFID and wireless sensor networks,'' *Sensors*, vol. 20, no. 9, p. 2495, Apr. 2020, doi: 10.3390/s20092495.

[49] B. Zhang, K. Hu, and Y. Zhu, ''Network architecture and energy analysis of the integration of RFID and wireless sensor network,'' in *Proc. Chin. Control Decis. Conf.*, May 2010, pp. 1379–1382, doi: 10.1109/CCDC.2010.5498193.

[50] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, ''TRM-IoT: A trust management model based on fuzzy reputation for Internet of Things,'' *Comput. Sci. Inf. Syst.*, vol. 8, no. 4, pp. 1207–1228, 2011, doi: 10.2298/csis110303056c.

[51] G. M. Lee and N. B. Truong, ''A reputation and knowledge based trust service platform for trustworthy social Internet of Things,'' in *Proc. 19th Int. Conf. Innov. Clouds*, Mar. 2016, pp. 104–111.

[52] F. Z. X. Li and J. Du, ''LDTS: A lightweight and dependable trust system for clustered wireless sensor networks,'' *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 924–935, Jun. 2013.

[53] B. A. Ali, H. M. Abdulsalam, and A. AlGhemlas, ''Trust based scheme for IoT enabled wireless sensor networks,'' *Wireless Pers. Commun.*, vol. 99, no. 2, pp. 1061–1080, Mar. 2018, doi: 10.1007/s11277-017-5166-3.

[54] F. Bao, I.-R. Chen, and J. Guo, ''Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems,'' in *Proc. IEEE 11th Int. Symp. Auto. Decentralized Syst. (ISADS)*, Mar. 2013, pp. 1–7, doi: 10.1109/ISADS.2013.6513398.

[55] I.-R. Chen and J. Guo, ''Dynamic hierarchical trust management of mobile groups and its application to misbehaving node detection,'' in *Proc. 28th Int. Conf. Adv. Inf. Netw. Appl.*, May 2014, pp. 49–56, doi: 10.1109/AINA.2014.13.

[56] F. Bao and I.-R. Chen, ''Dynamic trust management for Internet of Things applications,'' in *Proc. Int. Workshop Self-Aware Internet Things*, Sep. 2012, pp. 1–6, doi: 10.1145/2378023.2378025.

[57] R. Feng, S. Che, X. Wang, and N. Yu, ''Trust management scheme based on D-S evidence theory for wireless sensor networks,'' *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 6, Jun. 2013, Art. no. 948641.

[58] J. Guo, ''Trust-based service management of Internet of Things systems and its applications,'' ETD, Virginia Tech, 2018.

[59] Y. Wang, Y.-C. Lu, I. Chen, J. Cho, A. Swami, and C. Lu, ''LogitTrust: A logit regression-based trust model for mobile ad hoc networks,'' in *Proc. 6th ASE Int. Conf. Privacy, Secur., Risk Trust*, 2014, pp. 1–10.

[60] N. Pan, ''Integration of RFID and industrial WSNs to create a smart industrial environment,'' Ph.D. dissertation, Univ. Western Ontario, ON, Canada, 2018.

[61] N. A. M. Alduais, J. Abdullah, and A. Jamil, ''RDCM: An efficient real-time data collection model for IoT/WSN edge with multivariate sensors,'' *IEEE Access*, vol. 7, pp. 89063–89082, 2019, doi: 10.1109/ACCESS.2019.2926209.

[62] I.-R. Chen, F. Bao, and J. Guo, ''Trust-based service management for social Internet of Things systems,'' *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 6, pp. 684–696, Nov. 2016, doi: 10.1109/TDSC.2015.2420552.

[63] W. Zhang, S. Zhu, J. Tang, and N. Xiong, ''A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks,'' *J. Supercomput.*, vol. 74, no. 4, pp. 1779–1801, Apr. 2018, doi: 10.1007/s11227-017-2150-3.

[64] M. Mahinderjit-Singh and X. Li, ''Computational model for trust management in RFID supply chains,'' in *Proc. IEEE 6th Int. Conf. Mobile Adhoc Sensor Syst.*, Oct. 2009, pp. 734–740, doi: 10.1109/MOBHOC.2009.5336926.

[65] V. R. S. Dhulipala, N. Karthik, and R. Chandrasekaran, ''A novel heuristic approach based trust worthy architecture for wireless sensor networks,'' *Wireless Pers. Commun.*, vol. 70, no. 1, pp. 189–205, May 2013, doi: 10.1007/s11277-012-0688-1.

[66] M. Ammar, G. Russello, and B. Crispo, ''Internet of Things: A survey on the security of IoT frameworks,'' *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018, doi: 10.1016/j.jisa.2017.11.002.

[67] S. K. Mubarak, ''Advanced lightweight, dependable and secure trust system for clustered wireless sensor networks,'' in *Proc. Int. Conf. Innov. Inf., Embedded Commun. Syst. (ICIIECS)*, Mar. 2015, pp. 1–4, doi: 10.1109/ICIIECS.2015.7193162.

[68] H. Chen, H. Wu, J. Hu, and C. Gao, ''Agent-based trust management model for wireless sensor networks,'' in *Proc. Int. Conf. Multimedia Ubiquitous Eng.*, 2008, pp. 150–154, doi: 10.1109/MUE.2008.65.

[69] C. V. L. Mendoza and J. H. Kleinschmidt, ''Mitigating on-off attacks in the Internet of Things using a distributed trust management scheme,'' *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 11, 2015, Art. no. 859731, doi: 10.1155/2015/859731.

[70] M. F. Mubarak, J.-L.-A. Manan, and S. Yahya, ''A critical review on RFID system towards security, trust, and privacy (STP),'' in *Proc. IEEE 7th Int. Colloq. Signal Process. Appl.*, Mar. 2011, pp. 39–44, doi: 10.1109/CSPA.2011.5759839.

[71] X. Wu and F. Li, ''A multi-domain trust management model for supporting RFID applications of IoT,'' *PLoS ONE*, vol. 12, no. 7, Jul. 2017, Art. no. e0181124, doi: 10.1371/journal.pone.0181124.

[72] M. F. Mubarak, J.-L.-A. Manan, and S. Yahya, ''Enabling trust and privacy for RFID system,'' in *Proc. 12th Int. Conf. Intell. Syst. Design Appl. (ISDA)*, Nov. 2012, pp. 799–804, doi: 10.1109/ISDA.2012.6416639.

[73] M. F. Mubarak, J.-L.-A. Manan, and S. Yahya, ''Mutual attestation using TPM for trusted RFID protocol,'' in *Proc. 2nd Int. Conf. Netw. Appl., Protocols Services*, Sep. 2010, pp. 153–158, doi: 10.1109/NETAPPS.2010.34.

[74] A. Alqarni, M. Alabdulhafith, and S. Sampalli, ''A proposed RFID authentication protocol based on two stages of authentication,'' *Proc. Comput. Sci.*, vol. 37, pp. 503–510, Jan. 2014, doi: 10.1016/j.procs.2014.08.075.

[75] S. D. Kaul and A. K. Awasthi, ''RFID authentication protocol to enhance patient medication safety,'' *J. Med. Syst.*, vol. 37, no. 6, p. 9979, Dec. 2013, doi: 10.1007/s10916-013-9979-7.

SOMYA ABDULKARIM ALHANDI received the B.E. degree (Hons.) in computer science (software engineering). She is currently working as a Research Assistant with the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia. Her research interests include the IoT, WSN, trust evaluation model, and trustworthy.

HAZALILA KAMALUDIN received the B.Sc. degree (Hons.) in computer from Universiti Teknologi Malaysia, in 2002, the M.Sc. degree in information technology from the University of Teknologi Mara, in 2005, and the Ph.D. degree in information technology from Universiti Tun Hussein Onn Malaysia (UTHM), in 2018. She is currently with the Faculty of Computer Science and Information Technology, UTHM. Her research interests include the IoT, RFID, WSN, and data trust.

NAYEF ABDULWAHAB MOHAMMED ALDUAIS received the B.Eng. degree (Hons.) in computer engineering from Hodeidah University, Yemen, and the master's and Ph.D. degrees in electrical engineering from Universiti Tun Hussein Onn Malaysia (UTHM), Malaysia, in 2015 and 2019, respectively. He is currently with the Faculty of Computer Science and Information Technology, UTHM. He has authored numerous papers in journals and conference proceedings. His research interests include WSN, the IoT, edge computing, and artificial intelligence (AI). He is a Reviewer for high-impact factor journals, such as IEEE Access, IEEE Sensor Letters, IEEE Internet of Things Journal, IEEE Transactions on Systems, Man, and Cybernetics: Systems. He has received numerous medals and scientific excellence certificates. He is an Editor of the *Journal of Soft Computing and Data Mining* (JSCDM), UTHM.