IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 20, 2019, accepted May 7, 2019, date of publication May 13, 2019, date of current version May 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2916340

RobustTrust - A Pro-Privacy Robust Distributed Trust Management Mechanism for Internet of Things

KAMRAN AHMAD AWAN[1], IKRAM UD DIN[1], (Senior Member, IEEE), AHMAD ALMOGREN[2], (Senior Member, IEEE), MOHSEN GUIZANI[3], (Fellow, IEEE), AYMAN ALTAMEEM[4], AND SULTAN ULLAH JADOON[1]

[1]Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[2]College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[3]Computer Science and Engineering Department, Qatar University, Doha 2713, Qatar
[4]Department of Natural and Engineering Sciences, College of Applied Studies and Community Services, King Saud University, Riyadh 11543, Saudi Arabia

Corresponding author: Ahmad Almogren (ahalmogren@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research at King Saud University under Grant RGP-1437-35.

ABSTRACT In the promising time of the Internet, connected things have the ability to communicate and share information. The Internet of Things (IoT) cannot be implemented unless the security-related concerns have been resolved. Sharing information among different devices can compromise the private information of users. Thus, a suitable mechanism is needed to exclude the risk of malicious and compromised nodes. As follows, trust has been proposed in the literature as a useful technology to maintain users' security. Prior studies have proposed diverse trust management mechanisms to achieve adequate trust. The approach of cross-domain trust management is neglected that requires enormous considerations to address the difficulties related to cross-domain communication. In this paper, a cross-domain robust distributed trust management (RobustTrust) system is proposed, which makes a device fit for assessing trust towards different devices locally. In this system, the trust is divided into three components of security that help IoT nodes to become robust against compromised and malicious devices/nodes. The novelty of the proposed mechanism can be summarized in these aspects: A highly scalable trust mechanism, multiple components of evaluation to enhance robustness against attacks, and use of recommendations along with the feedback to build knowledge. Furthermore, the proposed mechanism is event-driven that helps nodes to evaluate trust more effectively as well as enhance the system efficiency. The proposed work is compared with the available trust evaluation schemes by concentrating on various attributes, such as trustworthiness, usability, and accuracy among others. The RobustTrust is validated by the extensive simulations considering absolute trust value's performance, the accuracy of trust estimation, and several potential attacks.

INDEX TERMS Direct observation, IoT, robust trust, trust management, trust evaluation.

I. INTRODUCTION

Internet of Things (IoT) [1] is an evolving large-scale Internet comprising a large number of connected devices to communicate with one another [2], [3]. In IoT, things can be human beings, monitors, laptops, smart devices [4], and sensors [5]. The new IoT paradigm has also introduced further applications, for instance, smart cities [6], [7], smart grids [8], and most importantly e-health [9], [10]. All these applications are aimed to improve the quality of life [11]. However, achieving all these applications depends on strong security means [12] to protect these billions of IoT devices [13]. Due to the heterogeneous environment of IoT, security is considered as a major factor that includes trust, access control [14], secure middle-ware [15], authentication [16], etc. The technologies involved in the IoT enable information sharing [17] among nodes, which raise an issue that how a single node can trust other nodes and how much information does a node share to preserve the privacy. To address this problem, the research community has

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

proposed trust management mechanisms [18] that make the node capable of maintaining trust and mitigating the risk of communication and information sharing with malicious and compromised nodes.

The motivation behind providing trust management mechanism is to make IoT nodes robust against misbehaving and compromised nodes [19]. Misbehavior of the compromised nodes raises the risk of false recommendations. If a node communicates and shares information with a malicious node, it may lead to a privacy compromise [20]. Furthermore, misbehaving nodes can execute several attacks and can also send wrong recommendations during their compromised status [21]. Hence, trust mechanisms have been introduced to eliminate security limitations. Now, with trust, each node evaluates trust towards other nodes before starting its communication procedures. If the degree of trust meets the threshold value, then the node will communicate, otherwise it will ignore those nodes with lower degrees.

There are several proposed trust management mechanisms that can be categorized as distributed [22] and centralized [23]. There are numerous shortcomings of centralized trust management mechanisms and a significant one among all is that if the central authority gets compromised, then there is no substitute gadget to manage and/or control the degree of trust. The compromised central authority can affect the entire network [24] while the significant advantage of distributed trust management mechanism [25] is that each device manages trust on its own and one compromised node cannot affect the aggregate network. Each model has its own parameters for the trust evaluation. Some of the existing trust mechanisms are discussed in Section II. Trust is considered as a vital issue that requires a huge amount of consideration. The existing trust management literature addresses the issue of misbehaving nodes, while some of these mechanisms focus on IoT attacks [26].

To design a trust mechanism, we follow the framework of Sharma *et al*. [27]. The proposed framework is generic to trust management and consists of multiple phases that perform specific activities. These phases involve trust gathering, trust computation, trust dissemination, update, and maintenance. The trust gathering phase is further divided into three sub-categories in which the first step is to choose the parameters of a trust management mechanism along with the information gathering and type of information. The information gathering signifies data that is used to compute trust that can be qualitative or quantitative. The second phase consists of classifying the working of a trust management mechanism, which performs computation and utilizes a suitable approach that can be statistical [28], probability [29] or intelligent fuzzy [30] and machine learning [31] approach. Furthermore, after clinching the information gathering and trust computation phase, the succeeding phase is trust dissemination in which the suitable working scenario of trust management mechanism is required to finalize that it works as a central authority or distributed. In the last phase, it is required to identify that the trust estimation process works as event-driven or time-driven. Figure 1 illustrates the broader view of the trust management framework.

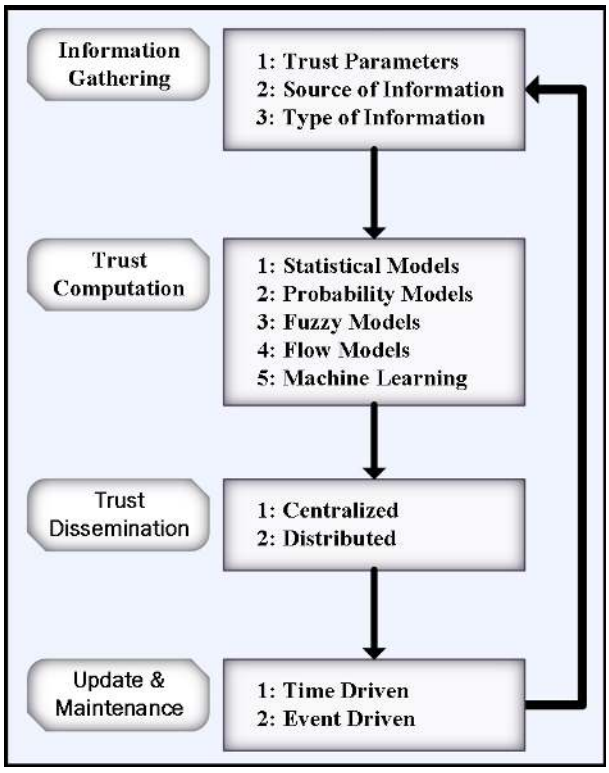

FIGURE 1. Generic trust management framework for IoT [27].

The proposed trust management mechanism divides the trust into three components where each component contains trust parameters to evaluate trust towards other nodes. These trust components provide nodes with the capability of robustness against attacks. In the proposed mechanism, a node gathers information from direct observations and recommendations, and scale the information quantitatively from 0.0 to 1.0 based on the pre-defined trust parameters. The trust dissemination is distributed which helps nodes to act independently and make them able to evaluate the trust locally. The major significance of distributed trust is that the nodes do not have to rely on any centralized authority. To improve the scalability and efficient utilization of limited storage, the node only stores the computation of experience component for the future. The experience evaluation can be used in the future with the help of trust propagation and aggregation. The trust development phase is responsible to form the overall trust of the components by using summation function [32]. Trust management will manage the overall trust evaluation of the interacting nodes.

The remaining article is organized as follows: Section II concisely illustrates the overview of existing trust management mechanisms. Section III contains detailed descriptions of the proposed trust mechanism along with the working, trust composition, and trust development of the RobustTrust. Section IV and V present the comparison and performance

evaluation of the proposed mechanism with the existing schemes, and Section VI concludes the paper.

II. LITERATURE REVIEW

Trust management plays an important role to provide reliable data merging [33]. It also helps to eliminate the risk of user privacy [34] and information security [35]. In this section, a literature survey has been conducted on the existing trust management mechanisms. Various proposed approaches are explained that evaluate trust and provide security to communicating gadgets in the IoT environment.

In 2012, a dynamic trust management protocol (DTP) was proposed for the IoT-based applications [36]. In the DTP, every node acts as an autonomous node to manage trust towards other nodes. Trust assessment in this model is event-driven and is based on multiple trust parameters, i.e., cooperativeness, community interest, and honesty. The evaluation of this mechanism shows that the protocol is resilient towards misbehaving nodes. In the IoT, nodes generate a bulk amount of data and trust management must provide the capability that the nodes can collect and analyze the trust in a trustworthy manner. The DPT lacks to analyze data and to uphold the confidentiality of users.

In 2013, a community of interest (CoI) based trust management for IoT was proposed to achieve scalability and adaptivity [37]. The model considers the CoI for the formation of nodes communities. The trust composition consists of multiple parameters, such as honesty, cooperativeness, and community interest. The presented study addresses the limited storage of nodes and proposes a storage management strategy. In the storage strategy, when a trustor computes trust towards a trustee, then the evaluation is stored in the empty space of the storage. When the storage space is full, then the trustor deletes trust of the earliest interacting node with below median. The storage management strategy also helps to improve the scalability and efficiency of the available limited nodes' storage. The quality of IoT service is an important aspects, therefore, the CoI based trust management mechanism may perform better by adding quality of IoT services.

Trustworthiness management mechanism (TMM-IoT) was proposed in [38] for the social IoT. The study focuses on the problem of how social IoT members process available information to build mechanisms for nodes on the basis of their behavior. The TMM-IoT are of two types, i.e., objective and subjective trustworthiness [39]. The trust elements used in the proposed mechanism are feedback systems, the entire amount of transactions, relationship factor, credibility, transaction factor, computation capability, and the notion of centrality. It is also mentioned that the subjective model has a delayed response. The objective model suffers when a node is trustworthy for the entire network but may contain the opinion from malicious or compromised nodes.

A trust management mechanism is proposed for the wireless sensor network, known as lightweight trust management based on Bayesian and entropy (LTMBE) [40]. The proposed approach utilizes Bayesian [41] and entropy [42] to perform trust computations. The LTMBE uses Bayesian to evaluate the trust of a node while the trust value estimation depends on the history of trust and decay factor. The mechanism further checks the trust value using the confidence level. The value of trust is deemed credible when the confidence level of that value is higher. The decay factor enhances the accuracy while evaluating trust and confidence level reduces the energy consumption. The intention of utilizing entropy theory is to specify weights to various values of trust.

In 2016, trust-based service management (TBM) for the IoT environment was proposed in [43]. The design of the proposed trust management model is adaptive and trust composition involves cooperativeness, community interest, and honesty. The trust assessment is achieved by recommendations and direct observations. In the proposed trust management model, the mechanism uses the past and new information with the help of propagation and aggregation that combines the information continuously. The trust formation is used to formulate the overall trust and trust management controls. The major concern of the TBM is the secure transmission of data and the maintenance of trust during communications.

Dirichlet-based trust management system (DB-TMS) was proposed in [44], which addresses the on-off attacks [45] and dishonest recommendations [46] in IoT. The parameters of trust used in this model are feedback system, service level threshold, service transacting weight, and computation capabilities weight. The trust composition of the proposed model is based on recommendations and direct observations. The DB-TMS uses the prediction factor and mitigates the dishonest recommendations to prevent on-off attacks while the proposed mechanism does not consider the security and reliability of collected data.

Another trust management scheme was proposed in [47], which helps mitigating on-off attacks using distributed trust management. For the computation of trust, the proposed model uses the information generated by direct observations. The initial value of the trust is zero, which shows that all nodes are set as unknown. The trust is built on the basis of several services provided by network nodes. The limitation of this scheme is that it only uses direct observations for the trust evaluation, while the use of recommendations is required to generate more effective and accurate trust.

In 2017, an efficient trust evaluation scheme (ETES) was proposed in [48], which focuses on the behavior detection of IoT nodes. The approach of evaluation in the ETES is quantitative. The factors that are used to evaluate trust consist of repetition rate, consistency of content packet, delay, and integrity. The proposed model uses the D-S theory [49] to infer and integrate the trust. The evaluation of ETES with the existing ones shows more adaptivity. Moreover, the evaluation results also show that the scheme is more robust against attacks.

Context-based trust management system (CB-TMS) for the IoT was proposed in [50]. The objective of this system is to use the trust value of a single node in different contexts. The

components of this model are i) objects that are used by their owner, ii) a service owner for the authentication of each entity, and iii) a trust management server for the evaluation of trust. The trust parameters involved in this model are feedback system, transaction weight, and computation capabilities weight. The significant of this model is the use of decision tree [51] to analyze the relationship among network components. The considerable aspect to increase the CB-TMS security and robustness is to use recommendations to evaluate the indirect trust. In addition, the generality of the system is uncertain.

A dependable trust management mechanism (GroupTrust) [52] is proposed that essentially focus to utilize the susceptible-infected-recovered (SIR) model [53]. The proposed research also stated that the estimation of trust individually depending on direct observations can become vulnerable. The GroupTrust seeks to provide a reliable trust mechanism during several potential attack [54] executions. The GroupTrust utilizes the feedback credibility based on pairwise similarity to maintain adequate resilience towards attacks. The significance property of the proposed model is the use of SIR model that specifies the threshold value of trust propagation that will enhance the credibility of the degree of trust. The experimental evaluation of GroupTrust shows the resilience towards diverse potential attacks and remains highly scalable.

An adaptive IoT trust measurement scheme was proposed in [55], which combines the communication history and stereotypical reputation. The proposed scheme works by evaluating a user's trust value towards nodes. In addition, the scheme combines the user's trust value with the personal trust from the interaction history. This scheme works in the following four phases: In the first step, the scheme captures the current situation's characteristics. The extraction of the situation's experience is produced in the second step. In the third step, the scheme uses history and performs computations to evaluate personal trust. Finally, the estimation scheme uses the evaluated personal trust and computes the final trust with a stereotypical reputation.

A trust management system based on communities of interest (TM-CoI) was proposed for IoT [56]. The TM-CoI integrates the transaction and social factors. The significance of this system is that the prediction has been made by using kalman filtering technique. A mechanism of using kalman filtering [57] might be effective to prevent several attacks and also to predict the behavior of nodes. The accuracy and efficiency of TM-CoI need to be evaluated in the context of identify trust by focusing on the scalability and effective identity management of nodes.

A trust management mechanism (TMM) was proposed in [58] for the reliable decision making among different things in the IoT environment. Trust evaluation in this model is done using direct observations and no recommendations are used by the trustor for building trust. The trust parameters used in this model are centrality, cooperativeness, and community interest. The proposed system also calculates the expected and overall trust. The TMM is effective for direct trust evaluation but the considerable attention is required to maintain the quality of service provided by one node to others efficiently.

Another trust management mechanism, i.e., SGSQoT [59] is proposed that utilizes the concept of community to maintain trust among nodes in IoT. The proposed mechanism considers self, social, green, and QoT trust. The study also stated that none of the existing trust management mechanism used these attributes together. The self-trust is calculated based on data processing, data privacy, and data transmission trust. The green trust [60] correlates to the environment and utilizes lifetime and response trust to estimate green trust. The direct trust computation consists of QoS and social trust that is further divided into sub-trust parameters. The indirect trust computations depend on recommendations and the trust value is calculated by obtaining recommendations from various neighboring nodes.

III. PROPOSED TRUST MANAGEMENT MECHANISM

Traditional methods for protecting IoT devices are cryptography [61] and access control [62]. However, in IoT, these methods alone cannot provide enough security due to complexity and heterogeneous communications. A compromised node can authenticate its bogus information using valid cryptography [63]. Access control is suitable for distributed environments [64], but every node that wants to be a part of the Internet, its identity must be embedded in the access control list.

Trust management is introduced as an alternative to all traditional methods that are able to resolve the above mentioned issues. Trust can be provided (with a mechanism) to IoT devices so that they can maintain trust relation locally. In this section, we elaborate the proposed RobustTrust system. In the RobustTrust, the goal is to provide devices with the capability in such fashion that they can distribute trust among other nodes and show resilience towards attacks. The trust management system is event-driven, which means that the trust value is updated only when a node interacts with other network nodes.

In the RobustTrust system, a node can distribute the evaluated experience of a particular node with other nodes. The RobustTrust is divided into three components which contains trust parameters for an efficient evaluation of trust. In level one component, the knowledge of a node towards other nodes is built by computing compatibility, integrity, and feedback. In level two component evaluation, a node builds the reputation of the interacting nodes on the basis of honesty, reliability, and cooperativeness. Later on, when the interaction is done, the node evaluates the experience based on competence, recommendations, and credibility parameters. The node evaluates all parameters based on the past information and scale the evaluation on the basis of performance of trustee from 0.1 to 1.0 to formulate the absolute trust value. The process of evaluation and scaling of information is explained in section III-C and III-D. For future interactions, nodes are capable of using the evaluation of experience to build

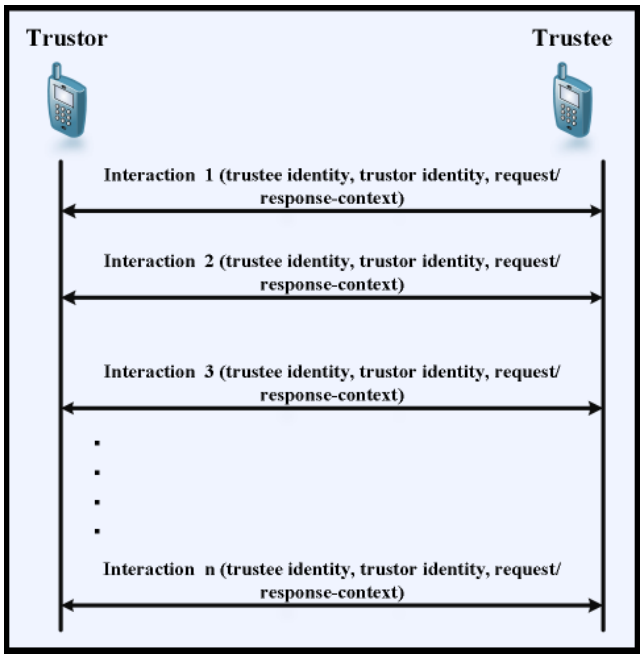

FIGURE 2. Trustor and trustee direct interaction model.

knowledge and also share their experience with other gadgets in the shape of recommendations. The experience components contain the recommendation parameter that helps gadgets to collect recommendations about a specific device. The collection of recommendations from neighboring nodes helps gadgets to increase the accuracy of trust evaluation. The trust propagation and aggregation components are included in the model that handle the past and new information for analyzing the trust calculation to meet the threshold value. By dividing the trust into these components, the proposed system is able to provide robustness to IoT nodes for keeping the resilience towards malicious nodes and potential attacks.

A. WORKING OF THE PROPOSED TRUST MANAGEMENT MECHANISM

A trust management model consists of multiple phases that perform dedicated activities. These phases are data collection, trust calculation, trust architecture, update, and maintenance. The objective of a trust management mechanism is to make nodes robust and provide the ability to nodes so that they are able to maintain trust towards other gadgets. To achieve scalability, a device can only keep evaluating the experience components data concerning the limited number of nodes. Trustors are able to build their trust using previous direct observations and recommendations. In the RobustTrust, nodes collects information from direct observations and scale them to compute trust. Figure 2 shows the direct interaction between trustor and trustee. The node is responsible to communicate along with the scaling of each parameter to evaluate the trust. The RobustTrust evaluation process is presented in Figure 3. In the proposed mechanism, we consider all aspects of trust management and address them with multi-level trust component evaluation. The trust composition phase consists of knowledge, reputation, and experience. To make the system robust against malicious nodes, an additional component of security is proposed, named *Experience*. By introducing the *Experience* component, nodes are able to calculate their experience and use it for knowledge building, and save the evaluation data for the future use. The trust propagation and aggregation are responsible to formulate an average value of trust by combining the past and current trust evaluations. It is also significant to form an overall trust from individual properties. To resolve this issue, the trust development components are introduced in which all the parameters are combined together by applying standard sigma function and formulate an absolute trust value that increases the decision making ability of nodes.

In IoT, millions of gadgets would be connected to the Internet, which require to keep trust among nodes. It is observed that the centralized trust management is not sufficient and may lead to delay. Thus, we consider this issue and propose a distributed trust management system. To maintain the efficiency and accuracy of nodes, the proposed mechanism is both direct observation and activity-based, where a node only updates its trust among other nodes on the basis of direct observations. The node uses recommendations only when it communicates with other devices for the first time. In RobustTrust, the experience component contains the recommendation parameter, thus, the mechanism can share and recommend the evaluation to other nodes.

B. TRUST COMPOSITION

The primary objective is to propose a cross-domain robust trust management mechanism. To achieve this, the trust has been divided into three major components, i.e., knowledge, reputation, and experience. Furthermore, each component contains several trust parameters for evaluation. All trust parameters are computed separately, as discussed in the following subsections.

1) KNOWLEDGE

A node builds its knowledge among other nodes on the basis of several parameters. These parameters are compatibility, integrity, and feedback. The compatibility trust property plays an important role for the trustor because it helps devices to predict whether they are able to work together or not. If the compatibility between two nodes is of a higher degree, then the chance of any conflict between these nodes is reduced. The most significant property of trust evaluation is integrity of a node which assists the trustor to analyze that the trustee is not destructive. When the trustor computes trust concerning the trustee, the trustor calculates the commitment of the trustee towards the work. This principle can come from numerous sources, such as morality. The feedback property of trust allows a node to perform an evaluation of services provided by any other node. This dimension of trust is strictly related to the pre-evaluated data. In the proposed mechanism, the feedback about a node is collected by the evaluation of experience component.

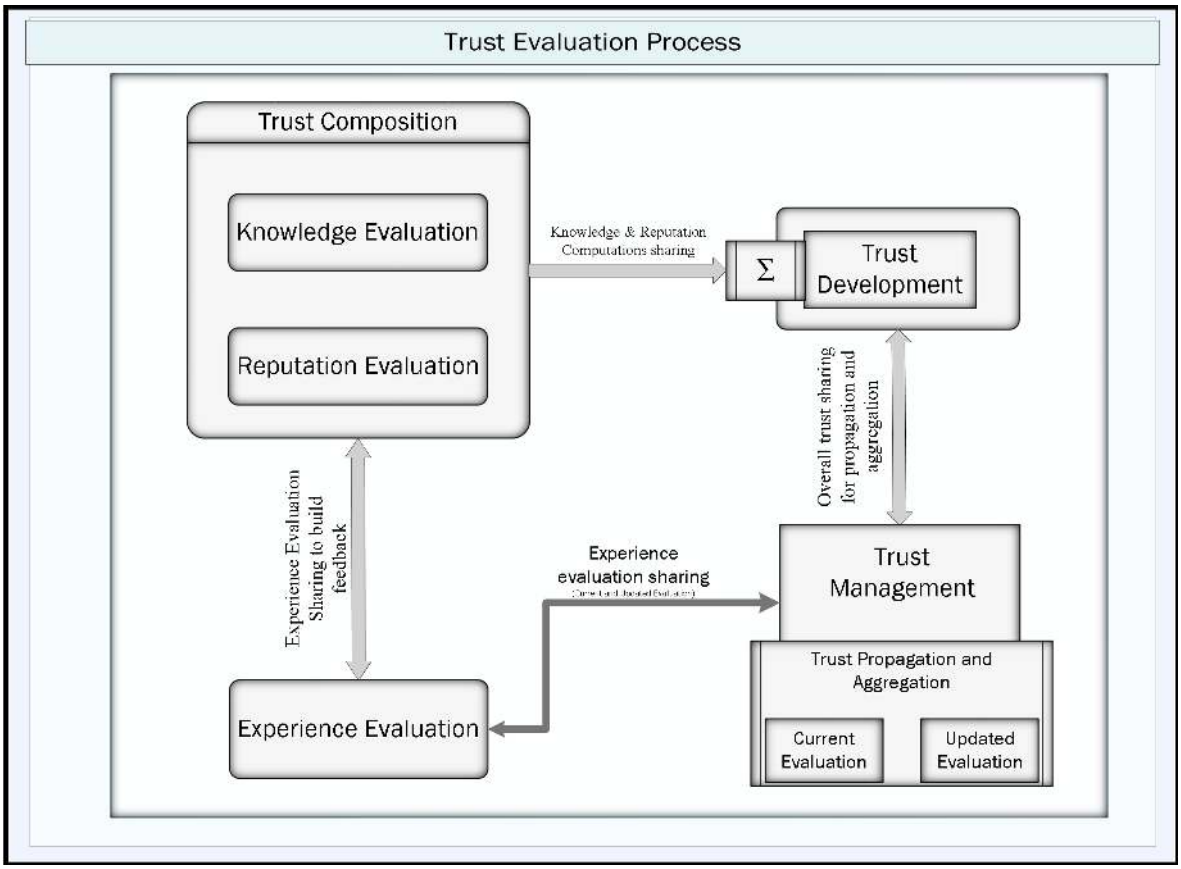

FIGURE 3. RobustTrust evaluation process.

2) REPUTATION

Reputation belongs to the belief in which a node evaluates the character of a particular node. In the proposed model, the reputation is evaluated using three parameters, e.g., honesty, reliability, and cooperativeness of a node. The honesty property of trust shows whether the node is honest or not. When the trustor interacts with the trustee, then honesty provides information regarding the dishonesty of a node. The honesty property is really important for any domain of trust management because a malicious gadget may disturb trust management and services of IoT applications. The node reliability represents quality of being trustworthiness of trustee towards the trustor. If the reliability between the trustor and a trustee is of a higher degree, then the performance between these nodes will be better for quite a long time. The most significant property of trust that helps to increase the quality of services provided by any node is cooperativeness. It enables the trustor to evaluate whether the trustee is socially cooperative or not. The main objective of this property is to predict that IoT nodes can be cooperative in pre-arranged protocol, but they might become un-cooperative while interacting outside the prescribed protocol.

3) EXPERIENCE

Experience belongs to an event or occurrence when the trustor interacts with a trustee to perform any specific task after the trust is established between them. When the task is completed, the trustor evaluates the experience of the trustee by using pre-defined trust parameters. In the proposed mechanism, the experience is evaluated when the interaction or event has been done. Here, experience is evaluated on the basis of competence, recommendation, and end-to-end packet delivery. The competence trust property is evaluated on the basis of the ability of a node to perform a task properly or effectively. Competence is evaluated on the performance of a node towards the task performed. If the trustor evaluates the competence of a trustee and the result of evaluation is of higher degree, then it represents that the task performed by the trustee is efficient and successful. The evaluation of indirect trust is a significant aspect because when a node does not have the required information to evaluate trust of a particular node, then that node requests neighboring nodes to share their experience about a specific node. The recommendation property of trust is used in RobustTrust to collect recommendations by requesting other nodes. Let us suppose the trustor does not have any past information about the trustee, which means that the trustor does not have direct observation towards the trustee, then the trustor requests other nodes to get recommendations about the trustee for building trust. Finally, the end-to-end packet delivery property provides the degree of communication cost and delays between two nodes at the time of interaction. If the delivery of packets is faster

and without any significant delay, then it will help nodes to perform a task in less time.

C. TRUST PROPAGATION AND AGGREGATION

The proposed trust management is a nonstop practice and updates trust towards gadgets whenever an event occurs. Trust propagation and aggregation continuously propagate and aggregate past and new information. The RobustTrust mechanism is based on qualitative data and the trust evaluation comes in real number, where the range of these numbers is from 0.0 to 1.0. In this range, 0.70 to 1.0 depicts the superior degree of trust or complete trust where 0.0 demonstrates the lowest degree of trust or zero trust. The trust value range can be of 0.5, in this case, the mid value shows the default degree of trust. The degree of trust ranging from 0.51 to 0.69 shows the medium trust or trust ignorance. During direct interactions, nodes collect information about the trustee and process the collected information to evaluate trust parameters. The quantitatively scaling of information is dependent on nodes, i.e., a node can assign any value based on the communication and services provided by the trustee. However, when the trustor interacts with the trustee and does not have any previous interaction or direction observation towards the trustee, then the trustor requests other nodes to provide their trust in the form of recommendations. The trustor uses the received recommendations and apply a standard sigma function [65] to evaluate the absolute value of trust concerning the trustee.

D. TRUST EVALUATION DEVELOPMENT

During the knowledge evaluation, trust parameters involve compatibility, integrity, and feedback, which are evaluated separately. The parameter of feedback is evaluated using the past experience component. Nodes evaluate and assign quantitative values to these parameters based on the response and capabilities of the trustee to perform a task efficiently. Later on, the trustor applies standard sigma function to evaluate the absolute knowledge trust evaluation. These absolute values of trust evaluation are further sent to the trust development component. The component of reputation builds trust by computing the trust parameters of honesty, reliability, and cooperativeness where a node will repeat the same process and send the absolute single value to the trust development phase. The trust development phase further processes both the evaluation of knowledge and reputation by applying the sigma function to evaluate the overall trust value of a node. The trust development component sends the overall trust value to the trust management component and then it performs trust propagation and aggregation to evaluate the final trust value. The complete process of trust evaluation is shown in Figure 3. A node evaluates its experience when the interaction between nodes is completed. To evaluate the experience, trust parameters consist of competence, recommendations, and end-to-end packet delivery. The node will scale these parameters based on the previous interaction and evaluate the absolute trust value. The assessment of experience is used to share with other node and evaluate the feedback parameter.

TABLE 1. Comparison of robusttrust with existing ones.

Trust Management Schemes	TR	US	AC	CM	AD	PR	GE
[36]	N	Y	N	N	Y	N	N
[37]	N	Y	Y	N	Y	N	N
[38]	Y	N	N	N	N	N	N
[40]	Y	N	N	N	N	Y	Y
[43]	Y	N	N	N	Y	N	Y
[44]	N	Y	N	N	Y	N	N
[47]	N	Y	Y	N	N	N	N
[48]	N	Y	N	N	N	Y	N
[50]	Y	N	Y	N	Y	Y	N
[52]	Y	Y	Y	N	N	Y	Y
[55]	N	N	Y	N	N	Y	N
[56]	N	N	Y	N	N	Y	N
[58]	N	Y	N	N	N	Y	Y
[59]	Y	N	N	Y	Y	Y	Y
RobustTrust	Y	Y	Y	Y	N	Y	Y

IV. EVALUATION CRITERIA OF ROBUSTTRUST

Trust management plays a vital role to ensure the IoT security [66]. To compare the proposed mechanism with the available trust management schemes, the comparison mechanism, proposed in [67], is adapted, wherein the study focuses on several evaluation criteria, as illustrated below. In Table 1, a comparison among the literature discussed in this paper is presented where *Y* shows the mechanism is capable of providing that specific service and *N* represents that the system lacks to provide particular services.

A. TRUSTWORTHINESS (TR)

To compare trustworthiness among trust mechanisms, our focus is on the robustness of the trust mechanism. The IoT system should be robust against potential attacks and provide enough resilience towards compromised and malicious gadgets. To evaluate the trustworthiness of a trust management scheme, our focus is on the robustness of the system.

B. USABILITY (US)

This criterion refers to the ease-of-use of trust models. A trust mechanism for IoT should be useful for users. To evaluate the usability of a trust management system, we evaluate it by focusing on the ease-of-use. The significance of usability is vital because the trust management mechanism must provide security by preserving the usability all at once.

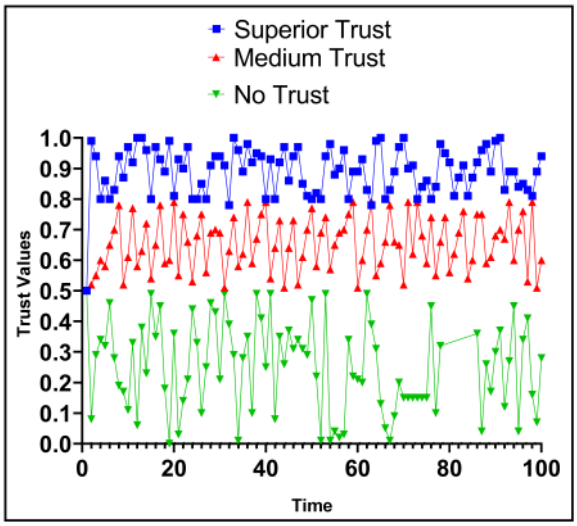

FIGURE 4. RobustTrust absolute degree of trust evolution.

C. ACCURACY (AC)

A trust evaluation mechanism should be accurate and efficient to evaluate trust in the heterogeneous environment of IoT. It is a vital aspect to achieve the accuracy of trust computation. To evaluate the accuracy, we focus on the ability to evaluate the trust accurately in a short interval of time. The accuracy of a trust computation helps nodes to take better decisions and also tries to maintain its robustness towards malicious nodes.

D. COMPREHENSION (CM)

The mechanism should support various factors to achieve the required degree of accurate evaluation. The significance of trust can be different for various users. It is possible that one user requires honesty and quality of service while others may need that a trust management mechanism must provide reliability and integrity. To evaluate the comprehension, our focus is the generality of trust parameters used in trust management.

E. ADAPTABILITY (AD)

The trust mechanism should be adaptive to changes in parallel to dynamic support. The mechanism is able to manage continuous changes happening in IoT. As the IoT environment is highly heterogeneous and changes occur rapidly, it is highly possible that a node have to communicate with several new nodes at the same time. In addition, the mobility is an important factor in the IoT environment, thus, trust management mechanism must be adaptive to the change. To evaluate the adaptability, our focus is to check the trust management mechanism acceptance towards changes occur around it.

F. PRIVACY (PR)

A trust evaluation mechanism should preserve the privacy of users. A trust mechanism must be able to restrict access of a node up to some extent and should ensure not to give access to the compromised node. In IoT, private data of a user is stored on nodes and every node can access data until a trust management procedure supports a mechanism to limit the access of nodes. In the evaluation of privacy, we focus on the robustness of a system to maintain the privacy and also restrict malicious nodes to access data.

G. GENERALITY (GE)

This criterion of evaluation refers to the generic trust mechanism, which means that the mechanism should be appropriate for a variety of systems, devices, and IoT applications. The evaluation of generality means that the mechanism is capable of deployment in different security situations and it provides the required efficiency and accuracy, and maintains the quality of IoT services.

V. PERFORMANCE EVALUATION

In this section, we describe the measurement outcomes of RobustTrust and comparison of the proposed work against existing trust management mechanisms. We evaluated our work against bad-mouthing, good-mouthing, and several scenarios of on-off attacks. The comparison of RobustTrust was done with SGSQoT [59] and GroupTrust [52].

The simulations have been carried out using NS-3 simulator wherein each node has several direct neighbors that provide different services over a period of time. The percentage of a malicious node is 40 to 60 during the performance evaluation of RobustTrust against potential attacks. The value of trust parameters is pre-defined and the threshold trust value is between 0.0 and 1.0. The trust value within 0.0 to 0.5 is deemed as no trust where 0.51 to 0.69 is regarded as medium trust, and 0.70 to 1.0 is considered as impeccable or superior trust. The default value of RobustTrust is 0.5 that allows newly join nodes to communicate with other nodes and build a reputation that helps nodes provide services.

A. ABSOLUTE TRUST EVOLUTION

In this section, we measure the functioning and storage management of RobustTrust. Furthermore, the scalability is also a significant consideration during simulations under different scenarios. The evaluation parameters of computations evaluation include 300 nodes, time(m), which is 100, the number of malicious nodes, which is also 100. The threshold value of trust is 0.0 to 1.0 and the default or ground trust value is 0.5. Figure 4 shows that the proposed mechanism successfully performs trust computations and estimates the absolute degree of trust. Moreover, there are numerous disseminated malicious nodes that are capable of communication in origin because of the default degree of trust and the proposed mechanism successfully distinguishes these nodes and assigns them no trust. The only concern that was observed during simulations is the nodes with inadequate storage face difficulties to store and manage the trust value.

B. TRUST EVOLUTION OF HONEST AND DISHONEST NODES

In this section, we illustrate the variation of estimated and actual degrees of trust of dishonest and honest nodes. The simulations were run for 100 minutes. Figure 5 and 6 show

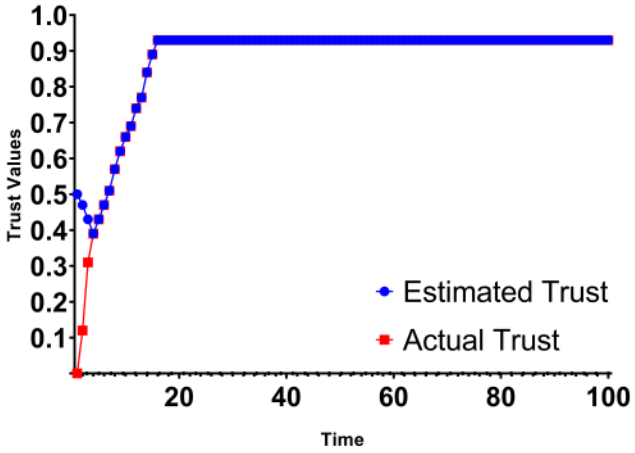

FIGURE 5. Trust degree of honest node.

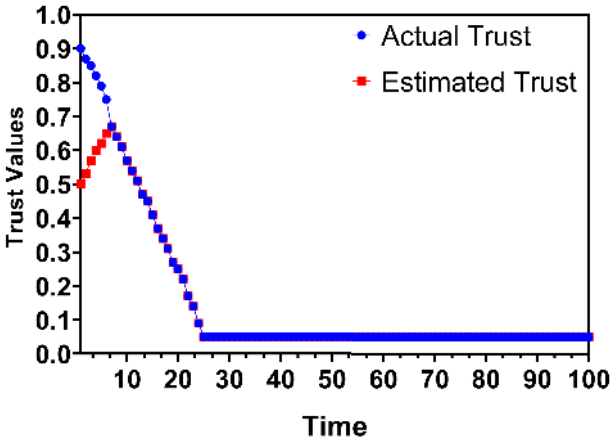

FIGURE 6. Trust degree of dishonest node.

that RobustTrust is able to estimate the degree of trust of the honest node within 3 minutes, while 8 minutes during trust estimation of the dishonest node. The actual and estimated trust values essentially depend on variances. The reduction in variance increases the difference of estimated and actual degrees of trust.

VI. GOOD-MOUTHING AND BAD-MOUTHING ATTACKS

In this section, we verify the effectiveness of RobustTrust toward good-mouthing and bad-mouthing attacks. The trust value is fixed, i.e., 0.0 as minimum and 1.0 as maximum. The default trust value is 0.5, time(m) is 20, and the number of transactions is set to 200.

We implement three trust management models to study the effectiveness of the proposed model against good-mouthing attacks. The decline in the degree of trust is noticed when the bad recommendation increases with time. Figure 7 shows the decline, which proves the performance of the proposed mechanism. The RobustTrust successfully identifies the good-mouthing and maintains the resilience towards attacks.

To validate the effectiveness of RobustTrust, we also implement three models with the same trust values.

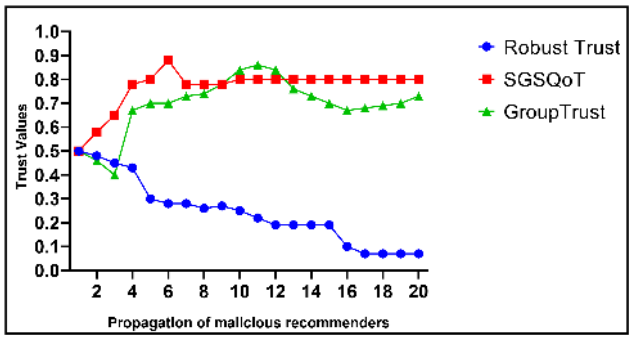

FIGURE 7. Trust values with good-mouthing attacks.

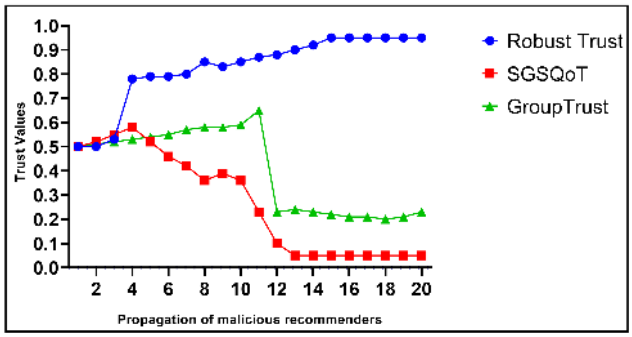

FIGURE 8. Trust values with bad-mouthing attacks.

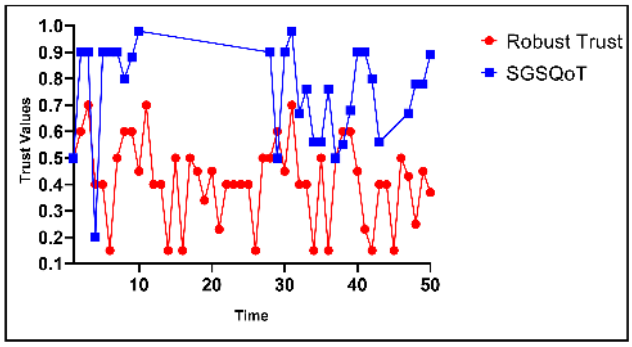

FIGURE 9. RobustTrust performance in first scenario of on-off attacks.

Figure 8 illustrates the performance of the proposed mechanism against good-mouthing attacks and an increase in the degree of trust signifies the robustness of the system against bad-mouthing attacks. The comparison of RobustTrust with other mechanisms clearly shows the performance achievement.

VII. ON-OFF ATTACK DETECTION

The on-off attack is one of the most significant challenges in IoT. In the majority of existing trust management mechanisms, the degree of trust decreases when the behaviors of anodes become malicious. To prove the robustness of the proposed mode, we implement two different scenarios and compare the performance with other mechanisms.

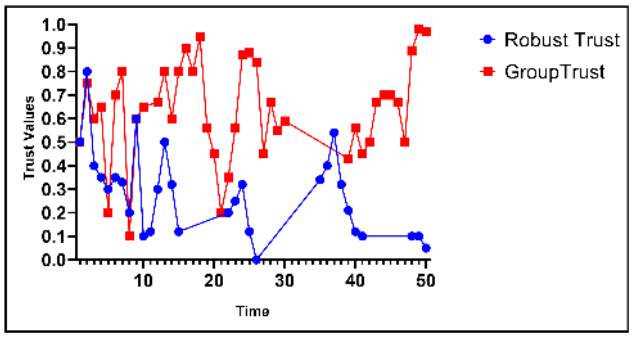

FIGURE 10. RobustTrust performance in second scenario of on-off attacks.

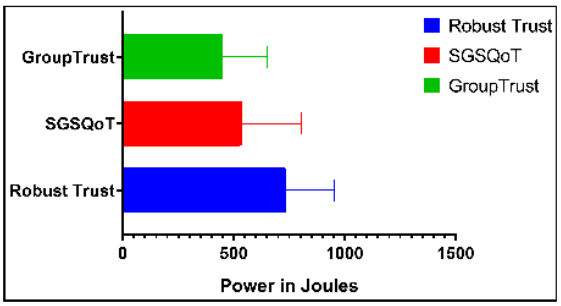

FIGURE 11. RobustTrust energy comparison.

In the first scenario of on-off attack, It was observed that the trust value of malicious node went down from 0.7 to 0.14 in just 6 minutes. Also, in the case of SGSQoT [59], malicious nodes regained their trust again after a specific period. Figure 9 demonstrates experimental results that the degree of trust of malicious nodes went downward and remained unsuccessful to reacquire the superior trust.

In the second scenario of on-off, the previous experiments are repeated and the performance of RobustTrust is compared with that of the GroupTrust [52]. In this scenario, the ambiguous and unsuccessful transactions are chosen randomly. Figure 10 depicts the experimental results where the proposed mechanism successfully detects the on-off attacks and the degree of trust of malicious nodes goes down from 0.8 to 0.09 in 10 minutes and 0.0 after 26 minutes. Furthermore, in the case of GroupTrust, the trust value of malicious nodes goes down from 0.65 to 1.0, but malicious nodes regain their trust to 0.92 and 0.95 after 18 and 19 minutes, respectively.

VIII. ENERGY CONSUMPTION COMPARISON

In IoT, there are numerous nodes that have low energy capacity where the effective utilization of energy is a significant challenge [68]. To evaluate the energy consumption of RobustTrust, it is observed in joules. The experimental setup for this evaluation is time(T) = 100m where the default trust value of nodes is 0.5 and the occurrence of an event is randomly defined. Figure 11 presents the energy consumption of the proposed mechanism in comparison with that of the SGSQoT and GroupTrust. The energy consumption of the RobustTrust is higher than others as it produces added computations to evaluate the absolute degree of trust. The RobustTrust needs to evaluate knowledge and reputation when an event occurs. It also evaluates experience at the end of a particular event. The evaluation of knowledge, reputation, and experience provides adequate robustness against attacks, however, it also consumes more energy as compared to SGSQoT and GroupTrust.

IX. CONCLUSION

In this article, a trust management mechanism is proposed for IoT, which is known as robust cross-domain trust management (RobustTrust). The proposed mechanism is able to make nodes capable to act independently and evaluate trust towards other nodes locally. The mechanism contains different components to compose trust that will provide nodes with robustness against various kinds of attacks. To improve the scalability, a node only keeps the result of the experience component. Trust propagation and aggregation are used to allow the mechanism to combine the past information with the new data. The model works on direct observations and requests for recommendations only when a node interacts with others for the first time. The trust model is event-driven, which means that a node only evaluates trust when an event occurs between two nodes. In this paper, we considered to make a node robust against attacks while maintaining trust across the domain. Experimental results show the performance of RobustTrust against several attacks where the system successfully recognizes attacks and maintains robustness against potential attacks. As a future work, our plan is to extend RobustTrust and propose a lightweight cross-domain trust management mechanism where the security and node vulnerability is a significant challenge.

REFERENCES

[1] M. Curado *et al.*, "Internet of Things," in *Cyber Resilience of Systems and Networks*. Cham, Switzerland: Springer, 2019, pp. 381–401.
[2] M. Dabbagh and A. Rayes, "Internet of Things security and privacy," in *Internet of Things From Hype to Reality: The Road to Digitization*. Cham, Switzerland: Springer, 2019, pp. 211–238.
[3] I. U. Din, M. Guizani, J. J. P. C. Rodrigues, S. Hassan, and V. V. Korotaev, "Machine learning in the Internet of Things: Designed techniques for smart cities," *Future Gener. Comput. Syst.*, to be published. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X19304030
[4] W. Yu *et al.*, "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018.
[5] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 78, pp. 544–546, Jan. 2018.
[6] P. Chamoso, F. De la Prieta, and J. B. Pérez, and J. M. C. Rodríguez, "Conflict resolution with agents in smart cities," in *Smart Cities and Smart Spaces: Concepts, Methodologies, Tools, and Applications*. Hershey, PA, USA: IGI Global, 2019, pp. 695–713.
[7] I. U. Din *et al.*, "The Internet of Things: A review of enabled technologies and future challenges," *IEEE Access*, vol. 7, pp. 7606–7640, 2019.
[8] M. Masera, E. F. Bompard, F. Profumo, and N. Hadjsaid, "Smart (electricity) grids for smart cities: Assessing roles and societal impacts," *Proc. IEEE*, vol. 106, no. 4, pp. 613–625, Apr. 2018.
[9] L. Vidyashree, M. A. Alworafi, and S. A. El-Booz, "Survey of security mechanisms in Internet of Things," in *Recent Findings in Intelligent Computing Techniques*. Singapore: Springer, 2019, pp. 353–361.
[10] S. U. Khan, N. Islam, Z. Jan, I. U. Din, A. Khan, and Y. Faheem, "An e-health care services framework for the detection and classification of breast cancer in breast cytology images as an IoMT application," *Future Gener. Comput. Syst.*, vol. 98, pp. 286–296, Sep. 2019.

[11] I. Lokshina and C. Lanting, "A qualitative evaluation of IoT-driven ehealth: Knowledge management, business models and opportunities, deployment and evolution," in *Data-Centric Business and Applications*. Springer, 2019, pp. 23–52.

[12] D. Degraen, "Exploring interaction design for the social Internet of Things," in *Social Internet of Things*. Cham, Switzerland: Springer, 2019, pp. 85–106.

[13] J. Cynthia, H. P. Sultana, M. N. Saroja, and J. Senthil, "Security protocols for IoT," in *Ubiquitous Computing and Computing Security of IoT*. Cham, Switzerland: Springer, 2019, pp. 1–28.

[14] S. Li, L. D. Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018.

[15] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291–319, 2018.

[16] P. Singhal, P. Sharma, and B. Hazela, "End-to-end message authentication using CoAP over IoT," in *Proc. Int. Conf. Innov. Comput. Commun.* New Delhi, India: Springer, 2019, pp. 279–288.

[17] P. J. Werbos, "The new AI: Basic concepts, and urgent risks and opportunities in the Internet of Things," in *Artificial Intelligence in the Age of Neural Networks and Brain Computing*. Amsterdam, The Netherlands: Elsevier, 2019, pp. 161–190.

[18] 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, 2018.

[19] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digit. Commun. Netw.*, vol. 4, no. 2, pp. 118–137, 2018.

[20] K. A. Awan, I. U. Din, M. Zareei, M. Talha, M. Guizani, and S. U. Jadoon, "Holitrust-a holistic cross-domain trust management mechanism for service-centric Internet of Things," *IEEE Access*, vol. 7, pp. 52191–52201, 2019.

[21] T. Ludwig, P. Tolmie, and V. Pipek, "From the Internet of Things to an internet of practices," in *Social Internet of Things*. Cham, Switzerland: Springer, 2019, pp. 33–47.

[22] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017.

[23] N. Djedjig, D. Tandjaoui, I. Romdhani, and F. Medjek, "Trust management in Internet of Things," in *Security and Privacy in Smart Sensor Networks*. Hershey, PA, USA: IGI Global, 2018, pp. 122–146.

[24] V. Adat and B. B. Gupta, "Security in Internet of Things: Issues, challenges, taxonomy, and architecture," *Telecommun. Syst.*, vol. 67, no. 3, pp. 423–441, 2018.

[25] C. Verikoukis, R. Minerva, M. Guizani, S. K. Datta, Y.-K. Chen, and H. A. Muller, "Internet of Things: Part 3," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 108–109, Mar. 2017.

[26] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[27] A. Sharma, E. S. Pilli, A. P. Mazumdar, and M. C. Govil, "A framework to manage trust in Internet of Things," in *Proc. Int. Conf. Emerg. Trends Commun. Technol. (ETCT)*, Nov. 2016, pp. 1–5.

[28] C. Chatfield, *Statistics for Technology: A Course in Applied Statistics*. Evanston, IL, USA: Routledge, 2018.

[29] D. R. Cox, *Applied Statistics—Principles and Examples*. Evanston, IL, USA: Routledge, 2018.

[30] H. R. Singh, S. K. Biswas, and M. Bordoloi, "Recent neuro-fuzzy approaches for feature selection and classification," in *Exploring Critical Approaches of Evolutionary Computation*. Hershey, PA, USA: IGI Global, 2019, pp. 1–19.

[31] M. Viquar, S. Basak, A. Dasgupta, S. Agrawal, and S. Saha, "Machine learning in astronomy: A case study in quasar-star classification," in *Emerging Technologies in Data Mining and Information Security*. Singapore: Springer, 2019, pp. 827–836.

[32] A. R. Booker, M. B. Milinovich, and N. Ng, "Subconvexity for modular form L-functions in the t aspect," *Adv. Math.*, vol. 341, pp. 299–335, Jan. 2019.

[33] Q. Zhang, L. T. Yang, Z. Chen, P. Li, and F. Bu, "An adaptive droupout deep computation model for industrial IoT big data learning with crowdsourcing to cloud computing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2330–2337, Apr. 2019.

[34] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2526–2536, Aug. 2018.

[35] C. H. Au and W. S. L. Fung, "Integrating knowledge management into information security: From audit to practice," *Int. J. Knowl. Manage.*, vol. 15, no. 1, pp. 37–52, 2019.

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

[37] 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. Auton. Decentralized Syst. (ISADS)*, Mar. 2013, pp. 1–7.

[38] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social Internet of Things," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, pp. 1253–1266, May 2014.

[39] W. Baohua and S. Zhang, "A subjective and objective integration approach of determining weights for trustworthy measurement," *IEEE Access*, vol. 6, pp. 25829–25835, 2018.

[40] S. Che, R. Feng, X. Liang, and X. Wang, "A lightweight trust management based on bayesian and entropy for wireless sensor networks," *Secur. Commun. Netw.*, vol. 8, no. 2, pp. 168–175, 2015.

[41] A. B. Abdessalem, N. Dervilis, D. Wagg, and K. Worden, "An efficient likelihood-free Bayesian computation for model selection and parameter estimation applied to structural dynamics," in *Structural Health Monitoring, Photogrammetry & DIC*, vol. 6. Springer, 2019, pp. 141–151.

[42] J. Xu and F. Kong, "Adaptive scaled unscented transformation for highly efficient structural reliability analysis by maximum entropy method," *Struct. Saf.*, vol. 76, pp. 123–134, Jan. 2019.

[43] 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./Dec. 2016.

[44] O. B. Abderrahim, M. H. Elhedhili, and L. Saidane, "DTMS-IoT: A Dirichlet-based trust management system mitigating On-Off attacks and dishonest recommendations for the Internet of Things," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov./Dec. 2016, pp. 1–8.

[45] A. Jain and S. Jain, "A survey on miscellaneous attacks and countermeasures for RPL routing protocol in IoT," in *Emerging Technologies in Data Mining and Information Security*. Singapore: Springer, 2019, pp. 611–620.

[46] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Future Gener. Comput. Syst.*, vol. 92, pp. 178–188, Mar. 2019.

[47] 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.

[48] 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, 2017.

[49] J. Wen, Y. Tian, S. Yehang, T. Yongchuan, and H. Weiwei, "Improved evidential fuzzy c-means method," *J. Syst. Eng. Electron.*, vol. 29, no. 1, pp. 187–195, 2018.

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

[51] B. Rawal and R. Agarwal, "Improving accuracy of classification based on c4.5 decision tree algorithm using big data analytics," in *Computational Intelligence in Data Mining*. Singapore: Springer, 2019, pp. 203–211.

[52] X. Fan, L. Liu, M. Li, and Z. Su, "Grouptrust: Dependable trust management," *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 4, pp. 1076–1090, Apr. 2017.

[53] M. Alam, K. Kuga, and J. Tanimoto, "Three-strategy and four-strategy model of vaccination game introducing an intermediate protecting measure," *Appl. Math. Comput.*, vol. 346, pp. 408–422, Apr. 2019.

[54] M. Ghasemi, M. Saadaat, and O. Ghollasi, "Threats of social engineering attacks against security of Internet of Things (IoT)," in *Fundamental Research in Electrical Engineering*. Singapore: Springer, 2019, pp. 957–968.

[55] H. Son, N. Kang, B. Gwak, and D. Lee, "An adaptive IoT trust estimation scheme combining interaction history and stereotypical reputation," in *Proc. 14th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2017, pp. 349–352.

[56] O. B. Abderrahim, M. H. Elhdhili, and L. Saidane, "TMCoI-SIOT: A trust management system based on communities of interest for the social Internet of Things," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 747–752.
[57] J. Yu and L. Chen, "From static to dynamic tag population estimation: An extended kalman filter perspective," in *Tag Counting and Monitoring in Large-Scale RFID Systems*. Springer, 2019, pp. 43–75.
[58] A. M. Kowshalya and M. L. Valarmathi, "Trust management for reliable decision making among social objects in the social Internet of Things," *IET Netw.*, vol. 6, no. 4, pp. 75–80, 2017.
[59] R. Das, M. Singh, and K. Majumder, "SGSQoT: A community-based trust management scheme in Internet of Things," in *Proc. Int. Ethical Hacking Conf.* Springer, 2019, pp. 209–222.
[60] X. Zhai, X. Guan, C. Zhu, L. Shu, and J. Yuan, "Optimization algorithms for multiaccess green communications in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1739–1748, Jun. 2018.
[61] A. Bhattacharjya, X. Zhong, J. Wang, and X. Li, "Security challenges and concerns of Internet of Things (IoT)," in *Cyber-Physical Systems: Architecture, Security and Application*. Cham, Switzerland: Springer, 2019, pp. 153–185.
[62] W. He, M. Golla, R. Padhi, J. Ofek, and M. Dürmuth, E. Fernandes, and B. Ur, "Rethinking access control and authentication for the home Internet of Things (IoT)," in *Proc. USENIX Secur. Symp. USENIX Secur.*, Baltimore, MD, USA, 2018, pp. 255–272.
[63] G. Lize, W. Jingpei, and S. Bin, "Trust management mechanism for Internet of Things," *China Commun.*, vol. 11, no. 2, pp. 148–156, 2014.
[64] A. R. Phanindra, V. B. Narasimha, and C. V. PhaniKrishna, "A review on application security management using web application security standards," in *Software Engineering*. Singapore: Springer, 2019, pp. 477–486.
[65] M. Marin and A. Öchsner, "Harmonic functions," in *Essential Partial Differential Equations*. Cham, Switzerland: Springer, 2019, pp. 289–308.
[66] M. Muthusamy and K. Periasamy, "A comprehensive study on Internet of Things security: Challenges and recommendations," in *Advancing Consumer-Centric Fog Computing Architectures*. Hershey, PA, USA: IGI Global, 2019, pp. 72–86.
[67] P. Wang and P. Zhang, "A review on trust evaluation for Internet of Things," in *Proc. 9th EAI Int. Conf. Mobile Multimedia Commun. (ICST)* (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2016, pp. 34–39.
[68] J. Bardzell, S. Bardzell, and S.-Y. C. Liu, "Beautifying IoT: The Internet of Things as a cultural agenda," in *Social Internet of Things*. Cham, Switzerland: Springer, 2019, pp. 3–21.

KAMRAN AHMAD AWAN received the bachelor's degree from The University of Haripur, Pakistan, in 2015, where he is currently pursuing the M.S. degree in computer science with the Department of Information Technology. His research interests include trust management in the Internet of Things and information security.

IKRAM UD DIN (S'15–SM'18) received the M.Sc. degree in computer science and the M.S. degree in computer networking from the Department of Computer Science, University of Peshawar, Pakistan, and the Ph.D. degree in computer science from the School of Computing, Universiti Utara Malaysia (UUM). He also served as the IEEE UUM Student Branch Professional Chair. He has 10 years of teaching and research experience in different universities/organizations. His current research interests include resource management and traffic control in wired and wireless networks, vehicular communications, mobility and cache management in information-centric networking, and the Internet of Things.

AHMAD ALMOGREN received the Ph.D. degree in computer science from Southern Methodist University, Dallas, TX, USA, in 2002. He was an Assistant Professor of computer science and a member of the Scientific Council, Riyadh College of Technology. He also served as the Dean for the College of Computer and Information Sciences and the head for the Council of Academic, Al Yamamah University. He is currently a Professor and the Vice Dean of the development and quality with the College of Computer and Information Sciences, King Saud University. His research interests include mobile and pervasive computing, cyber security, and computer networks. He has served as a Guest Editor at several computer journals.

MOHSEN GUIZANI (S'85–M'89–SM'99–F'09) received the B.S. (Hons.) and M.S. degrees in electrical engineering and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a Professor with the CSE Department, Qatar University, Qatar. Previously, he has served as the Associate Vice President of Graduate Studies with Qatar University, University of Idaho, Western Michigan University, and University of West Florida. He has also served in academic positions with the University of Missouri-Kansas City, University of Colorado-Boulder, and Syracuse University. He is the author of nine books and over 500 publications in refereed journals and conferences. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He is a Senior Member of the ACM. He has also served as a member, Chair, and General Chair for a number of international conferences. He has received three teaching awards and four research awards throughout his career. He has received the 2017 IEEE Communications Society Recognition Award for his contribution to outstanding research in wireless communications. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He has served as the IEEE Computer Society Distinguished Speaker, from 2003 to 2005. He has guest edited a number of special issues in the IEEE journals and magazines. He is currently the Editor-in-Chief of the *IEEE Network Magazine*. He serves on the Editorial Board of several international technical journals, and the Founder and Editor-in-Chief of the *Wireless Communications and Mobile Computing Journal* (Wiley).

AYMAN ALTAMEEM received the Ph.D. degree in information technology from the University of Bradford, U.K., and the M.Sc. degree in information systems from London South Bank University, U.K. He is currently the Dean of the College of Applied Studies and Community Services, King Saud University, Riyadh. His research interests include e-commerce, the Internet of Things, information security, and artificial intelligence.

SULTAN ULLAH JADOON received the Ph.D. degree in computer science from the School of Computer and Communication Engineering, University of Science and Technology Beijing. He is currently an Assistant Professor with the Department of Information Technology, The University of Haripur, Pakistan. He has 13 years of teaching and research experience in different national and international universities/organizations. His current research interests include networks and information security, cloud computing, and management information systems.