IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 30, 2019, accepted April 16, 2019, date of publication April 22, 2019, date of current version April 30, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2912469

HoliTrust-A Holistic Cross-Domain Trust Management Mechanism for Service-Centric Internet of Things

KAMRAN AHMAD AWAN[1], IKRAM UD DIN[1], (Senior Member, IEEE), MAHDI ZAREEI[2], (Member, IEEE), MUHAMMAD TALHA[3], (Member, IEEE), MOHSEN GUIZANI[4], (Fellow, IEEE), AND SULTAN ULLAH JADOON[1]

[1]Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[2]Tecnologico de Monterrey, Escuela de Ingenieria y Ciencias, Monterrey 64849, Mexico
[3]Deanship of Scientific Research, King Saud University, Riyadh 11543, Saudi Arabia
[4]Department of Computer Science and Engineering, Qatar University, Doha 2713, Qatar

Corresponding author: Ikram Ud Din (ikramuddin205@yahoo.com)

This work was supported in part by the SEP-CONACyT Research Project under Grant 255387, in part by the School of Engineering and Sciences and the Telecommunications Research Group, Tecnologico de Monterrey, and in part by the Deanship of Scientific Research, King Saud University, Riyadh, Saudi Arabia.

ABSTRACT Internet of Things (IoT) is proposed and used in diverse application domains. In IoT, nodes commonly have a low capacity to maintain security on their own expenses, which increases the vulnerability for several attacks. Many approaches have been proposed that are based on privacy and trust management to reduce these vulnerabilities. Existing approaches neglect the aspects of cross-domain node communications and the significance of cross-domain trust management. In this paper, we propose a Holistic Cross-domain trust management model (HoliTrust) that is based on multilevel central authorities. To provide multilevel security, the HoliTrust divides domains into communities on the basis of similarities and interests. Every community has its dedicated server to calculate and manage the degree of trust. In addition, these domains also have their dedicated servers to manage their specific domains, to communicate with the trust server, and to sustain trust among other domain servers. The trust sever is introduced in the HoliTrust that controls the domains, calculates the domain trust, manages the trust values, and distributes standard trust certificates to domains based on a degree of trust. Trust computation is performed on the basis of direct and indirect trust parameters. Furthermore, if a trustor communicates through the community, then the community server includes community trust of the trustee during the trust evaluation. If the communication of the trustor is across the domain, then the community server includes the domain trust along with the community trust of the trustee comprising direct and indirect observations. The overall trust evaluation of communities and domains is time-driven and the responsible authority computes trust after a specific interval of time. We have also compared the HoliTrust with the existing trust mechanisms by focusing on several holistic trust objectives, such as trust relation and decision, data perception trust, and privacy preservation.

INDEX TERMS Trust management, holistic trust, cross-domain, IoT, security.

I. INTRODUCTION

The Internet is rapidly evolving and connected devices with the Internet are also increasing significantly. The current architecture of the Internet is not capable of handling all these communications among billions of devices. Also, the current architecture does not have the capability to provide enough security to these enormous amounts of nodes.

The Internet of Things (IoT) [1] is introduced in which every physical object/node is connected to the Internet and is capable of communicating with other nodes. An IoT node can be a sensor, a mobile set, or other smart device [2]. However, the IoT brings various security challenges that are required to be addressed for its implementation. These security challenges include (i) a secure mechanism for

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

authentication [3], [4] of a node when it joins the IoT, (ii) an access control mechanism [5] to control the access of nodes for confidential information, (iii) a secure and robust privacy mechanism that preserve privacy [6]–[8] to the IoT nodes. The most significant challenge for the IoT security is the trust management mechanism [9]–[15] that maintains and performs computations. Furthermore, the trust computation model must have the capability to perform computations efficiently and provide scalability [12]. Nevertheless, the policy enforcement [16], [17] and secure middleware architecture [18] are also significant security challenges.

In this paper, we propose the HoliTrust that addresses the problems associated with the cross-domain trust management. In the HoliTrust, every domain is further divided into communities on the basis of similarities and interests. Every community has its own dedicated community server (CS) to perform trust calculations among nodes, calculates overall community trust, and communicates with the CS and the domain server. To add more, every domain has a dedicated domain server (DS) that coordinates communities within the domain and with other domain servers and trust servers. The trust server is located above all domains and is responsible for the evaluation of domain trust to generate standard trust certificates based on the degree of the trust. The trust server also stores the overall trust of domains for trust propagation and aggregation.

There are several existing trust management models which are proposed based on distributed and centralized approaches. In distributed trust management, every trustor is responsible for the calculation of trust. The distributed mechanism faces a number of failures and low scalability [19]. In centralized trust management, a central authority is responsible to manage the trust of all nodes. The significant challenge of centralized approaches is a failure of central authority. If the central authority fails, then there is no backup authority mechanism available to manage the trust. The HoliTrust model addresses all the above mentioned issues. The HoliTrust model contains multi-layer centralized authorities which consist of multi-layer authorities such as CS, DS and, trust server. If the CS fails, then the domain server is responsible for the upper-layer security to manage the community and the CS. Also, a node of one domain cannot communicate across the domain without the evaluation of community and domain trust that will help to recognize and identify the compromised, malicious, or failed central authority. However, the HoliTrust provides a multi-level security to provide IoT nodes with a secure and robust trust management mechanism to keep resilience towards possible attacks.

The remaining paper is classified as follows. Section II briefly elaborates the existing trust management mechanisms. Section III illustrates the proposed HoliTrust model. Section IV explains the working of nodes, community server, domain server, and trust server along with the trust computation process. Section V contains the comparison of the HoliTrust with the existing trust management approaches. And Section VI concludes the paper.

II. LITERATURE REVIEW

Several trust management mechanisms are developed to maintain the IoT trust. The distributed and centralized are the two main classifications of trust management mechanisms. In the distributed trust management, each node is responsible for evaluating and maintaining the trust among nodes. In the centralized trust management system, the IoT nodes are dependent on a primary authority to manage the trust among nodes. Several approaches have been proposed that address the challenges associated with the trust management. In this section, we conduct a comprehensive literature survey of the existing trust mechanisms, where Section V shows the comparison among them on the basis of various objectives.

In 2018, a trust management model is proposed to provide the essential security for the cloud-based IoT framework [20]. The proposed mechanism is a brain-inspired trust management model (BI-TMM) and converges the implementation of data reliability to IoT nodes. The BI-TMM employs the adaptive neuro-fuzzy inference system [21] with the weighted-additive approach [22] to evaluate the behavioral and data trust of a distinct node. The trust parameters are used to determine behavioral trust of nodes, which include relative frequency of interaction, intimacy, and honesty. The data trust is evaluated based on direct and indirect trust by utilizing past information obtained by interacting with nodes. The past information is the average value of nodes' previous trust. The strength of the proposed model can be summed up as an energy efficient trust management model that consumes less energy during the transmission of information. The efficiency of BI-TMM decreases when the number of malicious and compromised nodes increases in a network.

A trust management mechanism has been introduced to manage trust among sensor-enabled mobile devices for IoT [23]. The proposed trust management mechanism, namely SE-TMM, focuses on mobile devices that are not capable of maintaining security. In the SE-TMM, the security manager has been introduced to initiate a query to authenticate the node. The query is generated by the security manager if a node inquires other nodes about a particular information or service. The authentication of a node includes the verification of a request sends by a node. To provide confidentiality, the public key encryption mechanism is used to encrypt data. The security manager is bound to generate a public key for two communicating nodes. The public key generated by the security manager is unique. Thus, whenever a communication occurs among nodes, the public key is novel. The proposed approach is stepped ahead to provide confidentiality, authentication to users along with the integrity using encryption. However, the performance of SE-TMM is uncertain and theoretical evaluation is not sufficient to prove the effectiveness of the proposed model.

Another trust model, namely fuzzy-based trust management model (F-TMM) for IoT, is proposed in [24]. The F-TMM states that a lightweight authentication mechanism is required to authenticate whenever a new node tries to enter the IoT network [25], [26]. In the F-TMM, the reputation

of a node is built based on specific parameters and previous interactions. The trust evaluation matrices used to compute trust are packet forwarding, energy consumption, and packet forwarding capability of a node. After the evaluation of reputations, the node calculates the local and global trusts based on direct and indirect trust parameters. Furthermore, two fuzzy trust models are proposed for the global trust evaluation in the F-TMM.

A trust evaluation scheme (TES) [27] is proposed to detect the behavior of nodes in the IoT. The proposed mechanism is based on a quantitative model. The parameters used to evaluate the behavior of a node are the capacity of packet forwarding, the degree of repetition, spatial packet flexibility, data transmission delay, and data packet integrity. The direct trust evaluation of a node depends on the communication behavior. The indirect trust evaluation depends on the recommendations taken from numerous neighboring nodes. Trust parameters allow nodes to immediately recognize malicious and compromised nodes. The immediate identification of malicious nodes helps nodes to maintain the resilience towards several attacks. In the IoT, every node does not have the capability to perform calculations and maintain the security. So, the robustness of a TES may decline when a node owning a low capability performs computations.

To manage the trust of application market for the IoT, an interaction-based trust management model (IB-TMM) [28] is proposed to evaluate the trustworthiness of applications. To provide accuracy in decision making, the proposed model is based on quantitative calculations and obtain the absolute trust value. The evaluation of trust is calculated by extracting similarities among applications and users behavior. The connection between applications and users is created by using features of evaluation vector and feedback vector. After the establishment of a connection, the communication between applications and users is used to determine the behavior.

An intelligent trust management mechanism based on clustering for IoT (CITM-IoT) is proposed in [29]. The architecture of CITM-IoT consists of IoT applications, super-node, cluster, and master node. Cluster nodes are responsible for a successful transmission of data generated by the master-node. The master node is bound to coordinate nodes within a cluster. The major node in CITM-IoT is the super-node which is responsible for managing the trust of IoT environment. The CITM-IoT proposes several algorithms that perform specific tasks. These algorithms are proposed for formulating a cluster by estimation of boundaries. Algorithm 2 specifies the mechanism that allows nodes to change the master node. Algorithm 3 addresses the challenges associated with the IoT attacks. And algorithm 4 defines a mechanism for the master node to control other nodes inside the cluster. The significance of CITM-IoT is an intelligent formation of clusters. Furthermore, CITM-IoT proposes an efficient algorithm to examine and manage the trust, and observe the nodes.

A service-oriented based architecture for trust management (SOA-TM) is proposed in [30]. The proposed trust management is distributed and every node has to perform and maintain its trust towards other nodes. The direct trust evaluation of a node is obtained on the basis of information collected during direct interactions. To evaluate direct trust, the SOA-TM adopts the Bayesian framework. The indirect trust evaluation is also used in the SOA-TM that allows nodes to request other nodes for the recommendation about a particular node. The recommendations of other nodes are used by a particular node to compute the degree of the trust. The SOA-TM also proposes a storage strategy to store trust information for devices that have limited storage. Furthermore, the significance of the SOA-TM is the evaluation on the basis of proposed storage strategy. The IoT nodes use the proposed caching strategy to store the trust computations, and all nodes are able to store trust values in a limited storage memory.

A trust management mechanism based on distributed trust dissemination, named DTDM [31], is proposed to concentrate on the behavior to mitigate on-off attacks in the IoT. The DTDM classification involves the discovery of neighbors, the request of service, and the evaluation of trust. Initially, all neighbor nodes have a default trust value. A node can communicate with the neighboring node to build trust. In the second phase, nodes send a request to others to get services. Each node has a predefined reward or punishment for the services provided by other nodes. A node furnishes a reward for efficient services and punishment to inadequate services. In the last phase, nodes compute trust based on services provided by the node. The trust value range is between 1 and -1, where 1 represents trustworthy nodes and -1 signifies malicious and compromised nodes. The significance of DTDM is that it allows nodes to take the autonomous decision. The performance of DTDM is ambivalent towards good and bad-mouthing attacks. Furthermore, the approach only considers direct trust evaluations, therefore, the autonomous decision to identify the behavior of nodes can be more effective if the DTDM considers the evaluation of indirect trust by using recommendations.

To provide a reliable decision-making ability to the social IoT node, a trust management mechanism, named (SIOT-TM) [32], is proposed. To compute trust between two IoT nodes, the proposed mechanism uses direct and indirect trust matrices. The direct trust is estimated when a node is directly communicating with another node. The matrices used to evaluate direct trust includes centrality, cooperativeness, community of interest, and service score. In the SIOT-TM, the Bayes model [33] is adopted to evaluate the expected malicious and compromised node. The threshold value of a trust is predefined by the SIOT-TM and the node calculates the overall trust value to compare it with the threshold value. If the overall trust value is higher, then the threshold value represents the trustworthiness of nodes.

A centralized context-based trust management system (CTMS) [34] is proposed for IoT. The CTMS focuses on providing essential scalability, trustworthiness, and the utilization of decision tree application to enhance decision-making

abilities of nodes. The architecture of CTMS consists of objects, a service server, and a dedicated trust management server (TMS). In the CTMS, objects represent clients, users or supplicants that maintain relations and friendship among others. The service server is responsible for authenticating objects by collecting the required information. The service server can also recommend nodes for services by calculating similarities between nodes. The TMS receives feedback from objects and maintains the reputation of a node. The trust parameters used in the CTMS include feedback system, transaction weight, computation abilities, and content weight. The strength of the CTMS is that it utilizes Jaccard coefficient [35] to compute similarities among nodes.

A distributed trust management scheme (DTMS) [36] is proposed to provide defense against selective attacks. The DTMS focuses on the identification of malicious and compromised nodes. Malicious and compromised nodes are vulnerable to execute numerous attacks. In the DTMS, each node initially assigns a zero trust value to neighbor nodes. IoT nodes send a packet to determine neighboring nodes. Each node is capable of delivering specific services to other nodes. When a node demands for a service, then the successful service gets the reward. On the other side, if a node is unable to produce solicited services or collapse happens, then it gets punishment. The number of requested services is used to estimate the trust value of a particular node. The range of trust values lies between -1 and 1, where 1 represents the highest degree of trust and -1 manifests the negative trust or no trust.

A trust management mechanism based on community of interest (COI-TM) [37] is proposed to group the nodes into communities. The formation of communication depends on similarities and interests of nodes. The architecture of COI-TM consists of communities formation, bootstrap of trust evaluation, matrices, admin election, and community members updating. Each node is required to get authenticated and registered to join the community. After the formation of communities, nodes need to select an admin of the community. The matrices involved for determining the community admin are trust level of the node, capability, and sociability. Furthermore, nodes need to execute the admin selection process again when a current admin is deleted, loss the connection with the community nodes, leaves the community or it is no more in the authorized geographical area. The strength of the COI-TM is the use of Kalman filter [38] to evaluate and predict the trust value of nodes.

III. PROPOSED TRUST MANAGEMENT MECHANISM

The HoliTrust model is a combination of multiple central authorities which computes trust by collecting trust values from numerous centralized authorities that include communities servers, domain servers, and trust servers. The HoliTrust is proposed for cross-domain trust management that utilizes the concept of nodes communication among domains. In the HoliTrust, domains are further divided into a number of communities based on similarities and interest. Every community has its own community server to coordinate and perform trust computations. To secure communities, every domain has its dedicated domain server for the communication among domains and trust. Communities servers are not allowed to communicate across the domain. However, when a node is interacting across the domain, then the community server computes trust by getting information of the particular domain. To provide holistic security to IoT nodes, the HoliTrust introduces the trust server that handles all domains, computes and stores trust of domains, and issues certificates based on the degree of trust.

The proposed model comprises three layers of security, i.e., (i) a community server to secure communities, (ii) a domain server to secure the domain, and (iii) a trust server to manage the whole trust of domains. The security of these three-layer server excludes the risk of diverse attacks and also has the capability to keep resilience towards attacks. Significant aspects of the proposed model can be summed up as: (a) a community server that manages trust of IoT nodes and reduces the vulnerability of nodes occurs by a low capacity of maintaining trust, (b) a domain server to manage all communities within the domain. The ultimate security with the trust server makes the system secure from malicious and compromised nodes.

The existing centralized trust mechanisms are not able to provide holistic trust management because when a centralized authority is compromised then it may cause problems for the whole domain as there is no backup to maintain trust. Furthermore, in distributed trust management models, all nodes have to compute trust. However, this faces significant issues in managing trust. The major challenge in distributed trust management approach is such that a malicious node can compute trust of another node and assign them a higher degree of trust. Also, a compromised node can recommend a malicious node and may cause significant damage in the IoT network. The HoliTrust consists of multi-level centralized authorities where a malicious node of one community cannot affect other nodes because of the community server. Also, if a community server is compromised, then the domain server and trust server can easily recognize that compromised server. Hence, the multi-layer HoliTrust provides a secure and robust trust management approach.

IV. WORKING OF HOLITRUST MODEL

The HoliTrust is based on multiple central authorities to maintain scalability and provides holistic security to nodes. These authorities are community servers, domain servers, and trust servers. These servers work simultaneously by interacting with each other to maintain trust and stability by preserving resilience towards attacks. The communication between community servers, domain servers, and trust servers is illustrated in Figure 1. The working of servers and IoT nodes to compute trust is explained in the following sections, and Figure 2 shows the process of community server and trust evaluation of nodes.

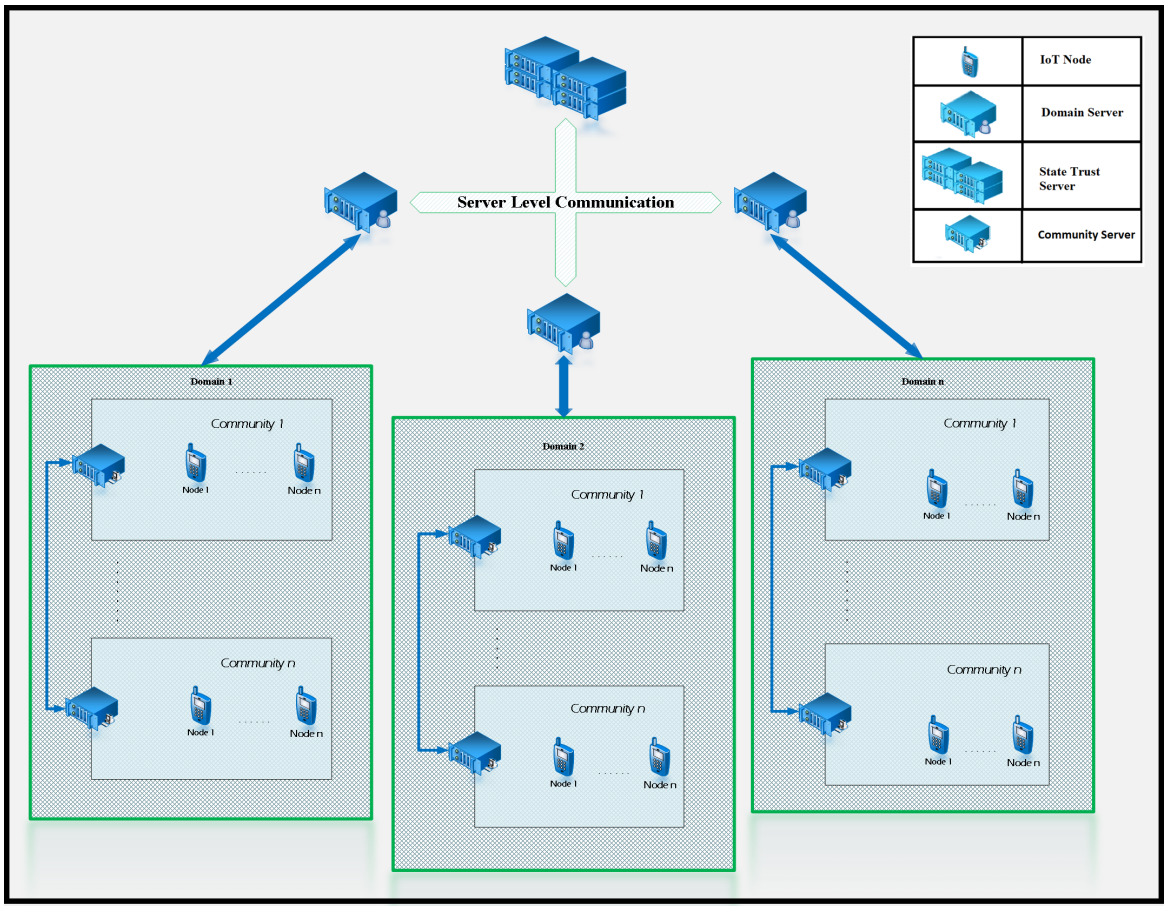

FIGURE 1. HoliTrust architecture.

A. IOT NODE

The HoliTrust consists of domains that are further divided into numerous communities and these communities contain nodes that can communicate with other nodes to perform specific tasks. These IoT nodes have their unique identity and when they communicate with each other, the message package contains node identity along with the community and domain information. In IoT, every node does not have the capability to perform computation and store trust. In the HoliTrust, when a node (trustee) requests another node (trustor) to communicate, the trustor is only responsible to analyze that trustee belongs to the same community and same domain, or different domain and community. After analysis, the trustor sends the trustee information to the community server for the trust evaluation. The IoT node has fewer responsibilities and therefore increases efficiency and scalability of nodes to perform other tasks.

B. COMMUNITY SERVER

The community server is responsible for trust computation and it is capable of communicating with other community servers within the domain. When a community server receives a request for trust evaluation, then it will execute the evaluation based on direct and indirect trust of a trustee. The calculation of trust based on direct and indirect trust is an event-driven process. The community server calculates the degree trust of the trustee whenever it receives a request from the trustor.

The direct trust evaluation involves the estimation of compatibility, honesty, and competence. The compatibility parameter of trust helps to calculate whether the trustor and trustee are capable of working together or not. If the compatibility between two nodes is maximum then the performance of these nodes is also higher. The honesty property helps to determine the malicious factor of a node. If nodes are malicious or compromised, then the honesty property of trust can recognize these nodes immediately. The competence of a node represents the capability of nodes to perform a specific task. If the competence of a node is higher, then the chance of completing a specific task is also higher. The indirect evaluation involves recommendations of various other nodes. The indirect trust is required when a community server does not have any past information about a particular node. To get recommendations, a community server requests other community servers and nodes to give recommendations about a particular node. The recommendations of other nodes are used to compute their trust.

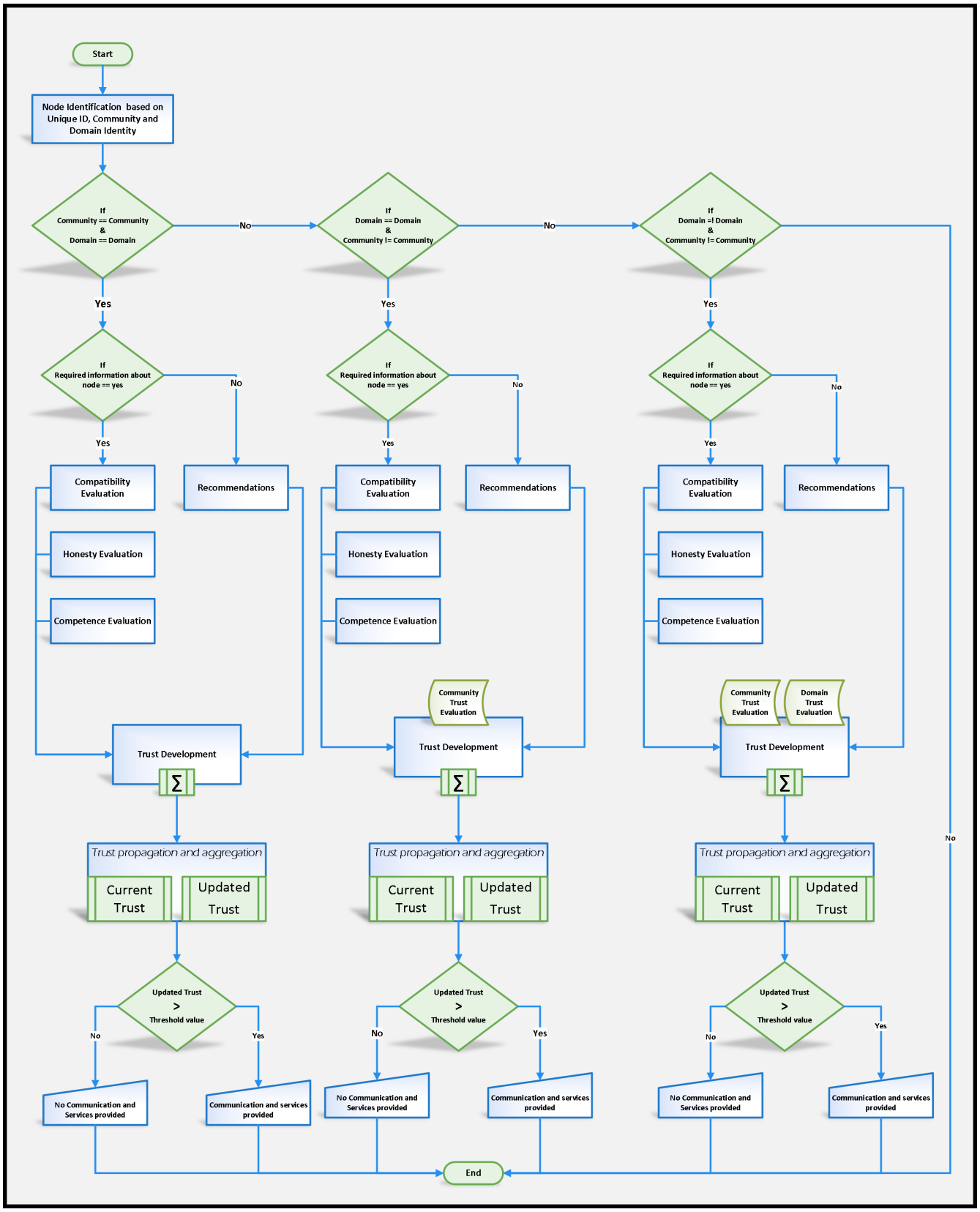

FIGURE 2. Flow diagram of node trust evaluation.

If the trustee belongs to the same community, then the community server computes trust based on direct trust or uses indirect evaluations in some cases. If the trustee belongs to some other communities of the same domain, then the community server includes the overall community trust during trust calculations. When the trustee belongs to a different domain and community, then the community server of the trustor requests its domain server to provide domain trust and community trust of the trustee.

C. DOMAIN SERVER

The domain server provides additional security to communities and secure the domain. It works as a bridge to compute the cross-domain trust of nodes. A trustor can only communicate across the domain when the domain server provides the trust of trustee's domain. The domain trust is used by the community sever to calculate the absolute trust value. The domain server is also responsible to manage the domain by coordinating with community servers to carry out the overall community trust value. Calculations of the overall community trust value is a time-driven process where domain server collects and provides these calculations to the trust server after a specific period of time. The trust server performs a specific function to formulate the trust of a domain. The rest of the process is explained in the following subsections.

D. TRUST SERVER

The trust server can be a city trust server, state trust server, or country trust server depending on the overhead of trust evaluations. One of the major responsibilities of the trust server includes calculations of domain trust values. A domain server collects data from communities and sends it to the trust server. The trust server stores and manages this data and performs calculations to estimate the trust degree of the domain. The domain degree of the trust is used further by the trust server and generates a standard trust certificate on the basis of trust and assigns it to a specific domain. The domain with standard trust certificates is allowed to communicate across the domain. The domain trust value calculation is a time-driven process and the trust server performs it after a specific interval of time.

E. TRUST DEVELOPMENT

The component of trust development allows a server to compute the absolute trust value. The community server computes three different parameters and finds the absolute trust value from the output of trust parameters by utilizing the standard sigma function. In addition, the community server uses stored data of a community to estimate the overall trust of a community and sends these calculations to the domain server. The domain server sends the overall community trust to the trust server to get a standard trust certificate for the domain. The trust server uses community trust calculations to compute the overall trust of a domain and apply the sigma function for the degree of trust computations. If the trust value is greater than the threshold value, then the trust server will assign a standard trust certificate to the domain. Domains with trust certificates are allowed to communicate across particular domains. The absolute trust value is mandatory to calculate because the HoliTrust is a quantitative model and based on absolute numbers to decide whether the node is trustworthy or not. However, servers compute the trust value and compare it with the pre-defined threshold value of trust to determine about nodes trustworthiness.

F. TRUST THRESHOLD VALUES

Trust threshold values of a node, community server, and a domain server are different from each other. The threshold trust value of IoT nodes is between 0 and 1 where 0 shows the lower degree of trust and 1 represents the higher degree. The degree of trust below 0.5 is considered as trust ignorance, 0.51 to 0.70 is considered as medium trust and 0.71 to 1.0 is considered as complete trust or supreme trust. The trust of a community server is managed by a domain server and the trust of a domain server is managed by the trust server. The threshold value for communities and domains is between 0 and 3 where 0.0 to 1.0 show no trust, 1.1 to 1.5 represent medium trust, 1.6 to 2.0 show a high degree of trust, and 2.1 to 3.0 exhibit supreme trust of a server. The servers in HoliTrust compute the degree of trust and deploy the trust development component to apply the standard sigma function for the absolute trust value. After obtaining the absolute trust, servers compare the degree of trust with the predefined threshold value to produce trust results.

G. TRUST PROPAGATION AND AGGREGATION

The trust management in the IoT is a continuous process and nodes or servers compute and update the trust degree on continuous basis. The community server of a specific domain propagates and aggregates the updated trust value with the past trust values. The domain server also propagates and aggregates the past value stored in it and updates trust of the domain. The trust propagation and aggregation allows to improve scalability, efficiency, and accuracy of a model.

V. COMPARISON OF HOLITRUST WITH EXISTING TRUST MANAGEMENT MECHANISMS

The trust management (TM) is a significant aspect to ensure and provide the required security to IoT nodes. To compare the HoliTrust with the existing trust management approaches, we have adapted objectives of the trust proposed by Yan *et al.* [14] for the achievement of holistic trust management. The trust objectives are explained below and Table 1 presents the comparison of the HoliTrust with other schemes. In this table, *(P)* means that which objective is partially supported by a particular scheme.

A. TRUST RELATIONSHIP AND DECISION (TRD)

The TM must provide an effective and reliable mechanism to evaluate the absolute trust value. The absolute trust value helps IoT nodes to take an immediate decision which increases the overall efficiency of the system.

TABLE 1. Comparison of HoliTrust with existing trust management mechanisms (adapted from [14]).

Trust Management Mechanism	TRD	DPT	PP	DFMT	DTCT	QIoTs	SSR	G	IT	HCTI
Mahmud *et al.* [20]	×	✓(P)	✓	✓	×	×	✓(P)	×	✓	×
Rehiman *et al.* [23]	×	✓	✓	✓	×	×	✓	×	✓	×
Chen *et al.* [24]	×	✓	✓	✓	✓	×	×	✓	✓*(P)*	×
Yu *et al.* [27]	×	×	✓	✓	×	✓	×	✓	✓	✓*(P)*
Kang *et al.* [28]	✓	×	✓	×	✓	✓	✓	×	×	×
Alshehri *et al.* [29]	✓	✓	×	×	✓	×	✓	×	✓	×
Chen *et al.* [30]	✓	×	×	✓	✓	✓	✓	×	✓*(P)*	✓*(P)*
Mendoza *et al.* [31]	×	×	✓	×	✓	×	✓	×	✓	✓
Kowshalya *et al.* [32]	✓	×	×	✓	×	✓	×	✓	✓	×
Abderrahim *et al.* [34]	×	✓	×	×	✓	✓	✓	✓	×	✓
Mendoza *et al.* [36]	✓	×	×	✓	✓	✓*(P)*	✓	✓	×	✓
Bao and Chen [39]	×	✓*(P)*	✓*(P)*	✓	✓	×	×	✓	✓	×
Bao and Chen [40]	×	✓*(P)*	✓*(P)*	✓*(P)*	✓*(P)*	×	×	✓	✓	×
Nitti *et al.* [41]	×	✓*(P)*	✓	✓	✓	×	✓	✓*(P)*	✓*(P)*	✓*(P)*
Liu *et al.* [42]	✓	✓*(P)*	✓*(P)*	✓	✓	×	✓	✓	✓*(P)*	✓
Ning *et al.* [43]	✓	×	×	✓	×	×	✓	✓	✓	×
Suo *et al.* [44]	✓	✓	×	×	✓	×	✓	×	×	✓
Quan *et al.* [45]	×		×	×	✓	✓	×	×	×	✓
Li *et al.* [46]	×	×	×	✓	×	✓	×	×	×	✓
Gessner *et al.* [47]	×	✓	×	✓	×	✓	✓	✓	×	×
DeLeusse *et al.* [48]	✓	×	✓	×	×	✓	✓*(P)*	✓	✓	×
Alam *et al.* [49]	×	×	✓	×	×	✓	✓	✓	×	×
Yan *et al.* [50]	✓	×	✓	✓	✓	×	✓	×	×	×
Jun *et al.* [51]	×	✓	×	×	✓	✓	✓	×	×	×
Roman *et al.* [52]	✓	✓	×	×	✓	×	×	×	×	✓
Kothmayr *et al.* [53]	✓	×	✓	×	✓	✓*(P)*	×	✓	×	✓
Javed *et al.* [54]	✓	×	✓	✓*(P)*	✓	×	×	×	×	✓
Ukil *et al.* [55]	✓	×	✓	✓*(P)*	×	✓	✓	×	×	✓
Khoo and Benjamin [56]	✓	×	×	✓	✓	×	✓	×	×	✓
Feng *et al.* [57]	✓	×	×	✓	×	✓	✓	✓	×	×
Sicari *et al.* [58]	×	×	✓	×	✓	✓	×	✓	✓	×
Huang *et al.* [59]	✓*(P)*	×	✓	×	✓	✓	✓	×	×	×
Gusmeroli *et al.* [60]	✓	×	×	✓	✓	×	×	✓	✓	✓*(P)*
HoliTrust	✓	✓	✓	✓	✓	✓	✓	✓*(P)*	✓	✓

B. DATA PERCEPTION TRUST (DPT)

This objective of the trust is concerned with the reliability to collect data of nodes. The reliability of data collection can be determined based on the system preciseness and responsiveness.

C. PRIVACY PRESERVATION (PP)

The TM mechanism should be flexible enough to preserve the privacy of confidential information of users. The mechanism must protect and restrict access to any unauthorized authority.

D. DATA FUSION AND MINING TRUST (DFMT)

In IoT, a huge amount of data is generated by the communication of nodes. The TM mechanism must be capable to process and analyze data. During processing and analyzing collected data, the TM should maintain the trustworthiness of data.

E. DATA TRANSMISSION AND COMMUNICATION TRUST (DTCT)

The TM mechanism must provide a secure transmission of information. Also, it is required that the TM provides a security to the communication of nodes.

F. QUALITY OF IOT SERVICES (QIOTS)

The TM should provide the trust at the right time to the right node and maintain the quality of service. The quality of IoT services is the objective property of trustees and the subjective property of trustors.

G. SYSTEM SECURITY AND ROBUSTNESS (SSR)

The robustness of TM is a significant factor for the IoT heterogeneous environment. The TM mechanism should provide the required security and robustness to nodes in order to gain the confidence of a node.

H. GENERALITY (G)

The generality of TM can be analyzed by the capability of a wide deployment. The TM mechanism should be generic and must have the generality to be deployed widely.

I. IDENTITY TRUST (IT)

The trustworthiness of IoT can only be achieved if the identity of a node is well managed. However, the TM mechanism should have the capacity to efficiently manage identities of nodes.

J. HUMAN-COMPUTER TRUST INTERACTION (HCTI)

The TM mechanism must provide security and usability to users in parallel. The usability of a mechanism is a major challenge because it is really difficult to provide usability that maintains the required level of security. The usability of TM is required so that users can easily interact with the system.

VI. CONCLUSION

In this paper, we proposed HoliTrust which is efficient to manage trust during cross-domain communications in the IoT. The prior researches have already proposed numerous trust management mechanisms, but the prologue of cross-domain trust management mechanism is ignored over years. To ensure the accuracy and efficiency of the HoliTrust, we developed multiple central authorities, i.e., community, domain, and trust servers. These authorities increase the accuracy and reduce the computation weight on IoT nodes. Reducing the computation weight helps to subdue vulnerability, intensify resilience towards attacks, and furnish adequate security. The HoliTrust is efficient to provide sufficient security to cross-domain communication by utilizing community trust and domain trust along with trust parameters.

REFERENCES

[1] 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.

[2] H. A. Khattak, H. Farman, B. Jan, and I. U. Din, "Toward integrating vehicular clouds with IoT for smart city services," *IEEE Netw.*, vol. 33, no. 2, pp. 65–71, Mar./Apr. 2019.

[3] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *Proc. 9th Int. Conf. Comput. Intell. Secur. (CIS)*, Dec. 2013, pp. 663–667.

[4] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," *Comput. Netw.*, vol. 141, pp. 199–221, Aug. 2018.

[5] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," *Comput. Netw.*, vol. 112, pp. 237–262, Jan. 2017.

[6] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in Internet of Things with privacy preserving: Challenges, solutions and opportunities," *IEEE Netw.*, vol. 32, no. 6, pp. 144–151, Nov./Dec. 2018.

[7] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation," *Future Gener. Comput. Syst.*, vol. 76, pp. 540–549, Nov. 2017.

[8] J. B. Bernabe, J. L. Hernandez-Ramos, and A. F. S. Gomez, "Holistic privacy-preserving identity management system for the Internet of Things," *Mobile Inf. Syst.*, vol. 2017, Aug. 2017, Art. no. 6384186.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] W. Abdelghani, C. A. Zayani, I. Amous, and F. Sèdes, "Trust management in social Internet of Things: A survey," in *Social Media: The Good, Bad, Ugly*, Y. K. Dwivedi *et al.*, Eds. Cham, Switzerland: Springer, 2016, pp. 430–441.

[14] 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.

[15] K.-D. Chang and J.-L. Chen, "A survey of trust management in WSNs, Internet of Things and future Internet," *KSII Trans. Internet Inf. Syst.*, vol. 6, no. 1, pp. 5–23, 2012.

[16] T. Pasquier, J. Singh, J. Powles, D. Eyers, M. Seltzer, and J. Bacon, "Data provenance to audit compliance with privacy policy in the Internet of Things," *Pers. Ubiquitous Comput.*, vol. 22, no. 2, pp. 333–344, 2018.

[17] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.
[18] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.
[19] N. B. Truong, U. Jayasinghe, T.-W. Um, and G. M. Lee, "A survey on trust computation in the Internet of Things," *J. Korean Inst. Commun. Inf. Sci.*, vol. 33, no. 2, pp. 10–27, 2016.
[20] M. Mahmud *et al.*, "A brain-inspired trust management model to assure security in a cloud based iot framework for neuroscience applications," *Cogn. Comput.*, vol. 10, no. 5, pp. 864–873, Oct. 2018. doi: 10.1007/s12559-018-9543-3.
[21] J.-S. R. Jang, C.-T. Sun, and E. Mizutani, "Neuro- fuzzy and soft compting—A computational approach to learning and machine intelligence," *IEEE Trans. Autom. Control*, vol. 42, no. 10, pp. 1482–1484, Oct. 1997.
[22] M. G. Iskander, "A fuzzy weighted additive approach for stochastic fuzzy goal programming," *Appl. Math. Comput.*, vol. 154, no. 2, pp. 543–553, 2004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0096300303007343
[23] K. A. R. Rehiman and S. Veni, "A trust management model for sensor enabled mobile devices in IoT," in *Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)*, Feb. 2017, pp. 807–810.
[24] 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.
[25] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 1, pp. 41–77, 2005.
[26] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sensor Netw.*, vol. 2, no. 4, pp. 500–528, 2006.
[27] 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.
[28] K. Kang, Z. Pang, L. D. Xu, L. Ma, and C. Wang, "An interactive trust model for application market of the Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1516–1526, May 2014.
[29] M. D. Alshehri, F. K. Hussain, and O. K. Hussain, "Clustering-driven intelligent trust management methodology for the Internet of Things (CITM-IoT)," *Mobile Netw. Appl.*, vol. 23, no. 3, pp. 419–431, 2018.
[30] I.-R. Chen, J. Guo, and F. Bao, "Trust management for SOA-based IoT and its application to service composition," *IEEE Trans. Services Comput.*, vol. 9, no. 3, pp. 482–495, May/Jun. 2016.
[31] 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.
[32] A. M. Kowshalya and M. L. Valarmathi, "Trust management for reliable decision making among social objects in the social Intrnet of Things," *IET Netw.*, vol. 6, no. 4, pp. 75–80, 2017.
[33] Bled Electronic Commerce, A. Jøsang, and R. Ismail, "The beta reputation system," in *Proc. 15th Bled Electron. Commerce Conf.*, 2002, pp. 1–14.
[34] 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.
[35] G. Dunn and B. S. Everitt, *An Introduction to Mathematical Taxonomy*. Chelmsford, MA, USA: Courier, 2004.
[36] C. V. L. Mendoza and J. H. Kleinschmidt, "Defense for selective attacks in the IoT with a distributed trust management scheme," in *Proc. IEEE Int. Symp. Consumer Electron. (ISCE)*, Sep. 2016, pp. 53–54.
[37] 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.
[38] C. K. Chui *et al.*, *Kalman Filtering*. Cham, Switzerland: Springer, 2017.
[39] 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.
[40] 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.
[41] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social Internet of Things," in *Proc. IEEE 23rd Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2012, pp. 18–23.
[42] Y. Liu, Z. Chen, F. Xia, X. Lv, and F. Bu, "A trust model based on service classification in mobile services," in *Proc. IEEE/ACM Int. Conf. Green Comput. Commun., Int. Conf. Cyber, Phys. Social Comput.*, 2010, pp. 572–577.
[43] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the Internet of Things," *Computer*, vol. 46, no. 4, pp. 46–53, Apr. 2013.
[44] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A review," in *Proc. Int. Conf. Comput. Sci. Electron. Eng. (ICCSEE)*, vol. 3, Mar. 2012, pp. 648–651.
[45] Z. Quan, F. Gui, D. Xiao, and Y. Tang, "Trusted architecture for farmland wireless sensor networks," in *Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Dec. 2012, pp. 782–787.
[46] X. Li, Z. Xuan, and L. Wen, "Research on the architecture of trusted security system based on the Internet of Things," in *Proc. 4th Int. Conf. Intell. Comput. Technol. Automat. (ICICTA)*, vol. 2, Mar. 2011, pp. 1172–1175.
[47] D. Gessner, A. Olivereau, A. S. Segura, and A. Serbanati, "Trustworthy infrastructure services for a secure and privacy-respecting Internet of Things," in *Proc. 11th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Jun. 2012, pp. 998–1003.
[48] P. de Leusse, P. Periorellis, T. Dimitrakos, and S. K. Nair, "Self managed security cell, a security model for the Internet of Things and services," in *Proc. 1st Int. Conf. Adv. Future Internet*, Jun. 2009, pp. 47–52.
[49] S. Alam, M. M. R. Chowdhury, and J. Noll, "Interoperability of security-enabled Internet of Things," *Wireless Pers. Commun.*, vol. 61, no. 3, pp. 567–586, 2011.
[50] Q. Yan, R. H. Deng, Z. Yan, Y. Li, and T. Li, "Pseudonym-based RFID discovery service to mitigate unauthorized tracking in supply chain management," in *Proc. 2nd Int. Symp. Data, Privacy, E-Commerce (ISDPE)*, Sep. 2010, pp. 21–26.
[51] W. Jun, M. Lei, and Z. Luo, "Data security mechanism based on hierarchy analysis for Internet of Things," in *Proc. Int. Conf. Innov. Comput. Cloud Comput.*, 2011, pp. 68–70.
[52] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013.
[53] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2710–2723, 2013.
[54] N. Javed and T. Wolf, "Automated sensor verification using outlier detection in the Internet of Things," in *Proc. 32nd Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, Jun. 2012, pp. 291–296.
[55] A. Ukil, J. Sen, and S. Koilakonda, "Embedded security for Internet of Things," in *Proc. 2nd Nat. Conf. Emerg. Trends Appl. Comput. Sci. (NCETACS)*, Mar. 2011, pp. 1–6.
[56] B. Khoo, "Rfid as an enabler of the Internet of Things: Issues of security and privacy," in *Proc. Int. Conf. Internet Things, 4th Int. Conf. Cyber, Phys. Social Comput. (iThings/CPSCom)*, Oct. 2011, pp. 709–712.
[57] H. Feng and W. Fu, "Study of recent development about privacy and security of the Internet of Things," in *Proc. Int. Conf. Web Inf. Syst. Mining (WISM)*, vol. 2, Oct. 2010, pp. 91–95.
[58] S. Sicari, A. Coen-Porisini, and R. Riggio, "DARE: Evaluating data accuracy using node reputation," *Comput. Netw.*, vol. 57, no. 15, pp. 3098–3111, 2013.
[59] X. Huang, B. Chen, A. Markham, Q. Wang, Z. Yan, and A. W. Roscoe, "Human interactive secure key and identity exchange protocols in body sensor networks," *IET Inf. Secur.*, vol. 7, no. 1, pp. 30–38, Mar. 2013.
[60] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the Internet of Things," *Math. Comput. Model.*, vol. 58, nos. 5–6, pp. 1189–1205, 2013.

KAMRAN AHMAD AWAN received the bachelor's degree in computer science from the Department of Information Technology, University of Haripur, in 2015, where he is currently pursuing the M.Sc. degree in computer science. His current research interests include information security, vehicular ad-hoc networks, and the Internet of Things with a particular emphasis on its trust management mechanisms.

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, in 2006 and 2011, respectively, and the Ph.D. degree in computer science from the School of Computing, Universiti Utara Malaysia (UUM), where he was a member of the InterNetWorks Research Laboratory, from 2014 to 2016. 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.

MAHDI ZAREEI (S'11–M'17) received the M.Sc. degree in computer network from the University of Science, Malaysia, in 2011, and the Ph.D. degree from the Communication Systems and Networks Research Group, Malaysia-Japan International Institute of Technology, University of Technology, Malaysia, in 2016. In 2017, he joined the School of Engineering and Sciences, Tecnologico de Monterrey, as a Postdoctoral Fellow, where he is currently a Research Professor. His researches mainly focus on wireless sensor and ad hoc networks, energy harvesting, cognitive radio networks, and performance optimization. He is a member of the Mexican National Researchers System (level I). He received the JASSO Scholarship, in 2015, to perform a part of his Ph.D. research with Osaka University. He is also serving as an Editor for the IEEE Access.

MUHAMMAD TALHA received the Ph.D. degree in computer science from the Faculty of Computing, University of Technology, Malaysia. He is currently with the Deanship of Scientific Research, King Saud University, Riyadh, Saudi Arabia. His research interests include image processing, medical imaging, features extraction, classification, and machine learning techniques.

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 served as the Associate Vice President of Graduate Studies, Qatar University, University of Idaho, Western Michigan University, and University of West Florida. He 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 more than 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 ACM. He also served as a Member, Chair, and General Chair of a number of international conferences. He received three teaching awards and four research awards throughput his career. He 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 served as the IEEE Computer Society Distinguished Speaker, from 2003 to 2005. He guest edited a number of special issues in IEEE journals and magazines. He is currently the Editor-in-Chief of the *IEEE Network Magazine*, serves on the Editorial Board of several international technical journals and the Founder and the Editor-in-Chief of *Wireless Communications and Mobile Computing* journal (Wiley).

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 associated with the Department of Information Technology, The University of Haripur. He has 13 years of teaching and research experience in different national and international universities/organizations. His current research interests include trust management in the Internet of Things, network and information security, cloud computing, and management information systems.