IEEE Access
Multidisciplinary Rapid Review Open Access Journal

Received January 25, 2020, accepted February 6, 2020, date of publication February 10, 2020, date of current version February 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2972968

Context-Aware Trust and Reputation Model for Fog-Based IoT

YASIR HUSSAIN[1], **HUANG ZHIQIU**[1], **MUHAMMAD AZEEM AKBAR**[1], **AHMED ALSANAD**[2], **ABEER ABDUL-AZIZ ALSANAD**[3], **ASIF NAWAZ**[1], **IZHAR AHMED KHAN**[1], **AND ZAHEER ULLAH KHAN**[1]

[1]College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
[2]Research Chair of Artificial Intelligence (RCAI), Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia
[3]Information Systems Department, College of Computer and Information Sciences, Imam Muhammad Ibn-Saud Islamic University, Riyadh 11432, Saudi Arabia

Corresponding authors: Yasir Hussain (yaxirhuxxain@nuaa.edu.cn) and Ahmed Alsanad (aasanad@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research, King Saud University, for funding through Vice Deanship of Scientific Research Chairs.

ABSTRACT Trust and reputation are important terms whether the communication is Humans-to-Human (H2H), Human-Machine-Interaction (HMI) or Machine-to-Machine (M2M). As Cloud computing and the internet of things (IoT) bring new innovations, they also cause various security and privacy issues. As numerous devices are continuously integrating as a core part of IoT, it is necessarily important to consider various security issues such as the trustworthiness of a user or detection of a malicious user. Moreover, fog computing also known as edge computing is revolutionizing the Cloud-based IoT by providing the Cloud services at the edge of the network, which can provide aid in overcoming security, privacy and trust issues. In this work, we propose a context-aware trust evaluation model to evaluate the trustworthiness of a user in a Fog based IoT (FIoT). The proposed approach uses a context-aware multi-source trust and reputation based evaluation system which helps in evaluating the trustworthiness of a user effectively. Further, we use context-aware feedback and feedback crawler system which helps in making trust evaluation unbiased, effective and reliable. Furthermore, we introduce monitor mode for malicious/untrustworthy users, which helps in monitoring the behavior and trustworthiness of a user. The proposed approach uses several tunable factors, which can be tuned based on the system's requirements. The simulations and results indicate that our approach is effective and reliable to evaluate the trustworthiness of a user.

INDEX TERMS Fog computing, internet of things, edge computing.

I. INTRODUCTION

Trust is an important aspect of communication whether it is Humans-to-Human (H2H), Human-Machine-Interaction (HMI) or Machine-to-Machine (M2M). It is estimated by Cisco[1] that, 50 billion "things" will be interconnected with the internet by 2020. As the internet of things (IoT) revolutionizes and combine devices to share data and information to build a smart world, it also causes several first-hand challenges. Many surveys [1]–[5] have highlighted the security, privacy, and trust issues in IoT. The classical IoT architecture is generally based on three layers [4] an application layer, a network layer, and a sensor layer. Due to the resource constrictive [6] nature of IoT devices, they rely on Clouds for data, processes, and services. Zhang *et al.* [7] have discussed the Cloud architecture, service models and deployment models in detail.

Fog computing extends[2] Cloud computing to the network's edge. In FIoT, sensors and other connected devices send data to a nearby Fog node. This could be a gateway device, such as a switch or router, which can perform initial processing on data or can help to identify malicious nodes. Many survey articles [8]–[10] had shown the importance of Fog computing in the context of IoT. Several survey articles [11]–[14] discuss

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

[1] CISCO (2015). Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are [online]. [accessed 16 September 2019]

[2] NIST (2017). The NIST Definition of Fog Computing [online]. [accessed 16 September 2019]

the architectural design of FIoT and its future opportunities and challenges.

Security, Privacy, and trust [8]–[10], [15], [15], [16] are the most common issues in Cloud-based IoT. FIoT can help in overcoming security, privacy and trust issues [8]–[10], [15], which reside normally in Cloud-based IoT. The current growth in IoT and Cloud technologies make it easy to expose to vulnerabilities. Connecting Cloud-based IoT networks with the help of a middleman (Fog) can help alleviate various issues. Many articles [8]–[13] have discussed the need and importance of Fog in Cloud-based IoT.

In this paper, we propose a context-based trust and reputation model for FIoT. Most of the previous models do not consider the user's context. In this work, we take into account the context of a connecting device to evaluate its trustworthiness. We propose a context-aware reputation evaluation approach to help evaluate a user's trustworthiness. Further, we use a multi-source based trust and reputation approach which makes the proposed approach unbiased, effective and reliable. We proposed a monitor mode that assists the system to monitor the behavior of untrusted users for better security. It can help to secure the FIoT from malicious users for requesting/manipulating any sensitive data.

This work makes the following unique contributions.

- A multi-source based trust evaluation approach which takes into account the context and reputation of participating nodes while evaluating a user's trustworthiness.
- We introduce context-aware feedback and feedback crawler system which helps in making trust evaluation unbiased, effective and reliable.
- A monitor mode is proposed which helps to identify malicious users before they can actually make any communication with the Cloud. By putting malicious users in monitor mode assists Fog nodes to prevent any security issue.
- An extensive evaluation of the proposed approach with simulations and results indicate that the proposed approach is effective and reliable to evaluate the trustworthiness of a user.

Rest of the papers is organized as follows: **Section 2** discusses related work. **Section 3** briefly describes purposed approach. **Section 4** presents the evaluation of our proposed approach. **Section 5** is about the conclusion and future work.

II. RELATED WORK

Trust is a crucial aspect of success these days. Hoffman *et al.* [17] have provided a generic trust model and metrics definitions. They highlight the importance of trust in the context of security, privacy, usability, and user experience. Guo *et al.* [18] have presented a trust-based privacy preserved approach to recommend to friends in SON (Social online Network). Husseini *et al.* [19] have proposed a trust model for resource constraint devices and associativity implemented with an authentication protocol. They use the privacy-preserved based model to evaluate the trust of a participant. They used the question of trust approach to improve the model immunity for malicious users. They used a user rating and context-aware feedback system to evaluate the trust of a participant focusing on Human-to-machine interaction by keeping the other aspects untouched.

Jøsang *et al.* [20] have provided a comprehensive survey of trust and reputation. They discussed, how trust and reputation can help to overcome security issues in different areas where users intact with each other. They have provided a number of models and proposed a system to measure trust and reputation to analyze the current trends. They used different commercial sites to show the used models such as the Google system of web page ranking, Amazon, eBay feedback forum, product review sites, expert's sites, and discussion forums. In a survey, Yan *et al.* [21] discussed the importance of trust management in IoT. They discussed the current trends and models to show the versatility of trust management.

Trustworthiness is an important aspect of social IoT. Nitti *et al.* [22] have proposed a subjective and objective model approach for trustworthiness management. Their experimental evaluation shows the difference between the two approaches and provides valuable thoughts. Al-Hamadi *et al.* [23] proposed a trust-based decision-making for health IoT. In their trust model, they used risk management, the reliability of trust and loss of health probability. Kang *et al.* [24] had proposed a trust model for IoT application and provide a working prototype for an android app that shows privacy leak in any concerned app.

Abdallah *et al.* [25] have presented an Infrastructure as a Service (IaaS) based Cloud trust model(TRUST-CAP). In their model, they highlighted the trust properties that should exist in a trust model. Their model focus on four components: integrity, access control, availability and privacy to secure the model from Man-At-The-End (MATE) attacks. Lin *et al.* [26] proposed a Mutual Trust-Based Access Control Model in Cloud Computing (MTBAC). Their proposed model is based on two aspects that are, user's trust-based access control (UTBAC) and Cloud service node's trust-based access control (CSTBAC). Trust evaluation in their model is based on three attributes which are confidentiality, integrity, and reputation.

Recently, trust has played a vital role to help preserve the privacy and to enhance the security of social networks [27]–[30]. Zlatolas *et al.* [31] proposed a model for privacy issues, trust and self-disclosure in online social networks (OSN) by considering various factors such as privacy risk, privacy value, trust on Facebook, self disclosure, privacy control and privacy concerns. They validate their model by using a survey attended by 602 respondents. Liu *et al.* [32] conducted a survey aiming at providing an overview of state-of-the-art researches in pairwise trust prediction using machine learning techniques in the domain of social networking. A similar work has been done by Chen *et al.* [33] in which they proposed a trust evaluation framework based on machine learning to facilitate human decision-making by considering multiple trust-related user features and criteria. Meo [34] have proposed PTP-MF (Pairwise Trust Prediction

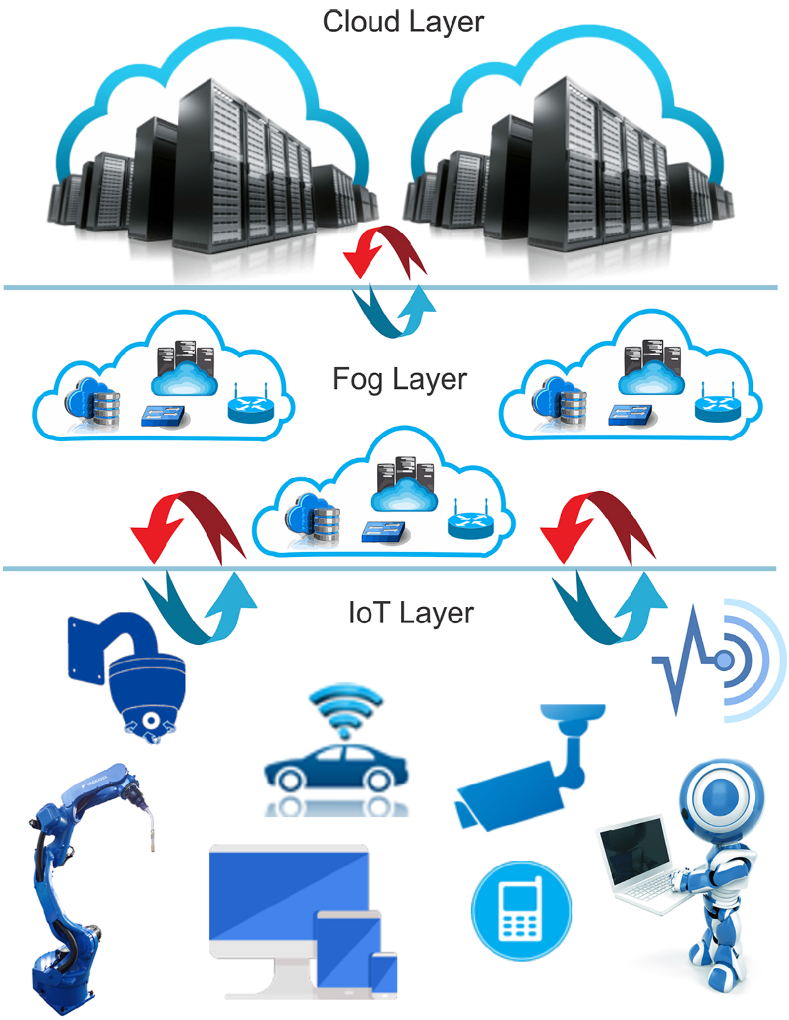

FIGURE 1. Three layered architecture of Fog-based IoT (FIoT).

through Matrix Factorization) algorithm, an approach to predicting the intensity of trust and distrust relations in Online Social Networks (OSNs). They use the dot product approach between a trustor *i* and trustee *j*. Further, they take leverage of trustee behavior to enhance the accuracy of their model.

Chen *et al.* [35] have proposed IoTrust, a trust architecture that integrates Soft Defined Network (SDN) in IoT, and a cross-layer authorization protocol based on IoTrust. They further propose a Behavior-based reputation evaluation scheme for the node and an organization reputation evaluation. Debe *et al.* [36] have proposed a decentralized trust model in order to maintain the reputation of publicly available fog nodes using Ethereum blockchain and smart contract technologies. The reputation is maintained considering users' opinions about their past interactions with the public fog nodes. A similar work has been done by Fortino *et al.* [37] which proposed a reputation-based model for grouping IoT agents Using blockchain. Fortino *et al.* [38] have proposed a trust and local reputation based model for group formation in the cloud of things. Zhang *et al.* [39] have proposed a trust model and related algorithm to decrease trust management overhead and improve malicious node detection ability based on domain partition. Wu *et al.* [40] have proposed a two-phase method to calculate service reputation. The first phase uses a dynamic weight method to calculate reputation and second one uses an olfactory response method to mitigate the unfair ratings.

There are several models [41]–[44], which are based on service level argument (SLA) and quality of service (QoS) which plays an important role in the trust evaluation of a cloud provider. Ghahramani *et al.* [41] have carried out comprehensive survey with respect to the enforcement principles to address the QoS guarantee issue. Manuel [42] has proposed a trust model of cloud computing based on Quality of Service (QoS) with the natural language-based algorithm. Another SLA-Based trust model for cloud computing was presented by Alhamad *et al.* [43]. Similarly, Kirkman and Newman [44] has presented a policy Model based on ORCON [3] to fill the trust gap between different Clouds and to provide better trust management for Cloud users. In their

[3] DNI (2016). Orcon, [accessed 16 September 2018]

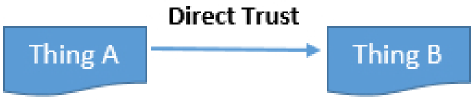

FIGURE 2. Direct trust in FIoT.

work, they proposed cloud insurance, trust the third party and using local data storage to increase user trust for a Cloud provider. Fog is providing aid to current Cloud-based IoT infrastructure to help to overcome security, privacy, and trust issues. Fog can also help to eliminate middle authority which seems to be an essential part of Cloud-based IoT by bridging the gap between IoT and Cloud.

III. CONTEXT-AWARE TRUST AND REPUTATION MODEL FOR FIOT

Fog-based IoT (FIoT) is a three-layered architecture as shown in figure 1. First, IoT layer where devices collect and sense data and forward to the Fog/Edge node. The second layer, Fog/Edge node can perform preprocessing on the collected data at the local network before outsourcing it to the Cloud. Finally, the data is outsourced to a Cloud to perform extensive computation and storage purposes. In this section, we briefly describe the proposed approach. First, we define what trust and reputation are in FIoT. Second, we narrate what is context and the role of context. Then we briefly describe our proposed model and its framework.

A. TRUST AND REPUTATION IN FIOT

There are several definitions of *Trust* which makes it is hard to generalize it in a single statement. Gambetta [45] has defined trust as *"Trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends"*. McKnight and Chervany [46] have defined it as *"Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible"*. Hussain and Huang [47] has defined trust in IoT as, *A "Thing's" belief in another "Thing's" honesty, reliability, and capabilities based on its experiences"*, Whereas Reputation can be defined as, *A "Thing's belief in another "Thing's" honesty, reliability, and capabilities recommended by other "Things"*. Now, there can be different types of trust. In this work, we identify three kinds of trust such as direct trust, derived trust, and recommendation trust. **Direct Trust -** Such trust can be defined as *"Thing A" trust directly "Thing B" based on its own experience*. Figure 2 is an example of Direct Trust.

Derived Trust - Whereas derived Trust can be defined as *If "Thing A" trust directly "Thing B" and "Thing B" trust directly "Thing C" then we can say that "Thing C" can be trusted by "Thing A"*. Figure 3 shows an example of derived trust.

Recommendation-based Trust - Recommendation-based Trust can be defined as, If "Thing A" trust directly "Thing B" and "Thing B" trust directly "Thing C" then "Thing B" can recommend "Thing C" to "Thing A" as trusted. In recommendation-based trust, we assume "Thing A" trust "Thing B's" recommendations based on its reputation and previous experience. Figure 4 is an example of Recommendation-based trust.

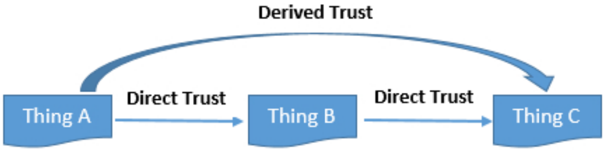

FIGURE 3. Derived trust in FIoT.

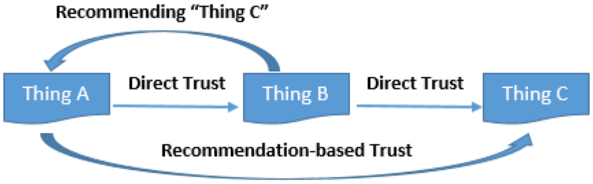

FIGURE 4. Recommendation trust in FIoT.

B. ROLE OF CONTEXT IN FIOT

Before we continue to explain the working of the proposed approach, it is necessary to explain what is the context in FIoT. A context defines a user/device's sole purpose for the network. For example, a video surveillance node, whose behavior is supposed to record the video feeds, video recording in the context of that vary node. In case a node tries to access any other kind of information, it has violated its sole purpose. Incorporating such information while evaluating the node's trustworthiness can help to improve the trust and reputation evaluation in FIoT.

C. ARCHITECTURE DESIGN

This section discusses the architecture design of the proposed approach in detail. Table 1 shows system general abbreviations and notations of our system. As shown in figure 5 starting from the ground level (IoT Layer) IoT device/user can be denoted as D_{id}, where id is a unique identification number. These devices/users sense and collect data and send it to local area network Access Point "AP_{LAN}" to forward it to the Fog node "F_i".

The fog layer, which is the key concept of our proposed work, relies only on the user's public key for Trust Evaluation (TE). Recently, a number of researchers [8], [48]–[51] have proposed authentication techniques for FIoT. For the simplicity of trust mechanism, here we assume UserID(D_{id}) based approach to uniquely identify a device/user for evaluation of its trust level(TL), where TL range between [0, 1]. The TE has two major components S1 and S2, where S_1 is the logic carrying server having all the logical parts to evaluate the trustworthiness of the D_{id} and S_2 is database server having the trust level of all users $\sum_{i=1}^{n} TL_{D_{id}}$. Mutual separation of logic

TABLE 1. System general abbreviations and notations.

Notation	Description
D_{id}	IoT user/device Where id is Universal identification number.
D_{id}^{CTX}	IoT user/device context.
F_i	Fog node Where i is a Universal identification number.
TE	Trust Evaluation System
$S_1, S_2 \in TE$	S_1, S_2 System logical, Data store unites.
CTX	Context of a user/device
TL	Trust Level Where $TL \in [0, 1]$.
$TL_{D_{id}}$	Trust Level of an IoT user/device.
$TL_{D_{id}}^{F_i}$	Trust Level of an IoT user/device in a specific Fog node.
$TL_{D_{id}}$	Trust Level of an IoT user/device.
FB	Feedback Where $Fb \in [0, 1]$.
$FB_{D_{id}}^{F_i}$	Feedback of an IoT user/device from a specific Fog node.
$RV_{D_{id}}$	Reputation value of a user/device.
$MM_{D_{id}}$	Monitor Mode status of a specific device.
$\alpha, \beta, \gamma, \rho$	Weight factors used for trust and reputation evaluation.
CD	Connected devices/nodes.
TT	Trust Table, generated based on Fog/Cloud node's historical experience.

and trust data results in an extra layer of protection which prevents access/manipulation of trust level from hackers users.

We will discuss the Logical *TE* process in detail in the coming sections. Fog node forward $TL_{D_{id}}^{F_i}$ to the Cloud Provider which is on Cloud Layer. An extensive trust evaluation can be performed by the Cloud in order to find the device trustworthiness $TL_{D_{id}}^{C_i}$. After a successful transaction, the Cloud can return a trust reward/punishment based on the content of the user. Consequently, it can be gain or loss in trust on the basis of the user's participation. We use context-aware feedback *FB* system to compute the gain/loss in trust of a particular device $FB_{D_{id}}^{F_i}$ where $FB \in [-1, 1]$.

We introduce the monitor mode in our system to identify malicious users before they start a communication. By putting malicious users in monitor mode helps the Fog nodes isolate malicious/untrustworthy users. It can help the system to prevent form possible security issues. The multi-source trust evaluation approach makes our system more reliable, effective and trustworthy. Further, we use weight factors that can be tuned based on the requirements of a particular system.

To evaluate the trust of a user we use two approaches collaboration-based approach and contents based approach. we have briefly enlightened the mentioned approaches as following;

1) COLLABORATION-BASED TRUST

In Collaboration based trust evaluation approach, we build the $TL_{D_{id}}$ of a user through linking it with other devices/users and Fog nodes by taking their Context *CTX* and reputation into account. With this approach, the system can know the current status of a device's/user's trust level based on its interaction with other devices/Fog nodes. By collaborating with a number of devices, Fog node can effectively know the trustworthiness of a connecting user and can identify as malicious or trustworthy on the basis of its own as well as other participating devices experience. Here, we consider the reputed and directly connected devices/users and Fog nodes to participate in a user's trust evaluation.

2) CONTENT-BASED TRUST

The content-based trust approach basis on the worthiness of the content a device or user shares. The Fog node checks the *CTX* relevance of a connecting user and sends gain/loss in trust as a reward/punishment. This approach helps to assist the system to declare a user as malicious if it sends irrelevant or malicious data to the system. Furthermore, this approach can also assist the system to overcome the cold-star problem.

D. TRUST EVALUATION PROTOCOL

For the effective and reliable trust evaluation, it is insufficient to focus on a single source. For improved trust evaluation, we use a systematic multi-source trust evaluation approach to build the trust level of a user by taking into account of participating user's reputation and context. Based on the previous $TL_{D_{id}}$, the system will collaborate with directly connected devices/users and Fog nodes to participate in the $TE_{D_{id}}$ based on their reputation and relevance to the context. Here, we only consider directly connected nodes for the trust evaluation process. Figure 6 shows the logical model of our purposed approach. When a device is connected to a Fog node F_i it shares its D_{id} along with its trust table(*TT*)(Eq. 1.1). This *TT* contains the trust levels of other users with which this user/device has interacted. The system uses *TT*'s as collaboration (derived trust) for other users *TE* in the future. Current F_i looks the D_{id} in its trust database. If no previous $TL_{D_{id}}$ transaction history has found then *TE* can be expressed via Eq. 1.2 by using our purposed Collaboration-based and Content-based approach.

$$TT^{D_{id}} = \sum_{i=1}^{n} TL_{D_{id}^{i}} \tag{1.1}$$

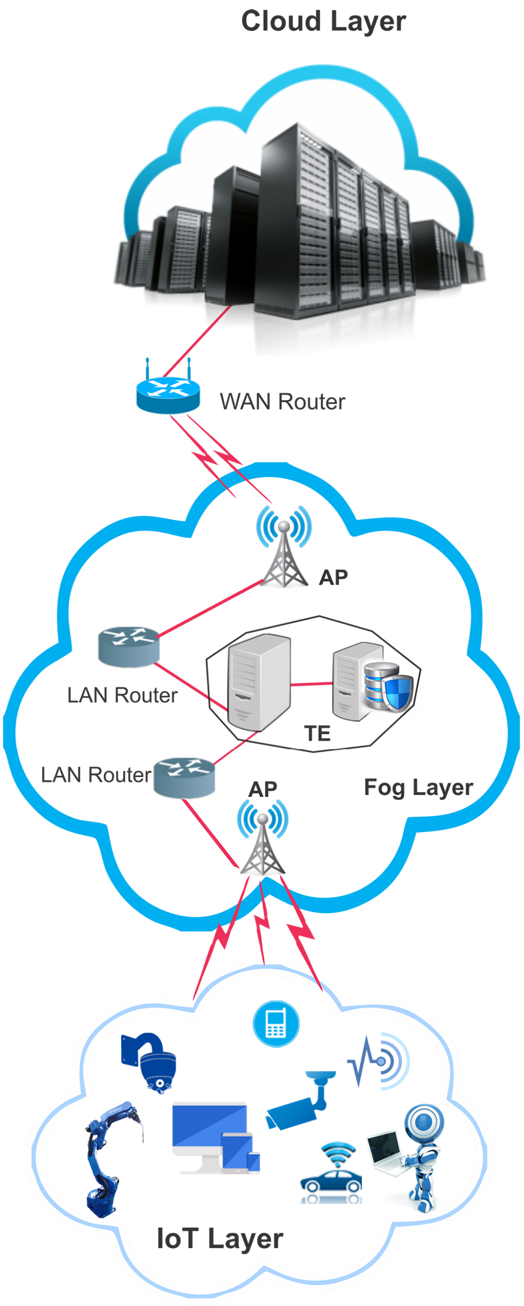

FIGURE 5. Context-aware trust and reputation System for FIoT.

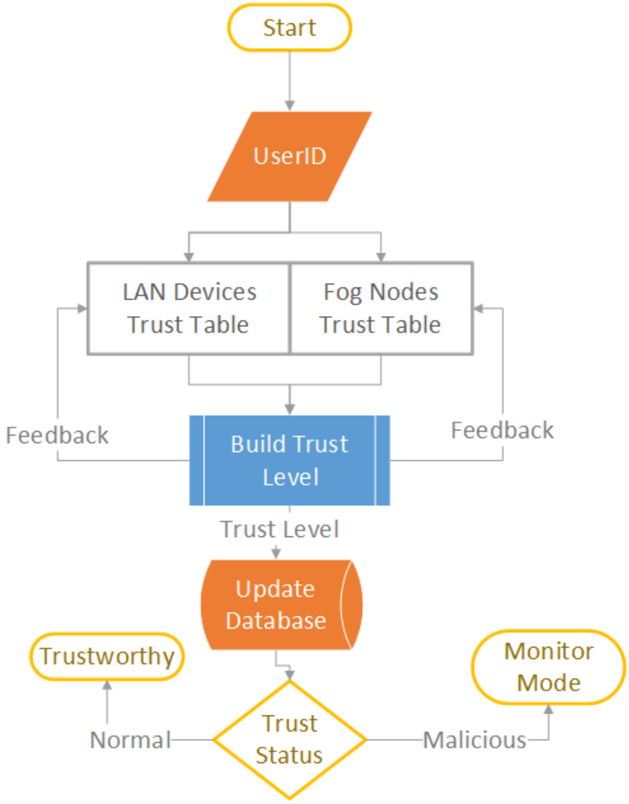

FIGURE 6. Context-aware trust evaluation logical architecture for FIoT.

D_{id} is unique for every IoT user. N is collective number of TL found for that particular D_{id} in CD, F nodes respectively based on the relevance of the context.

$$TL^{CD,F}_{D_{id}} = \beta \times \sum_{i=1}^{n} \frac{TL^{CD_i^{TT}}_{D_{id}}}{N} + \gamma \times \sum_{i=1}^{n} \frac{TL^{F_i^{TT}}_{D_{id}}}{N} \quad (1.2)$$

β, γ are the weight factors that can be tuned accordingly.

Furthermore, for the cold-star problem, the system can perform an initial content-based evaluation to further classify the node as trusted or malicious. If $TL^{CD,F}_{D_{id}} \in \emptyset$ then $TL^{New}_{D_{id}} = 0.5$ and be synced in all $CD's/F's$ that have participated in the $TE_{D_{id}}$. It also put the device/user in monitor mode to monitor its behaviors to declare it as trusted or malicious. If a previous transaction record is present, then trust evaluation can be expressed as

$$TL^{New}_{D_{id}} = \alpha \times TL^{Current}_{D_{id}} + \beta \times \sum_{i=1}^{n} \frac{TL^{CD_i^{TT}}_{D_{id}}}{N} + \gamma \times \sum_{i=1}^{n} \frac{TL^{F_i^{TT}}_{D_{id}}}{N} \quad (1.3)$$

E. REPUTATION EVALUATION PROTOCOL

We extend our previously proposed [47] reputation algorithm by taking into account the context of the users/devices and Fog nodes. This reputation approach is used to build a multi-source based evaluation system with the help of neighboring devices/users and Fog nodes which are trustworthy and reputed to help to evaluate the trustworthiness of a connecting device. Our modified Page Rank based reputation evaluation protocol can be defined as:

$$RV^{CTX}_{D_{id}} = \sum_{v \in B_{D_{id}}} \frac{RP(v)}{L(v)} \quad (1.4)$$

The reputation of a device/user $RV^{CTX}_{D_{id}}$ is reliant on the RP value of a node v enclosed in the set $B_{D_{id}}$, where $B_{D_{id}}$ contains the $RV^{CTX}_{D_{id}}$ from all reputed nodes linking to node D_{id}, where $L(v)$ are the aggregated number of links from $B_{D_{id}}$. The Pseudo 1 shows the overall working of our proposed reputation evaluation approach, where the reputation value range between 0-3. Table 2 shows reputation values and their

TABLE 2. Reputation values and their description.

Value	Description
$0-1$	low Reputed.
$1-2$	Moderate Reputation.
$2-3$	Highly Reputed.

corresponding meanings. A value between 0-1 reflects a low reputed node, a value range between 1-2 reflects a moderate reputation and a value range between 2-3 reflects a highly reputed node.

Algorithm 1 Context-Aware Reputation Evaluation Pseudo

```
Result: Reputation Score
Input: $D_{id}$ for $\forall$ $RV_{D^{CD}_{id}}$ AND $RV^{F_i}_{D_{id}}$ do
    Compute $RV_{D_{id}}$ by Eq. (1.4)
    if $RV_{D_{id}} \geq Range$ AND $RV^{CTX}_{D_{id}} = D^{CTX}_{id}$ then
        return $RV^{CTX}_{D_{id}}$
    else
        return 0
    end
end
```

F. CONTEXT EVALUATION

An important ingredient of our work is the evaluation of a node's context. As discussed earlier each node in the network servers a specific purpose. Take the previous example of a video surveillance node whose sole purpose is to take video feeds where its context is $D^{CTX}_{id} = VideoRecording$. If a connecting device is not found in the trust database the system will evaluate its trust level as discussed in section III-D and put it in $MonitorMode$. Further, the current fog node will perform a content-based trust evaluation to check its CTX and set the D^{CTX}_{id} to its resolved context. If a connecting device/user is found in the trust database the system will compute the context relevance and send gain/loss in trust as discussed in section III-C.

1) CONTEXT-AWARE FEEDBACK (GAIN/LOSS)

After evaluating the trust of a device/user F_i releases the $TL_{D^{CTX}_{id}}$ to reputed devices/Fog nodes that had collaborated in its trust evaluation. It can assist other Fog nodes for the $TE_{D^{CTX}_{id}}$ of the device in the future.

$$FB^{F_i}_{D_{id}} = TL^{New}_{D_{id}} - TL^{Current}_{D_{id}} - 1 \geq FB_{D_{id}} \leq 1 \quad (1.5)$$

A positive value indicates a gain in trust level, whereas negative value reflects trust lost. The context-aware feedback system can help to keep the TE process unbiased and reliable. Cloud can also provide $FB^{C_i}_{D_{id}}$ back to the Fog node using our purposed Content-based approach. Which can be a gain or loss in the trust level of a device/user based on its content worth. It is like a reward/punishment system to help to keep the system unbiased and assist the system to find malicious or untrustworthy devices that contribute data vise irrelevant/malicious data to the system.

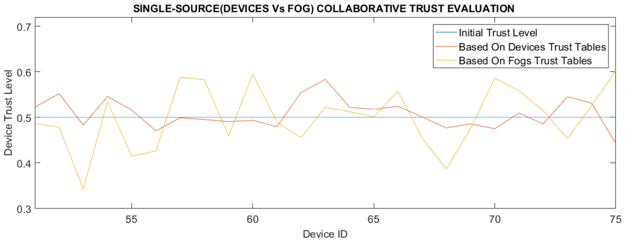

FIGURE 7. A comparing between users/devices and Fog nodes based trust evaluation.

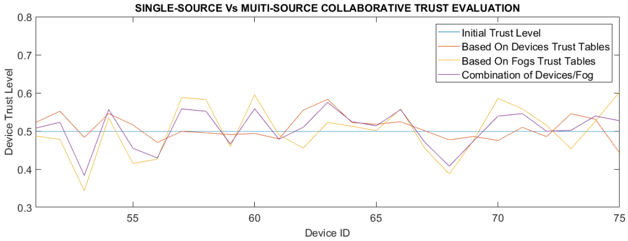

FIGURE 8. A comparing between single-source and multi-source based trust evaluation approach.

2) CONTEXT-AWARE FEEDBACK CRAWLER

The context-aware feedback crawler helps to generate a trust table after a specific period of time. It is an extensive trust evaluation, in which F_i re-evaluate the $TL_{D_{id}}$ of particular devices based on their context, behavior and $TrsutLevel$. This approach can help to sync Fog nodes about the trustworthiness of users/devices based on their interactions. Trust Feedback Crawler can be expressed as:

$$FBC^{F_i} = TT_t \quad (1.6)$$

where t is a specific time period and F_i is current Fog node.

3) MONITOR MODE

IF $TL_{D_{id}} < TrustLimit$ then system set $ModitorMode = 1$ and put the user in $FBC^{List}_{D_{id}}$. By setting $ModitorMode$ the Fog nodes can act maliciously with such users. This approach help secure the system and can help monitor such users for an unusual behavior.

$$MM_{D_{id}} = \begin{cases} 1 & \text{if } TL_{D_{id}} \leq TrustLimit \\ 0 & \text{otherwise} \end{cases} \quad (1.7)$$

IV. SIMULATION AND RESULTS

We performed extensive simulations to see the effectiveness of our system. In this section, we discuss why our approach is better. We also discuss the effect of the weight factors in our purposed model and show the significance of monitor mode. For better understanding, we divide this section into two subsections. Section IV-A introduces simulation setups and section IV-B discusses the results of our simulations and shows why our approach is better.

A. SIMULATION SETUP

Table 3 shows the simulation setup parameters. We set up three different simulation setups to show the effectiveness of

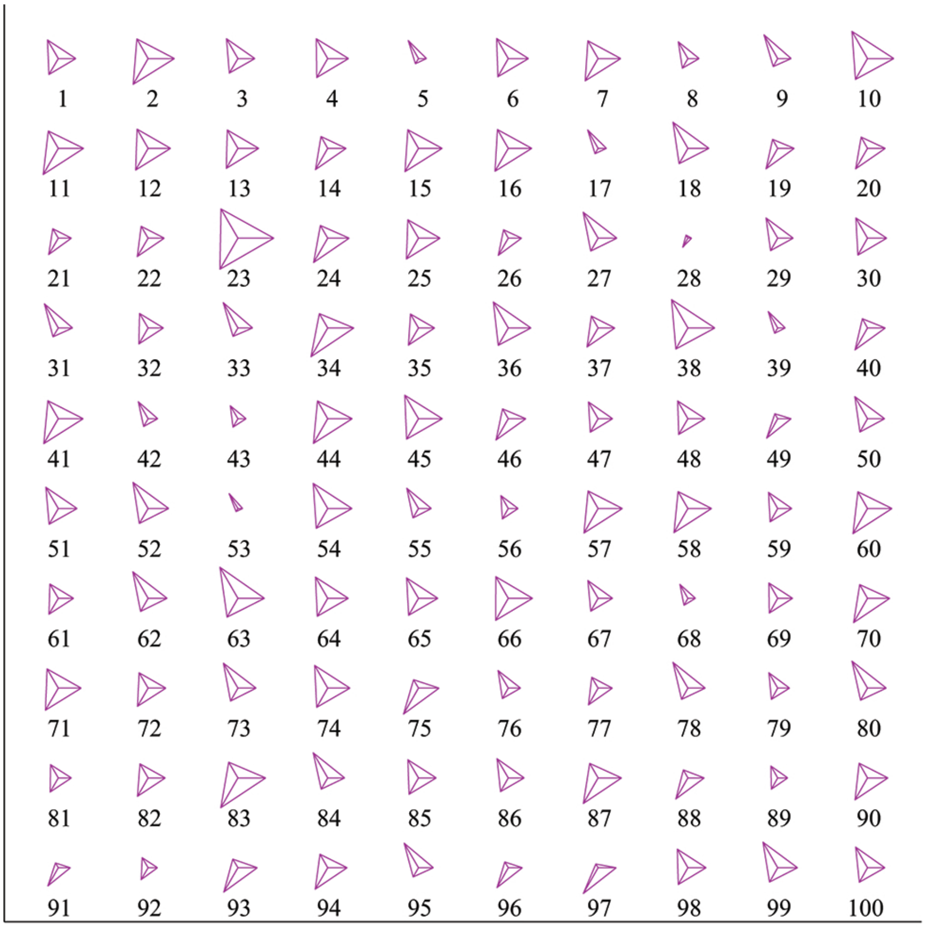

FIGURE 9. Comparative analysis of multi-source vs single source trust evaluation with each user.

TABLE 3. Simulation setups.

Parameter	Setup 1	Setup 2	Setup 3
α	0.7	0.7	0.7
β	0.6	0.5	0.5
γ	0.5	0.6	0.5
$TrustLimit$	0.5	0.5	0.45

our approach. Each setup contains 10 Fog nodes *TT*, where each *TT* contains *TrustLevels* of 100 users. We assign to every new user an initial trust value as described in our section III. In each setup, we use different weight factors and *TrustLimits* to show the effectiveness and flexibility of our system. The weight factors α, β and γ are used to prioritize current node, devices/users nodes, and neighboring Fog nodes, accordingly. We varied these control variables to show the effeteness and versatility of the proposed approach. In setup 1, the α value is set to 0.7, the value for β is set to 0.6, the value for γ is set to 0.5, and the baseline value of trust *TrustLimit* is set to 0.5. In setup 2, we keep the weight factor α and *TrustLimit* same as are and change $\beta = 0.6$, $\gamma = 0.5$ to check the weight effect on our system. In setup 3, we set $\alpha = 0.7$, $\beta = 0.5$, $\gamma = 0.5$ and *TrustLimit* $= 0.45$ to check its effect on our proposed approach.

B. RESULTS

In this section, we discuss why and how our approach is effective and can help in identifying malicious/untrustworthy users in FIoT. First, we discuss why our multi-source approach is better than single-source trust evaluation. Then we discuss the weighted mean approach and show how it affects the system. Finally, we conclude this section by showing the significance of monitor mode.

1) EFFECTIVENESS OF MULTI-SOURCE TRUST EVALUATION APPROACH

we ran a number of simulations to show that a single source could not be fully trusted. As shown in figure 7 by collaborating with single-source whether these are users or Fog nodes, a single source evaluates the trust value of a user either very height or very low. Furthermore, as we mentioned earlier, a single source cannot be entirely trustworthy. After evaluating the trust level with a single-source approach, we evaluate the system with the multi-source approach by using the same parameters as in single-source trust evaluation. As figure 8

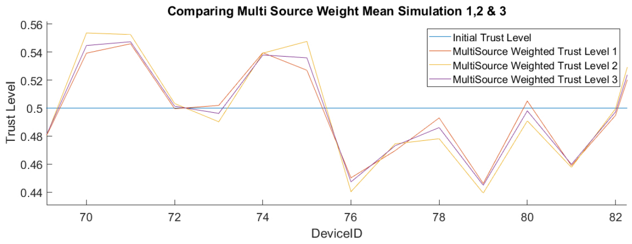

FIGURE 10. Effect of weight factors on simulation setup 1, 2 and 3.

and figure 9 shows, with the multi-source approach the system assigns a weighted sum based trust value which is more effective, unbiased and reliable. One can clearly see that the proposed multi-source technique provides better results as compared to a single source trust evaluation approach.

2) EFFECT OF THE WEIGHT FACTORS

In this section, we discuss the effectiveness of the weight factors in trust evaluation. To verify the effect of using different weight factors for different sources, we compare our simulation setups. Figure 10 shows the comparison among simulation setup 1, 2 and 3. We use the same value of α for each setup. We can see that when the weight is $\beta > \gamma$, the system gives a relatively very high or very low level of trust as compared to the $\beta < \gamma$. When we use the same weight factors for the condition of β and γ, it gives more reliable and effective results. We can see that a change in weight factors clearly affect the system. With our purposed approach, trust evaluation can be tuned to achieve the required level of security. The proper utilization of weight factors can help in prioritizing the source and making the system reliable, effective and unbiased.

3) SIGNIFICANCE OF MONITOR MODE

In simulation setup 1 our purposed approach successfully identifies 48% devices below the *TrustLimit* and 52% as trusted. Malicious devices are handled by monitor mode where the system can monitor their activities. Figure 11 Shows the comparison of how a change in the weight factors and trust limit affect the system. We clearly observe by tuning these factors, we can achieve better security. The proposed monitor mode system can act maliciously with users who are below the trust limit. Further, in the proposed context-aware feedback and feedback crawler system, the malicious users can be synced among all the Fog nodes, which can assist them to identify and monitor such malicious users.

C. DISCUSSION

The broader impact of our work is to show that multi-source trust evaluation can significantly improve trust evaluation. Further, we discuss the importance of context that could be incorporated and could provide vital insights. This work is the first step in this direction and results encourage future research on it. The work can be improved in several different ways. In this work, we use the user's trust tables based on their

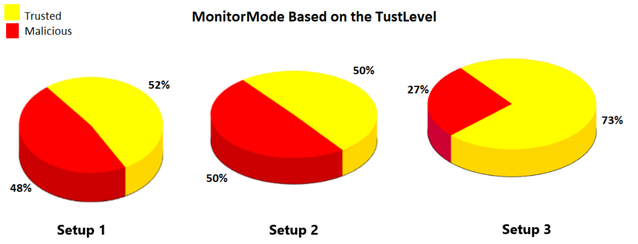

FIGURE 11. Comparison of weight factors on simulation setup 1, 2 and 3.

historical experiences with other users/devices. Although it helps to incorporate the user-to-user (indirect trust) relationships still a user could provide malicious trust values for other users to help them attain a good reputation. In the future, we consider exploiting the possibility of machine learning approaches to learn deeper user-to-user relationships. Machine learning can help capture malicious users by taking into account various factors automatically that could easily be neglected by human-directed models.

V. CONCLUSION

In this work, we proposed a context-based trust and reputation model for Fog-based IoT to identify malicious nodes. Our proposed approach incorporates the context of a connecting device/user for the trust evaluation. Furthermore, we proposed a context-based reputation model that considers the reputed nodes for the trust evaluation related to the context of the connecting node. This work further proposed Trust Feedback and Trust Feedback Crawler system to ensure the trust evaluation system unbiased and effective. The monitor mode has also been proposed to monitor the malicious nodes. In the future, we intend to provide an end-to-end solution for a service model that could be integrated into the Fog based IoT networks. Fog-based IoT is at its early stage and there are a lot of aspects that need attention.

REFERENCES

[1] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT middleware: A survey on issues and enabling technologies," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 1–20, Feb. 2017.

[2] H. Kim and E. A. Lee, "Authentication and authorization for the Internet of Things," *IT Prof.*, vol. 19, no. 5, pp. 27–33, 2017.

[3] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[4] 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.

[5] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA J. Autom. Sinica*, vol. 4, no. 1, pp. 27–40, Jan. 2017.

[6] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, and M. Guizani, "Internet of Things architecture: Recent advances, taxonomy, requirements, and open challenges," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 10–16, Jun. 2017.

[7] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-the-art and research challenges," *J. Internet Servey Appl.*, vol. 1, no. 1, pp. 7–18, May 2010.

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

[9] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.* Cham, Switzerland: Springer, 2015, pp. 685–695.

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

[11] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput.*, 2012, pp. 13–16.

[12] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 854–864, Dec. 2016.

[13] F. Jalali, S. Khodadustan, C. Gray, K. Hinton, and F. Suits, "Greening IoT with Fog: A survey," in *Proc. IEEE Int. Conf. Edge Comput. (EDGE)*, Jun. 2017, pp. 25–31.

[14] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in Fog computing: A survey," *Future Gener. Comput. Syst.*, vol. 88, pp. 16–27, Nov. 2018.

[15] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, Mar. 2012.

[16] T. Dillon, C. Wu, and E. Chang, "Cloud computing: Issues and challenges," in *Proc. 24th IEEE Int. Conf. Adv. Inf. Netw. Appl.*, Apr. 2010, pp. 27–33.

[17] L. J. Hoffman, K. Lawson-Jenkins, and J. Blum, "Trust beyond security: An expanded trust model," *Commun. ACM*, vol. 49, no. 7, pp. 94–101, Jul. 2006.

[18] L. Guo, C. Zhang, and Y. Fang, "A trust-based privacy-preserving friend recommendation scheme for online social networks," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 4, pp. 413–427, Jul. 2015.

[19] A. El Husseini, A. M'Hamed, B. El Hassan, and M. Mokhtari, "Trust-based authentication scheme with user rating for low-resource devices in smart environments," *Pers. Ubiquit. Comput.*, vol. 17, no. 5, pp. 1013–1023, Jun. 2013.

[20] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.*, vol. 43, no. 2, pp. 618–644, Mar. 2007.

[21] 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.

[22] 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.

[23] H. Al-Hamadi and I. R. Chen, "Trust-based decision making for health IoT systems," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1408–1419, Oct. 2017.

[24] K. Kang, Z. Pang, L. Da 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.

[25] E. G. Abdallah, M. Zulkernine, Y. X. Gu, and C. Liem, "TRUST-CAP: A trust model for cloud-based applications," in *Proc. IEEE 41st Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2017, pp. 584–589.

[26] G. Lin, D. Wang, Y. Bie, and M. Lei, "MTBAC: A mutual trust based access control model in Cloud computing," *China Commun.*, vol. 11, no. 4, pp. 154–162, Apr. 2014.

[27] V. Sharma, I. You, D. N. K. Jayakody, and M. Atiquzzaman, "Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things," *Future Gener. Comput. Syst.*, vol. 92, pp. 758–776, Mar. 2019.

[28] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A comprehensive study on the trust management techniques in the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9326–9337, Dec. 2019.

[29] M. Rashmi and C. V. Raj, "A review on trust models of social Internet of Things," in *Emerg. Res. Electron., Comput. Sci. Technol.* Cham, Switzerland: Springer, 2019, pp. 203–209.

[30] L. Fotia, F. Messina, D. Rosaci, and G. M. L. Sarné, "Using local trust for forming cohesive social structures in virtual communities," *Comput. J.*, vol. 60, no. 11, pp. 1717–1727, Nov. 2017.

[31] L. N. Zlatolas, T. Welzer, M. Hölbl, M. Heričko, and A. Kamišalić, "A model of perception of privacy, trust, and self-disclosure on online social networks," *Entropy*, vol. 21, no. 8, p. 772, Aug. 2019.

[32] S. Liu, L. Zhang, and Z. Yan, "Predict pairwise trust based on machine learning in online social networks: A survey," *IEEE Access*, vol. 6, pp. 51297–51318, 2018.

[33] X. Chen, Y. Yuan, L. Lu, and J. Yang, "A multidimensional trust evaluation framework for online social networks based on machine learning," *IEEE Access*, vol. 7, pp. 175499–175513, 2019.

[34] P. D. Meo, "Trust prediction via matrix factorisation," *ACM Trans. Internet Technol.*, vol. 19, no. 4, pp. 1–20, Nov. 2019.

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

[36] M. Debe, K. Salah, M. H. U. Rehman, and D. Svetinovic, "IoT public fog nodes reputation system: A decentralized solution using ethereum blockchain," *IEEE Access*, vol. 7, pp. 178082–178093, 2019.

[37] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarne, "Using blockchain in a reputation-based model for grouping agents in the Internet of Things," *IEEE Trans. Eng. Manage.*, to be published.

[38] G. Fortino, F. Messina, D. Rosaci, and G. L. Sarné, "Using trust and local reputation for group formation in the Cloud of Things," *Future Gener. Comput. Syst.*, vol. 89, pp. 804–815, Dec. 2018.

[39] P. Zhang, Y. Kong, and M. Zhou, "A domain partition-based trust model for unreliable clouds," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2167–2178, Sep. 2018.

[40] Y. Wu, C. Yan, Z. Ding, G. Liu, P. Wang, C. Jiang, and M. Zhou, "A novel method for calculating service reputation," *IEEE Trans. Autom. Sci. Eng.*, vol. 10, no. 3, pp. 634–642, Jul. 2013.

[41] M. H. Ghahramani, M. Zhou, and C. T. Hon, "Toward cloud computing QoS architecture: Analysis of cloud systems and cloud services," *IEEE/CAA J. Autom. Sinica*, vol. 4, no. 1, pp. 6–18, Jan. 2017.

[42] P. Manuel, "A trust model of cloud computing based on Quality of Service," *Ann. Oper. Res.*, vol. 233, no. 1, pp. 281–292, Oct. 2015.

[43] M. Alhamad, T. Dillon, and E. Chang, "SLA-based trust model for cloud computing," in *Proc. 13th Int. Conf. Netw.-Based Inf. Syst.*, Sep. 2010, pp. 321–324.

[44] S. S. Kirkman and R. Newman, "Bridging the cloud trust gap: Using ORCON policy to manage consumer trust between different clouds," in *Proc. IEEE Int. Conf. Edge Comput. (EDGE)*, Jun. 2017, pp. 82–89.

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

[46] D. H. McKnight and N. L. Chervany, "The meanings of trust," Univ. Minnesota, Minneapolis, MN, USA, Tech. Rep. MISRC Work. Paper Ser. 96-04, 1996.

[47] Y. Hussain and Z. Huang, "Trfiot: Trust and reputation model for fog-based IoT," in *Proc. Int. Conf. Cloud Comput. Secur.* Cham, Switzerland: Springer, 2018, pp. 187–198.

[48] H. Wang, Z. Wang, and J. Domingo-Ferrer, "Anonymous and secure aggregation scheme in fog-based public cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 712–719, Jan. 2018.

[49] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in Internet of Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1143–1155, Oct. 2017.

[50] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, and J. Shen, "Secure intelligent traffic light control using fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 817–824, Jan. 2018.

[51] M. H. Ibrahim, "Octopus: An edge-fog mutual authentication scheme," *Int. J. Netw. Secur.*, vol. 18, no. 6, pp. 1089–1101, Nov. 2016.

YASIR HUSSAIN received the B.Sc. degree from Bahauddin Zakariya University (BZU), Pakistan, in 2013, and the master's degree in computer science from the Virtual University of Pakistan, in 2015. He is currently pursuing the Ph.D. degree in computer science with the Nanjing University of Aeronautics and Astronautics, Nanjing, China. He is particularly interested in cloud computing, fog computing, machine learning, deep learning, recommender systems, and predictive modeling.

HUANG ZHIQIU received the B.Sc. and M.Sc. degrees in computer science from the National University of Defense Technology of China, and the Ph.D. degree in computer science from the Nanjing University of Aeronautics and Astronautics, China. He is currently a Full Professor with the Nanjing University of Aeronautics and Astronautics. His research interests include big data analysis, cloud computing, and web services.

MUHAMMAD AZEEM AKBAR received the M.Sc. and M.S. degrees in computer science from the University of Agriculture Faisalabad (UAF), Faisalabad, Pakistan, and the Ph.D. degree in software engineering from Chongqing University, China. He is currently working as a Researcher with the Nanjing University of Aeronautics and Astronautics, Nanjing, China. He published more than 25 research articles in well-reputed journals and conferences. He has an Outstanding Academic Carrier. His research interests are global software development, requirements engineering, empirical studies, global software requirements change management, software defect prediction, the Internet of Things, code recommender systems, and software risk management.

AHMED ALSANAD received the Ph.D. degree in computer science from De Montfort University, U.K., in 2013. He is currently an Associate Professor with the Information System Department and a Chair Member of pervasive and mobile computing with CCIS, King Saud University, Riyadh, Saudi Arabia. He has authored and coauthored more than 12 publications including refereed IEEE/ACM/Springer journals, conference articles, and book chapters. His research interests include cloud computing, health informatics, ERP, and CRM.

ABEER ABDUL-AZIZ ALSANAD received the bachelor's degree in computer science from Prince Sultan University, the master's degree in information systems from King Saud University, and the Ph.D. degree in information systems with the College of Computer and Information Science, King Saud University. She is currently an Assistant Professor with the Information Systems Department, College of Computer and Information Sciences, Imam Muhammad Ibn-Saud Islamic University. She has published several conference and journal articles. Her major interests include software engineering, requirement engineering, and change management.

ASIF NAWAZ received the M.S. degree in software engineering from the National University of Sciences and Technology, Islamabad, Pakistan, in 2010. He is currently pursuing the Ph.D. degree from the Nanjing University of Aeronautics and Astronautics, Nanjing, China. His main interests include software engineering, machine learning, geographical information systems, data analysis, and decision support systems.

IZHAR AHMED KHAN received the B.Sc. degree from the University of Engineering and Technology, Pakistan, in 2008, and the master's degree in computer science from Mid Sweden University, Sweden, in 2011. He is currently pursuing the Ph.D. degree in computer science with the Nanjing University of Aeronautics and Astronautics, Nanjing, China. His current research interests include machine learning, data mining, and anomaly detection systems.

ZAHEER ULLAH KHAN received the master's degree in computer science from the University of Peshawar, Pakistan, and the M.S. degree from the Abdul Wali Khan University Mardan, Pakistan. He is currently pursuing the Ph.D. degree with the Nanjing University of Aeronautics and Astronautics, China. He has published many researcher articles in image processing and bioinformatics. His research interest includes predictive models for RNA/DNA sequences and generative models.