Trustee: A Trust Management System for Fog-enabled Cyber Physical Systems

Aisha Kanwal Junejo, Nikos Komninos, *Member, IEEE*, Mithileysh Sathiyanarayanan, and Bhawani Shankar Chowdhry, *Senior Member, IEEE*

Abstract—

In this paper, we propose a lightweight trust management system (TMS) for fog-enabled cyber physical systems (Fog-CPS). Trust computation is based on multi-factor and multi-dimensional parameters, and formulated as a statistical regression problem which is solved by employing random forest regression model. Additionally, as the Fog-CPS systems could be deployed in open and unprotected environments, the CPS devices and fog nodes are vulnerable to numerous attacks namely, collusion, self-promotion, bad-mouthing, ballot-stuffing, and opportunistic service. The compromised entities can impact the accuracy of trust computation model by increasing/decreasing the trust of other nodes. These challenges are addressed by designing a generic trust credibility model which can countermeasures the compromise of both CPS devices and fog nodes. The credibility of each newly computed trust value is evaluated and subsequently adjusted by correlating it with a standard deviation threshold. The standard deviation is quantified by computing the trust in two configurations of hostile environments and subsequently comparing it with the trust value in a legitimate/normal environment. Our results demonstrate that credibility model successfully countermeasures the malicious behaviour of all Fog-CPS entities i.e. CPS devices and fog nodes. The multi-factor trust assessment and credibility evaluation enable accurate and precise trust computation and guarantee a dependable Fog-CPS system.

Index Terms—Cyber Physical Systems, Fog Computing, Trust Computation, Trust Credibility

1 Introduction

As an emerging paradigm, fog-enabled cyber physical systems (Fog-CPS) combine computation and communication capabilities with the physical space [1]. Fog computing encourages local data processing and ”edge analytics”. Low latency, location-awareness, local resource pooling, decentralization, and geographic distribution are some of the distinguished features of fog computing. Despite the opportunities provided by the Fog-CPS, they face increased security and trust challenges. Recent cyber attacks on cyber physical systems including Ukrainian power grid [2], DNS provider Dyn and others underline the threat of connectivity and vulnerability of resource constrained devices to be compromised.

Identity and access management can prevent fake entities from joining a Fog-CPS system. However, it is difficult to guarantee that entities have not been compromised. In Fog-CPS systems, the CPS devices can provision low-latency services from fog nodes in vicinity. Nevertheless, some fog nodes may not maintain good quality of service (QoS) due to various factors such as, service cost, energy usage, application characteristics, data flow, network status, and malicious behaviour of other entities. Without trust mechanisms, such interactions are subject to risk and uncertainty that an entity might experience. Considering the above-mentioned challenges, it is essential that each entity in Fog-CPS must have a certain level of trust on one another. Trust can be established by monitoring the interactions of Fog-CPS entities. Precisely, the trustworthiness of an entity can be assessed on various dimensions such as service quality, competence, integrity, benevolence, honesty [3] and capability [4].

1.1 Motivation

To the best of our knowledge, there is no trust model which considers a hostile environment in Fog-CPS systems. As the Fog-CPS shares many commonalities with cloud computing [5]–[9], Internet of Things (IoT) [10] [11], wireless sensor networks (WSN) [12], and mobile adhoc networks (MANETs) [13]–[15] , the models proposed for these systems are somehow relevant, but they cannot be directly applied to fog scenarios due to the decentralized and distributed architecture. Most of the existing studies on IoT, MANETs, and CPS only assess the trustworthiness of sensor nodes and CPS devices. However, due to the fog nodes operation in open and unprotected environments, they are also vulnerable to cyber attacks and can be compromised. It is therefore essential to assess the trustworthiness of all Fog-CPS entities. Trustworthiness can be assessed based on several parameters such as quality of service (QoS), capability and communication features etc.

It is underlined that similar to other distributed systems namely P2P, MANETs, and sensor clouds, the Fog-CPS are also vulnerable to self-promotion, bad-mouthing, opportunistic service, on-off, collusion, Sybil, and ballot-stuffing

- *A. K. Junejo, N. Komninos, and Mithileysh Sathiyanarayanan are with the Department of Computer Science, School of Mathematics, Computer Science, and Engineering, City University of London, EC1V 0HB, London, UK.*
  E-mail: aisha.junejo@city.ac.uk, nikos.komninos.1@city.ac.uk, mithileysh.sathiyanarayanan@city.ac.uk
- *B. S. Chowdhry is with the Faculty of Electrical, Electronics and Computer Engineering, Mehran University of Engineering and Technology, Jamshoro 76062, Pakistan. E-mail: bhawani.chowdhry@faculty.muet.edu.pk.*

Manuscript received Nov, 2018.

attacks [16]. These attacks aim to degrade the accuracy of trust computation model or impact the availability of TMS itself. For instance, in self-promotion attack, attackers attempt to increase their own trust by reporting false parameters. Bad-mouthing attack occurs when a node gives bad recommendations about other nodes. In the case of Fog-CPS, malicious CPS devices can send false parameter reports regarding their experience with fog nodes to purposefully decrease their trust.

Additionally, fog nodes can be opportunistic at times meaning that they will provide good service only for their own benefit. Similar to opportunistic service, in on-off attacks, malicious entities can behave good and bad depending upon the situation. Likewise, in collusion attacks, several compromised CPS devices can collaborate to modify the trust results of other entities. In Sybil attack, a malicious node (i.e. CPS devices in Fog-CPS) can create several fake IDs to report false values of trust parameters. Moreover, in Fog-CPS, ballot stuffing attack occurs when a CPS device submits more parameter reports than permitted in a given time period. These attacks can result into imprecise trust computation which does not reflect the true actions and/or performance of Fog-CPS entities. It is therefore essential to devise countermeasures against these attacks such that the trust cannot be maliciously manipulated.

Considering the limitations of existing approaches, in this paper, we propose a trust management system (TMS) which handles trust computation, management and dissemination. Our proposed trust computation model includes several components for trust computation and credibility evaluation of fog nodes and CPS devices. A major advantage of the credibility evaluation is the prevention of Sybil, collusion, and data anomalies attacks.

1.2 Contributions

The contributions of this paper are four-fold. First, a holistic TMS which provides a trust computation and dissemination platform is proposed. Second, trust computation is formulated as a statistical regression problem and random forest regression is employed to solve it. Third, for trust computation a hostile environment in Fog-CPS systems is considered. Additionally, a generic trust credibility evaluation model is proposed to countermeasure the malicious behaviour of compromised entities. The credibility of each newly computed trust value is evaluated and subsequently adjusted by correlating it with a standard deviation threshold. Fourth, the proposed TMS provides a trust distribution framework to disseminate the trust scores. Any entity which is part of the Fog-CPS network can query the trust scores of other entities before making a decision to collaborate.

The rest of this paper is organized as follows. The related work is presented in section 2. The architecture of a Fog-CPS systems is discussed in section 3. Our proposed TMS is elaborated in section 4. The experimental results of proposed trust management system are presented in section 5. The conclusion and future work are discussed in section 6.

2 Related Work

As fog computing is a new area of research so there are not many trust models. However, as it shares many commonalities with cloud computing, WSN, IoT, and MANET, the trust models proposed for these systems are considered.

1. Cloud Computing: Majority of the studies compute trust based on objective trust but some adopt a hybrid approach [6]–[9] where trust is the fusion of objective and subjective evidence. The literature identifies two popular methods to compute objective trust, a) subjective logic [17], and b) real-time adaptive trust evaluation approach [5] [8]. In adaptive trust evaluation approaches, the trust computation problem is modeled as a process of multi-attribute decision making (MADM) and weights are assigned adaptively either by information entropy [5] or maximizing deviation method [8]; whereas in subjective logic weights are assigned manually or subjectively [17].

Nagarajan et. al [9] employ a hybrid trust model which is based on subjective logic to combine 'hard' trust from measurements and properties and 'soft' trust from past experiences and recommendations to reduce uncertainties. Gosh et. al [7] propose a framework which combines trustworthiness and competence to estimate the risk of interaction. Li et. al [18] propose a trust model for web services which considers the users' preferences and the impact of vicious ratings on trust evaluation. The proposed model is based on subjective logic and does not consider the real-time QoS attributes which make it impractical for Fog-CPS. Recently, Talal et.al [19] propose a reputation based trust management approach to compute subjective trust of cloud services.

2. IoT: Namal et. al [10] propose a TMS for cloud-based IoT applications which employs "Weighted Sum" for trust aggregation and considers multi-dimensional parameters namely, availability, reliability, capability, and response time for trust formation. However, a major limitation of this work is the inconsideration of security protection against attacks [20]. Nitti et. al [11] propose a trustworthiness management system for social IoT. The trust of a service provider is computed by centrality, objective, and subjective trust. Tian et. al [21] proposed a trust evaluation approach for sensor-cloud systems in which trust is formulated as a multiple linear regression (MLR) problem. Average energy consumption, response time, and package delivery ratio are considered as features in MLR. Recently, Tian et. al [22] propose a novel energy-efficient and trustworthy protocol based on mobile fog computing to evaluate the trustworthiness of sensors.

3. MANETs: Wang et. al [13] proposed a logistic regression based trust Model for MANETs. The two classes of logistic regression classifier are trustworthy (0) and untrustworthy (1). The probability of trust being in one class or another is considered as the probabilistic statistical estimation of trust. Shabut et. al [14] proposed a recommendation based trust model for MANETs. The proposed model includes a defence scheme which utilises clustering technique to dynamically filter out attacks related to dishonest recommendations during a time period based on the number of interactions, compatibility of information, and closeness between the nodes. Li et. al [12] proposed a trust management scheme for vehicular ad hoc networks (VANETs). Dempster–Shafer theory and collaborative filtering techniques are used for trust aggregation. Trustworthiness of vehicles in VANETs is evaluated by data and node trust. Recently, Xia et. al [15] proposed a trust model based on Grey-Markov chain

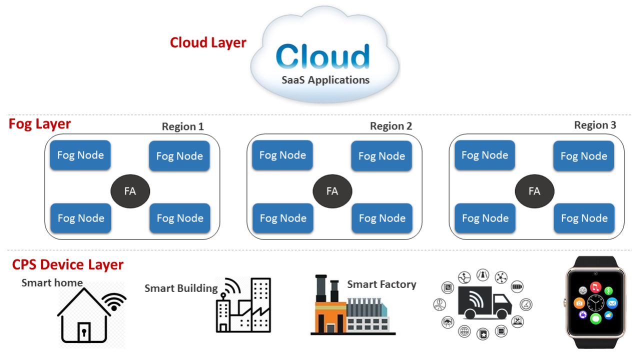


Fig. 1: Fog-enabled Cyber Physical Systems

prediction technique to predict trust of nodes in MANET. The process of node trust assessment is based on node's historical behaviours, in which the trust decision factors include the subjective reputation and indirect reputation.

4. Cyber Physical Systems: Interestingly, for CPS, many different approaches namely trusted computing, game theory, and generic probabilistic graph modelling have been proposed.

Rein et. al [23] proposed the concept of trust establishment in a cooperative cyber physical system. The proposed model employs trusted computing and trusted event reporting to verify the authenticity of security related events in critical infrastructures. Pawlick et. al [24] adopt a game theoretical approach for trust computation in CPS. The game captures the strategical and adversarial aspects of CPS security. Yan et. al [25] adopted a perception-oriented approach to quantify trustworthiness in cyber physical systems. A multi-dimensional perception approach based on three major metrics of ability, benevolence, and integrity is considered.

Discussion: After reviewing the literature, we conclude that the trust computation is essentially a regression problem wherein the trust of an entity can be accurately predicted based on a set of features. For instance, the trust of a fog node can be estimated based on its computational and processing capabilities, response time, and task success ratio. Likewise, the trust of a CPS device can be based on the its performance and communication features. Regression analysis based schemes perform better than other trust computation models (for cloud) namely subjective logic, weighted sum, and adaptive trust evaluation, as they regress over all records and assign the weights that best fit the input features. Trust models proposed for cloud computing do not consider a hostile environment wherein service providers can be compromised. Considering the advantages of regression, in this paper random forest regression is employed for trust computation of fog nodes and CPS devices. Some works also proposed the trusted computing technology for trust assessment in CPS devices. However, trusted computing is equipped with several cryptographic constructions namely, random number generation, remote attestation, binding, and sealing. Such computationally expensive operations are not appropriate for resource limited CPS devices and IoT sensors.

TABLE 1: Notations and their Meanings

Notation	Description
FA	Fog Assist Node
CPS	Cyber Physical Device
$\Delta\lambda$	time window for trust evaluation
t	time stamp for QoS evidence gathering
$\sigma_t(f_i)$	instant trust of ith fog node at time t
$T_{fa \rightarrow fog}$	Fog node objective trust computed by FA
$T_{cps \rightarrow fog}$	Fog node trust based on CPS device experience
T_{fog}	Fog node trust
$T_{cps \rightarrow fog}$	CPS device trust based on fog node experience
$c(i, f_j)$	parameter report sent by ith CPS device for jth fog node
σ	Standard Deviation of Trust T over a time window $\Delta\lambda$

3 Fog-CPS Architecture

Fig. 1 illustrates the architecture of our proposed TMS. It is based on the three-layer architecture proposed by Open Fog Consortium and other studies [26]–[29]. A Fog-CPS consists of three layers namely, *CPS devices*, *fog* and *cloud*. These layers are arranged in an increasing order of computing and storage capabilities. The *CPS devices* layer has two types of devices, mobile CPS devices and fixed CPS devices. The *fog* layer consists of network equipment, such as routers, bridges, gateways, switches and base stations, augmented with computational capability, and local servers. The *fog* layer has two types of entities namely fog nodes and ”Fog Assist” (FA) nodes.

The FA nodes are dedicated for entity registration, service orchestration, provisioning, and trust management. It is assumed that FA is protected by security measures namely, encryption, authentication and access control, firewalls and intrusion detection systems. A few recent studies [28] [30] also advocate the need of dedicated nodes for service orchestration and consider them secure even if Fog-CPS system deployment is in an open and hostile environment. As shown in Fig. 1, the fog layer is divided into several geographical regions with each being managed by a FA node. The region-based approach enables the dissemination of trust among Fog-CPS entities in different regions. The *cloud* layer is a consolidated computing and storage platform that provides various applications for the acquisition, processing, presentation and management of the Fog-CPS system.

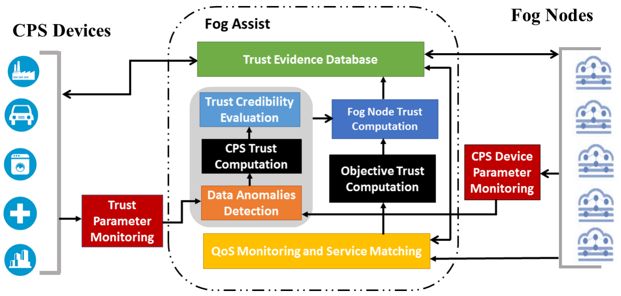

CPS Devices
Fog Assist
Fog Nodes
Trust Evidence Database
Trust Credibility Evaluation
Fog Node Trust Computation
CPS Trust Computation
Objective Trust Computation
Data Anomalies Detection
CPS Device Parameter Monitoring
Trust Parameter Monitoring
QoS Monitoring and Service Matching

Fig. 2: Fog-CPS Trust Management System

4 Proposed Trust Management System

In a trust relationship, the trustor is an entity which shares some of its assets and/properties with another entity

TABLE 2: Fog Node Trust Parameters

Fog Assist	**CPS Device**
FA Trust Parameters	*CPS Trust Parameters*
CPU frequency	Energy Consumption
Memory size	Response Time
Hard disk capacity	Bandwidth
Current CPU utilization rate	
Current memory utilization rate	
Current hard disk utilization rate	
Average response time	
Average task success ratio	

namely trustee for the benefit of a third party. Precisely, in Fog-CPS systems, the fog nodes and CPS devices are the trustor and FA (as it is managing TMS) is the trustee. Moreover, the beneficiary can be the Fog-CPS system users and/or other entities. Next, we present our proposed TMS as shown in fig. 2. It consists of eight modules namely, 1) QoS Monitoring and Service Matching, 2) Objective Trust Computation, 3) Trust Parameter Monitoring, 4) CPS Device Parameter Monitoring, 5) Data Anomalies Detection, 6) CPS Trust Computation, 7) Trust Credibility Evaluation, 8) Fog Node Trust Computation and 9) Trust evidence Database. The different modules of TMS enable FA to accurately and precisely compute the trust of fog nodes and CPS devices respectively. For fog nodes, trust is computed by aggregating the QoS evidence monitored by FA, and the CPS device parameters reflecting their experience with the fog nodes. Likewise, the trust of CPS devices is computed based on communication features monitored by fog nodes. ***Trust Parameter Monitoring*** module is installed in each CPS device and fog node. It quantifies the latency, energy consumption and bandwidth utilized in communication between the fog nodes and CPS devices, and vice versa.

QoS Monitoring and Service Matching module assists FA in evaluating the service quality and finding the services matching the user requirements. The QoS evidence is later fed into the ***Objective Trust Computation*** module in order to compute the objective trust. FA subsequently stores all the monitored parameters and trust results in the ***Trust Evidence Database***.

Moreover, any anomalies in parameters monitored by fog nodes and CPS devices are detected by ***Data Anomalies Detection*** component prior to being incorporated into ***CPS Trust Computation***. Next, the ***Trust Credibility Evaluation*** module finds the discrepancies in trust computed in consecutive time instances. The trust inconsistencies are analyzed to prevent the malicious behaviour of Fog-CPS entities. Lastly, the objective and CPS trust are sent to the ***Fog Node Trust Computation*** module to compute the final trust of fog nodes. The details of each of these modules are given below. Table 1 lists the notations used throughout this paper.

4.1 QoS Monitoring and Service Matching

As the name suggests this module includes features for monitoring the service quality parameters and matching the services as per the given requirements. As discussed in section 4, there are two types of CPS devices namely, fixed and mobile. Generally, the service matching is not required in fog scenarios where fixed CPS devices are deployed. Because the interactions among devices are already established. The entities function as per the requirements of specific application scenario. However to generalize the TMS, a service matching feature is added such that the proposed TMS can also be applied to fog scenarios with mobile CPS devices. For service matching, a set of requirements are taken as input and subsequently the resource matching is carried out on the available fog nodes. FA selects highly trusted fog nodes based on their trust values.

However, for trusted service matching, it is essential to monitor the real-time service parameters of fog nodes. In the interactive process, this module dynamically monitors the service parameters and is responsible for getting run-time service data. The FA monitors four kinds of parameters (see Table 2) namely, fog node specification, average resource usage, average response time, and average task success ratio. The fog node specification profile includes CPU frequency, memory size, and hard disk capacity. The average resource usage information consists of the current CPU utilization rate, current memory utilization rate, current hard disk utilization rate, and current bandwidth utilization rate.

4.2 Objective Trust Computation

The trust of a fog node is computed by aggregating the trust computed from QoS evidence and the experience of CPS devices. The objective trust is computed from directly monitored QoS evidence. Random forest regression [31] is employed to predict the objective trust of a fog node based on the QoS parameters listed in table 2. In prediction problems, the regression models are trained over a substantial number of samples in order to improve the accuracy. So for objective trust computation, the first task was to generate the trust labels corresponding to a set of service parameters. The trust label is assigned based on average task success ratio and service quality. Trust gets a high value if the average task success ratio is high and the fog node fulfilled the service request by maintaining the acceptable service quality vice versa.

Following this, the random forest regression is executed to predict the objective trust at a given time instance based on the service parameter features. As the QoS features are high dimensional (i.e. each sample has multiple features to consider). At each node in a tree, the optimization happens by selecting one feature randomly and optimizing for it. This process is repeated multiple times until the best feature is found and subsequently split at that node. Once this happened, the data is split based on that feature and each split is passed to the two nodes below.

Let $F = \{f_1, f_2, ..., f_n\}$ denote n trusted fog nodes in a Fog-CPS environment. The instant trust degree $\sigma_t(f_i)$ of f_i at time instance t is predicted using random forest regression procedure explained above. The prediction of $\sigma_t(f_i)$ at t is based on the QoS parameters quantified at that time instance. Subsequently, objective trust is calculated using Eq. (1):

$$T_{fa \to fog} = \bar{\sigma} \times s(f_i) = \sum_{t=1}^{\Delta\lambda} (\sigma_t(f_i) \times s_t(f_i)), \qquad (1)$$

where $s(f_i) = \{s_1(f_i), s_2(f_i), ..., s_n(f_i)\}$, and $\sum_{t=1}^{n} s_t(f_i) = 1$. $s_t(f_i) \in [0, 1]$ is the weight assigned to each instant trust degree $\sigma_t(f_i)$ and is given by Eq. (2).

$$s_t(f_i) = \frac{(1 - (t+1)^{-1})}{\sum_{t=1}^{n} (1 - (t+1)^{-1})} \tag{2}$$

s is a time-based attenuation function which assigns more weight to $\sigma_t(f_i)$ computed at recent time instances.

4.3 Trust Parameter Monitoring

A "Trust Parameter Monitoring" module is installed in each CPS device and will enable them to quantify the utilization of energy, bandwidth and response time when communicating with a fog node.

4.4 CPS Device Parameter Monitoring

Similar to CPS devices, the fog nodes also monitor a few parameters for each CPS device which is connected to it. Both fog nodes and CPS devices evaluate each other on same set of parameters. The fog nodes subsequently report them to FA which computes the trust for CPS devices.

4.5 Data Anomalies Detection

After the multi-dimensional parameters (table 2) related to communication features are reported by CPS devices and fog nodes. The data anomalies are identified by comparing the parameter values with the predefined range. If a parameter value falls within the range, then it is considered for trust computation otherwise not.

4.6 CPS Trust Computation

This module computes the trust of CPS devices for fog nodes. The instant degree of trust based on a set of parameters is predicted by the random forest regression model. Precisely, regression evaluates the relationship between parameters and trust. Subsequently, the CPS trust $T_{cps \to fog}$ of a fog node f_j is computed using Eq. (3)

$$T_{cps \to fog} = \frac{\sum_{i=1}^{p} c(i, f_j)}{p} \tag{3}$$

where $c(i, f_j)$ is the trust computed from the ith report sent by the CPS devices provisioning services from a fog node f_j and p is the total number of reports. Additionally, it is noted that similar to fog nodes, the trust of CPS devices $T_{fog \to cps}$ is also computed using Eq. (3).

4.7 Trust Credibility Evaluation

As discussed in section 1.1, the Fog-CPS systems can be deployed in open and unprotected locations and are therefore at the risk of compromise. Moreover, such distributed systems can also be subject to collusion, on-off, bad-mouthing, and self-promotion attacks. Compromised entities might try to change the trust of other nodes by reporting false parameters. For instance, in collusion attacks, the attackers can either work alone or in coalitions to increase/decrease the trust of Fog-CPS entities. Solving this problem is not straightforward because on the one hand, it is not easy to predetermine the number of compromised entities and on the other hand, it is essential to minimize the impact of malicious attackers. Keeping these constraints in mind, a trust credibility evaluation model is designed to adjust the trust of Fog-CPS entities in three cases whereby the CPS devices, fog nodes and FA could be compromised.

Case 1 - Compromise of CPS Devices: Compromised CPS devices may try to change $T_{cps \to fog}$ by reporting false parameters. The proposed credibility model and data anomalies detection modules can handle these discrepancies.

Case 2 – Compromise of Fog Nodes: Compromised fog nodes can report false parameters to change the $T_{fog \to cps}$. Similar to case 1, this problem is redressed by monitoring the rate of change of trust and subsequently adjusting it based on trust computed in previous time instances.

Case 3 – Compromise of FA: As the TMS model is maintained by the FA node so its compromise can lead to following problems:

- *Inaccurate Computation of T_{fog}, $T_{cps \to fog}$ and $T_{fog \to cps}$:* The FA computes the trust of Fog-CPS entities and then store it in the Trust Evidence Database which is publicaly accessible. So, if an entity finds a discrepancy in its trust score, it can request the recomputation of trust based on the current values of parameters. If its request is not entertained then it can inform all involved fog nodes and CPS devices.

- *Tampering the QoS and CPS device Parameters:* A compromised FA node can also change the parameter values reported by the Fog-CPS devices. This can be addressed by the making the "Trust Evidence Database" accessible to the relevant entities. The fog nodes and CPS devices can verify and/or compare their reported set of parameters to those stored in the Database. The discrepancy could be reported back to the FA node and the involved entities. To address all these cases of compromise, trust credibility evaluation is applied in all computations i.e. T_{fog}, $T_{cps \to fog}$ and $T_{fog \to cps}$ by default. Hence, any "large" differences will be adjusted. Precisely, when new CPS devices and fog nodes are taking part in the network their trust value is expected to be 0.5. While the network operates trust values will be increased or decreased. Trust credibility evaluation model analyses the change in T during consecutive time instances $[t_0, t]$ and subsequently recomputes the trust in recent time instance t using Eq. (4):

$$T_t = T_{t_0} \pm \sigma T_t, \tag{4}$$

where σ is the standard deviation in T over a time window $\Delta\lambda$. The standard deviation σ informs about the spread of the possible values of trust. σ is computed by Eq. (5):

$$\sigma = \sqrt{\frac{\sum(T - \mu)^2}{\Delta\lambda}} \tag{5}$$

where μ is mean of trust T at a time instance t. The standard deviation should be taken/considered for every newly calculated trust value. If the trust T in recent time instance t is less than the previous time t_0 and the difference is greater than σ then the T in t is increased otherwise it is decreased.

TABLE 3: Simulation Parameters

Parameters	Values
No: of Fog Nodes	2
No: of CPS devices connected with each fog node	20
No: of FA nodes	1
No: of regions	2
No: of Cloud Providers	1
No: of Simulation Instances	5

4.8 Fog Node Trust Computation

Having discussed objective and CPS trust modules. The next task is to aggregate them to compute trust of a fog node and to assign weights to objective and CPS trust. Through weight assignment, it is easy to define the proportion of CPS and objective trust in computing the trust of a fog node. Fog node trust is calculated as follows:

$$T_{fog} = \delta \times T_{cps \rightarrow fog} + (1 - \delta) \times T_{fa \rightarrow fog} \tag{6}$$

where δ is the weight of $T_{cps \rightarrow fog}$, and, $(1 - \delta)$ is the weight of $T_{fa \rightarrow fog}$. If we set $\delta = 1$, the weight of $T_{fa \rightarrow fog}$ becomes 0, and the equation 6 will only consider CPS trust. However, many studies [32]–[34] show that objective trust $T_{fa \rightarrow fog}$ is a helpful component in building a dependable trust relationship. When the system is highly dynamic and most CPS devices are malicious, the objective trust $T_{fa \rightarrow fog}$ should be set with a high weight. Intuitively, the value of $T_{cps \rightarrow fog}$ calculated above should have a higher weight if the number of rating CPS devices is higher.

4.9 Trust Evidence Database

FA stores the trust values of each fog node and CPS device in the trust evidence database. Any device can look up and/or query FA and acquire the trust scores of other entities and based on which makes a decision to collaborate.

5 Experimental Evaluation

In this section, the results of trust computation are presented.

5.1 Implementation Environment

As discussed in section 4, the Fog-CPS consists of three layers, *CPS devices*, *fog* and *cloud*. Communication between these layers is possible in four different ways, 1) device to device, 2) device to fog node, 3) fog node to fog node, and, 4) fog node to cloud service provider. For evaluating our proposed TMS, we have simulated a generalized Fog-CPS network (see fig. 3) in iFogSim [35]. Moreover, the random forest regression model is trained and tested in Spyder 3.2.6. It is a scientific Python development environment which is packaged in Anaconda. All benchmarks were executed on a Windows machine running Windows 10 with Python 3.6.4. on Intel (R) Core(TM) i5-4310U CPU@2.000GHz with 8.0 GB RAM.

The simulation parameters are listed in table 3. There is one cloud service provider and one FA. Moreover, there is one fog node in each region of *fog* layer. Twenty CPS devices are provisioning services from each of the fog nodes. CPS devices belong to different Fog-CPS application scenarios namely, weather forecasting, health monitoring, energy consumption, and vehicular ad hoc networks (VANETs) etc. The QoS parameters for fog nodes and CPS devices are acquired from iFogSim [35] simulator. For experimental purposes, the simulation model quantifies the multidimensional QoS parameters in following three cases, 1) CPS device to fog node communication, 2) fog node to CPS device communication, and 3) FA monitoring fog nodes. A communication loop is created wherein a CPS device provisions a service (i.e. compute, storage, network, and software) from a fog node and subsequently reports its experience in the form of a set of parameters.

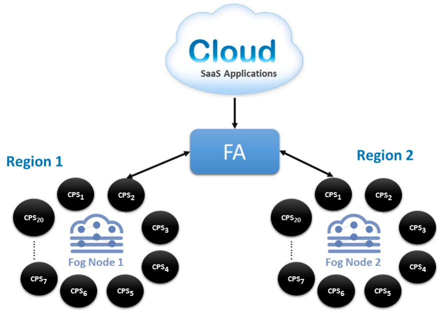


Fig. 3: Experimental Set-up

5.2 Random Forest Regression Training and Testing

As discussed in section 4.2, that random forest regression is employed to compute the trust of fog nodes and CPS devices. Next, we discuss how the regression model is trained and tested for accurate prediction of trust. The iFogSim [35] simulator quantifies the QoS parameters but it does not generate their corresponding trust labels. In order to generate the trust labels, we run the simulated Fog-CPS model (see Fig. 3) 30 times, acquired the QoS parameter values. For fog nodes, FA monitors the average CPU, memory, disk utilization, average task success ratio, and average response time. Whilst the CPS devices monitor the communication features namely, response time, bandwidth, and energy consumption.

As 20 CPS devices are connected to each fog node, in each simulation, every device is sending 20 reports thus totalling to 400 reports for one fog node. Eventually, for both fog nodes, 24,000 reports are sent in 30 executions of simulation. Likewise, FA also monitors the service quality once during each run of simulation thus generating 60 samples for both fog nodes. All the acquired QoS parameters are subsequently averaged to find the normality and based on which the trust labels are generated for each set of service features. Precisely, the objective trust gets a high value if the average task success ratio is high and the fog node fulfilled the service request by maintaining the acceptable service quality vice versa. Likewise, the CPS trust assigned a higher value if the parameters reported by CPS devices are in a given range which is quantified by averaging the parameter values in 30 runs of simulations.

Train-Test Split: Random Forest Regression model from ”sklearn. ensemble” with parameters n_estimators = 50 and max_depth = 6 is used. After statistical analysis of the

TABLE 4: Trust Results

ID	$T_{cps\rightarrow fog}$	$T_{fa\rightarrow fog}$	T_{fog}	Time
FN_1	0.60	0.59	0.70	t_1
	0.64	0.67	0.74	t_2
	0.80	0.57	0.89	t_3
	0.69	0.77	0.74	t_4
	0.59	0.60	0.73	t_5
	0.54	0.63	0.69	t_6
FN_2	0.60	0.50	0.79	t_1
	0.58	0.90	0.58	t_2
	0.80	0.55	0.67	t_3
	0.53	0.58	0.63	t_4
	0.75	0.78	0.82	$t5$
	0.59	0.76	0.83	t_6

datasets, a train-test split ratio of 70-30 is used. The goal with the test set is to capture the total variance in the data which is essentially the total number of examples to learn. As the CPS device dataset has a high number of training examples and a few number of features, the variance in that dataset could be captured with a lower training set. However, due to a small objective trust dataset, a high ratio of training-test split was required. So to be consistent in experimental evaluation, same ratio of 70-30 is used is used for both datasets. In the proposed TMS, Random Forest Regression is employed to predict both objective trust $T_{fa\rightarrow fog}$ and CPS device trust $T_{cps\rightarrow fog}$. The mean square error (MSE) is zero (0) in case of $T_{fa\rightarrow fog}$ as this dataset is very small having only 60 samples, out of which 70% (42 samples) are used for training and rest (18) for testing. So, achieving zero MSE with a non-linear regression model is justifiable. However, it was also expected that the regression model might show different accuracy results with a bigger dataset. In the case of CPS device trust $T_{cps\rightarrow fog}$, for example, the MSE is 0.12 meaning that the model predicted 88 % of the trust labels accurately.

5.2.1 Trust Results

Having trained the regression model, we next computed final trust of fog nodes and CPS devices based on models discussed in section 4. For these set of experiments, the QoS parameters are quantified in six different time periods with an increment of ten minutes in each subsequent time instance. Precisely, the first time period was 20 minutes, the second 30 minutes, and so forth. The experimental results are divided into three categories, 1) TMS Results - Hostile free Environment, 2) TMS Results - Hostile Environment, and 3) Comparative Analysis.

5.3 TMS Results- Hostile free Environment

In this experiment, it is assumed that all Fog-CPS entities operate legitimately conforming the system/protocol specifications. The trust values of both fog nodes and CPS devices are presented. For fog nodes, there are three results namely, CPS trust $T_{cps\rightarrow fog}$, objective trust $T_{fa\rightarrow fog}$, and fog node trust T_{fog} listed in Table 4. Hereinafter, the notations CPS_i, FN_i, t_i denote ith CPS device, fog node, and time instance respectively.

5.3.1 CPS Trust $T_{cps\rightarrow fog}$

Fig 4(a) illustrates the trust of a CPS device for fog node FN_1 based on energy consumption, response time, and bandwidth predicted using random forest regression model. The trust of a CPS device in first time instance t_1 is 0.79, t_2 is 0.84, t_3 is 0.72, t_4 is 0.78, t_5 is 0.62, and t_6 is 0.74.

Fig. 4(a) also illustrates the final CPS trust $T_{cps\rightarrow fog}$ for fog nodes FN_1 and FN_2 computed using Eq. (3) presented in Sec. 4.6. The CPS trust for both fog nodes FN_1 and FN_2 is also listed in 1st column of Table 4. As can be seen from Fig. 4(a), in all time instances, the CPS trust $T_{cps\rightarrow fog}$ of both fog node FN_1 and FN_2 is trustworthy i.e. greater than threshold 0.5.

5.3.2 Objective Trust $T_{fa\rightarrow fog}$

Fig. 4(b) lists the objective trust $T_{fa\rightarrow fog}$ values of fog nodes computed using Eq. (1) presented in Sec. 4.2. The second column of Table 4 also lists the $T_{fa\rightarrow fog}$. As it can be seen that in the 1st time instance t_1, the fog node FN_1 has slightly higher objective trust $T_{fa\rightarrow fog}$ than fog node FN_2. In the 2nd time instance t_2, FN_2 has higher objective trust $T_{fa\rightarrow fog}$ than FN_1. Whereas in the 3rd time instance t_3, the objective trust $T_{fa\rightarrow fog}$ of both fog nodes is almost equal. Moreover, in 4th time instance the objective trust $T_{fa\rightarrow fog}$ of FN_1 is again greater than fog node FN_2. Likewise in 5th and 6th time instances, the objective trust $T_{fa\rightarrow fog}$ of fog node FN_2 is greater than fog node FN_1. Overall as per the QoS evidence, the performance of both fog nodes is trustworthy.

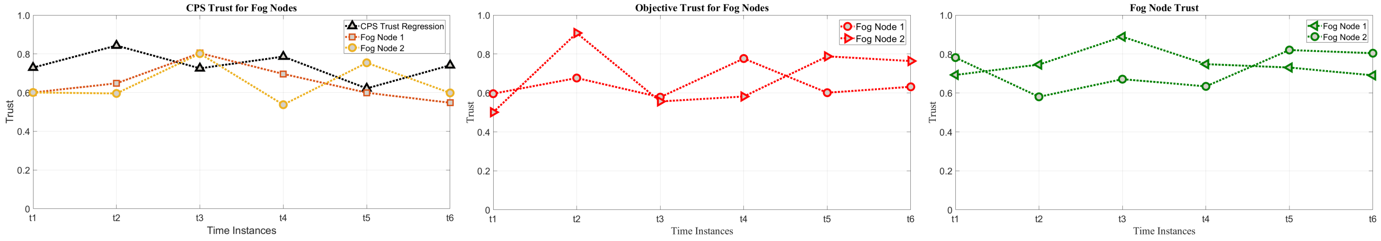
5.3.3 Fog Node Trust T_{fog}

Having computed the CPS and objective trust scores, the FA aggregates them to compute the final trust of fog nodes T_{fog} using Eq. (6) presented in Sec. 4.8. Again according to our assumption, both the fog nodes and CPS devices operate honestly; and therefore assigned equal weight $\delta = 0.5$ in Eq. (6). Fig. 4(c) illustrates the final trust T_{fog} of two fog nodes. The third column of Table 4 lists the fog node trust T_{fog}. FA also compute a trust score of all CPS devices which are getting services from different fog nodes. Both fog nodes and CPS devices assess each other on same set of parameters i.e. energy consumption, bandwidth, and response time.

5.4 TMS Results- Hostile Environment

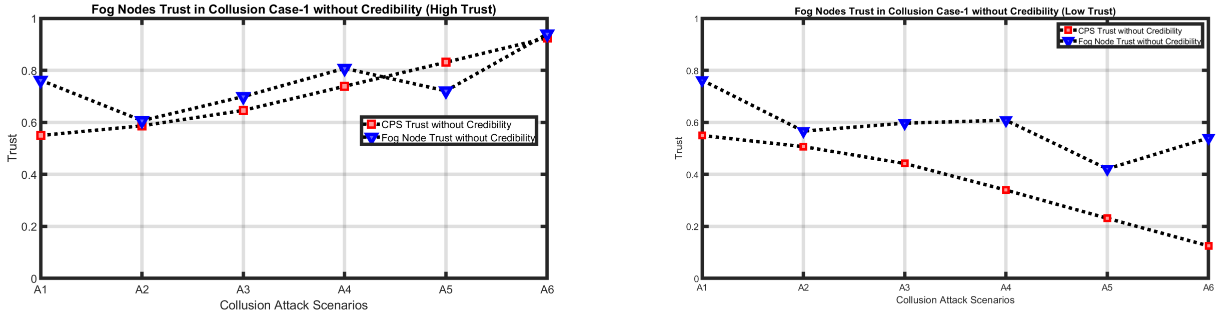
In section 4.7, the compromise of Fog-CPS entities and its impact on trust computations was discussed. This experiment is designed to elaborate the effectiveness of the trust credibility model. The credibility in Case-1 is evaluated wherein the the CPS devices are considered compromised. However, similar results will be produced for compromised FA and Fog nodes when the environment changes. Following this, we present the trust of fog nodes computed in a hostile environment by taking into consideration several attacking scenarios. Precisely, six attacking scenarios are considered whereby a percentage of parameter reports sent by CPS devices are considered malicious. Hereinafter, the notation A_i is used to denote ith attacking scenario.

In the ***first*** attacking scenario A_1, there are 0% malicious parameters i.e. all CPS devices are honest. In the ***second*** attacking scenario A_2, 10% parameters are considered malicious. Likewise, in the ***third*** A_3, ***fourth*** A_4, and ***fifth*** A_5 attacking scenarios, 25%, 50%, and 75% parameters are malicious. Lastly, in the ***sixth*** attack scenario A_6, all parameters



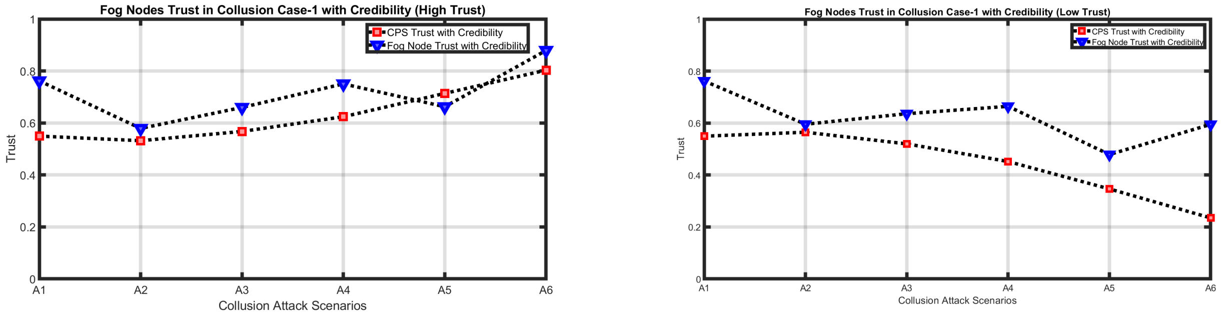
(a) (b) (c)

Fig. 4: Fog Nodes Trust in Hostile free Environment



(a) (b)

Fig. 5: Fog Nodes Trust without Credibility in Hostile Environment (***First*** Case C_1)



(a) (b)

Fig. 6: Fog Nodes Trust with Credibility in Hostile Environment (***First*** Case C_1)

are malicious. The attacking scenarios are designed such that effectiveness of credibility model can be evaluated in different configurations of hostile environments. Subsequently, we demonstrate how our trust computation model maintains the accuracy of trust results even in presence of malicious CPS devices.

The trust credibility model is evaluated in two cases where CPS devices send parameters with high and low values to change the trust of fog nodes. Two cases, C_1 and C_2, of credibility evaluation are formulated as follows:

In the ***first*** case, C_1, the malicious CPS devices send parameters with very high values in the range of [0.8 - 1] and very low values in the range of [0.05 - 0.2] in all attacking scenarios. In the ***second*** case, C_2, the CPS devices send parameters with an increment and decrement of 0.1 (i.e slightly changing the values from threshold value of 0.5). Precisely in each attacking scenario, the respective percentage of malicious CPS devices send parameters reports with an increment and decrement of 0.1.

Our credibility model analyzes the rate of change in $T_{cps \rightarrow fog}$ in consecutive time instances and subsequently adjusts the CPS trust in current time instance using Eq. (4). However, for finding an appropriate value of σ, the standard deviation in a hostile free environment during six time instances $[t_1, t_2, \ldots, t_6]$ is computed using Eq. (5). Similarly, the standard deviation in two hostile environments (i.e. credibility cases) is also computed. Lastly, final standard deviation is computed by the difference among three standard deviations. Following above computational procedure, we found $\sigma = 0.03$ and subsequently used it in credibility evaluation model. Next, we present the trust results in two credibility cases.

5.4.1 Credibility Evaluation Case-1

In the ***first*** case, C_1, we elaborate how credibility model maintains accurate and precise computation of CPS trust $T_{cps \rightarrow fog}$ and fog node trust T_{fog}. Both results with or without credibility are presented. It is noted that the attacking scenarios take place in different time instances i.e. $[t_1, t_2, \ldots, t_6]$. However, the results do not mention the time instances but they should be considered when analyzing the results.

$T_{cps \to fog}$ and T_{fog} trust results without considering the credibility are shown in fig. 5. When malicious CPS devices report high trust values, $T_{cps \to fog}$ increases in each subsequent attacking scenario as shown in fig. 5(a). As a result, T_{fog} is also increasing. Similarly, in case of low trust values, the $T_{cps \to fog}$ and T_{fog} are decreasing with increasing percentage of malicious CPS devices in different attacking scenarios.

Fig. 6 illustrates the CPS trust $T_{cps \to fog}$ and fog node trust T_{fog} computed by considering the credibility model in the first case. From fig. 6(a), it can be observed that CPS trust is increasing with high trust values in each attacking scenario due to increasing percentage of malicious devices. It has increased from 0.54 in A_1 to 0.80 in A_6 which subsequently increased the fog node trust T_{fog}. However, due to the credibility model, there has not been a dramatic increase in trust. Likewise, fig. 6(b) shows the CPS trust $T_{cps \to fog}$ and fog node trust T_{fog} computed when the malicious CPS devices send low values of trust. Again, it can be observed that CPS trust $T_{cps \to fog}$ sharply decreases from 0.54 in A_1 to 0.23 in A_6. Fog node trust T_{fog} is also changing due to change in $T_{cps \to fog}$, it dropped from 0.73 to 0.60.

It can be analyzed that without credibility model malicious CPS devices can easily increase/decrease the trust of fog nodes and subsequently push trust to highest 1 and lowest 0 values. It is therefore essential to compute the credibility of $T_{cps \to fog}$ and adjust any discrepancies accordingly.

5.4.2 Credibility Evaluation Case-2

The ***second*** case C_2 of credibility evaluation is designed to check the robustness of credibility model in detecting smaller changes in CPS trust. In this experiment, the malicious devices are slightly changing the parameters values with an increment and decrement of 0.1. In other words, in case of high trust, if in A_1, all devices are sending parameters values between 0.5 and 0.6. In second attacking scenario A_2, 10% would send values between 0.6 and 0.7; while the rest of them will report values between 0.5 and 0.6. Likewise, in A_3, 25% would send values between 0.7 and 0.8; while the rest of them will report values between 0.5 and 0.6. The same happens to low trust wherein CPS devices try to slightly decrease the trust in each subsequent attacking scenario.

Fig. 7(a) shows the CPS and fog node trust computed without considering the credibility model. It can be analyzed that there has been a slight increase in CPS trust $T_{cps \to fog}$ in each attacking scenario. CPS trust increases from 0.54 in A_1 to 0.66 in A_6. Fog node trust T_{fog} is also changing accordingly. Similar to high trust, the malicious CPS devices can also collude to decrease the $T_{cps \to fog}$. Fig. 7(b) shows the trust when CPS devices are sending parameter values which result into lower trust. Again, it can be observed that CPS trust $T_{cps \to fog}$ is decreasing from 0.54 to 0.25 in each subsequent attacking scenario. The decrease in $T_{cps \to fog}$ also decreased the T_{fog} which dropped from 0.74 in A_1 to 0.60 in A_6.

The trust results computed with credibility model are shown in fig. 8. Again, both conditions of devices increasing and decreasing the CPS trust are considered. Fig. 8(a) illustrates the results with high trust. It is noted that the credibility model successfully identifies change in trust in consecutive time instances and/or attacking scenarios and adjusts it accordingly. Overall the CPS trust $T_{cps \to fog}$ remained between 0.54 to 0.56. As a result, T_{fog} also did not decreased much. However, the change in T_{fog} is due to the objective trust $T_{fa \to fog}$ in the specific time instance.

Fig. 8(b) shows the CPS and fog node trust when CPS devices are colluding to decrease the trust of fog nodes. The CPS trust is decreasing as more and more devices are sending values between 0.5 and 0.1 in different attacking scenarios. As a result of this, the CPS trust decreased from 0.54 to 0.36. It is underlined that CPS trust without credibility reached 0.25 in A_6 (see fig. 7(b)) , however due to the credibility model it did not change so low this time. Moreover, due to credibility model the fog node trust T_{fog} remained between 0.76 to 0.67.

5.4.3 Resilience against Attacks

The Fog-CPS systems can be vulnerable to many attacks as explained in section 1, with the aim of attackers to degrade the accuracy of trust computation model or impact the availability of the TMS . For example, in collusion attack, the malicious attackers can collaborate together to increase/decrease the trust of fog nodes. Likewise, in self-promoting and bad-mouthing attacks, the compromised devices report positive and negative parameters to change the trust of fog nodes.

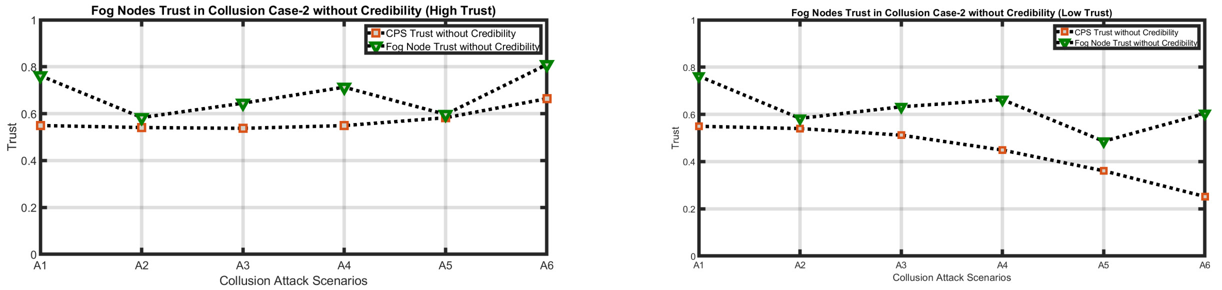
It can be observed that despite having different nature of attacks, in all cases, trust changes dramatically and therefore the key to addressing this challenge was to detect and subsequently adjust the change in trust. In line with this, a notion of trust credibility evaluation was introduced and the change in trust is quantified by correlating it with the standard deviation. We believe that the adoption of a generalized technique i.e. measuring standard deviation of trust in hostile and hostile free environments is adequate to develop a resilient trust management system. Our approach is also similar to the credibility model proposed in [19] which countermeasures the Sybil and collusion attacks.

5.5 Comparative Analysis

As the research in fog computing is in its early stages, there are very few trust models. There is no trust model which computes trust for both fog nodes and CPS devices. Due to these limitations, the fog node trust T_{fog} results of proposed TMS are not comparable to existing approaches. However, the CPS trust results are compared with one existing study [10].

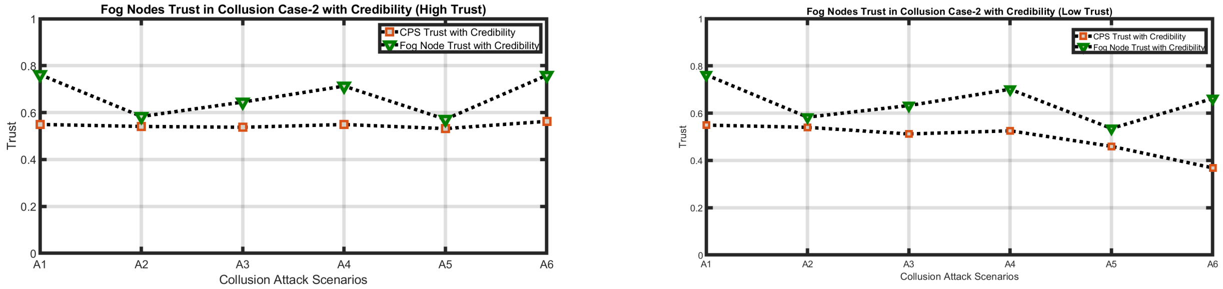
5.5.1 Autonomic Trust Management Framework [10]

In this work, a trust model for dynamic cloud based IoT systems is proposed. The autonomic trust management framework is based on IBM 's MAPE-K feedback control loop. A major limitation of the proposed framework is the inability to detect the data anomalies. With the current



(a) (b)

Fig. 7: Fog Nodes Trust without Credibility in Hostile Environment (***Second*** Case C_2)



(a) (b)

Fig. 8: Fog Nodes Trust with Credibility in Hostile Environment (***Second*** Case C_2)

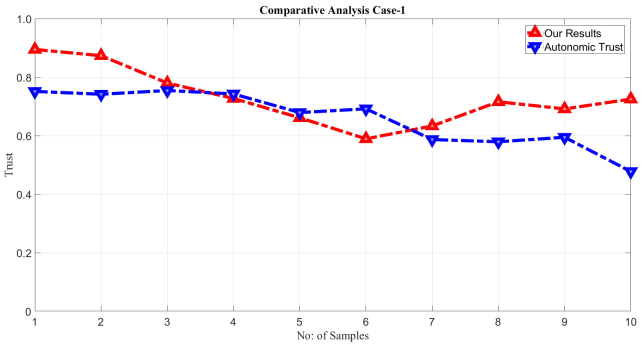


Fig. 9: Comparative Analysis Case-1

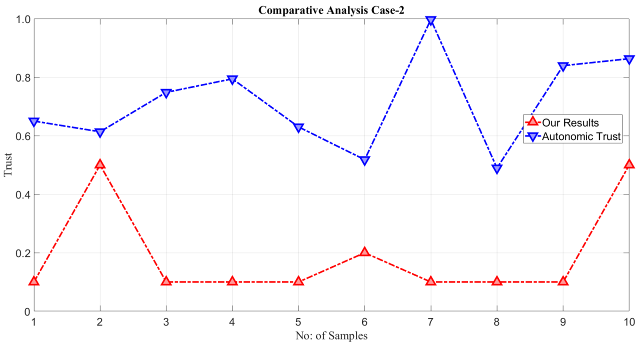


Fig. 10: Comparative Analysis Case-2

proposed model, if the anomalous parameters are incorporated into trust computation then the resulting CPS trust is inaccurate and does not fall between -1 and 1, as reported in Eq. (1) and (2) in section 6 of [10]. However, in our proposed trust computation model, the data anomalies are detected. All parameter values which are out of the range are not considered into trust computation. To evaluate the limitations of [10], three cases of comparative analysis are considered, 1) Normal case, 2) Parameters values greater than V_{max} (upper limit of range), and 3) Parameter values less than V_{min} (lower limit of range). In all cases, the CPS trust $T_{cps \to fog}$ computed by our model is compared with [10]. In each comparison case, ten samples are taken randomly and do not belong to a specific attacking scenario and time instance.

5.5.2 *Comparative Analysis Normal Case*

In the normal case, it is assumed that all parameters are within a given range. Fig. 9 illustrates the CPS trust $T_{cps \to fog}$ of both models. It can be seen that the CPS trust computed by our model lies between 0.58 and 0.89. Similarly, in case of [10], $T_{cps \to fog}$ lies between 0.47 and 0.75. Overall, in normal case, the trust computation in both models are trustworthy .

5.5.3 *Comparative Analysis* $(> V_{max})$

In the second case, the parameter values greater than V_{max} are considered. Fig. 10 shows the CPS trust $T_{cps \to fog}$ results. It can be analyzed that CPS trust computed by our model lies between 0.1 to 0.5. However, in case of [10], the CPS trust lies between 0.48 to 0.99. However, there are false parameters but the autonomic trust model is considering them therefore resulting into inaccurate results.

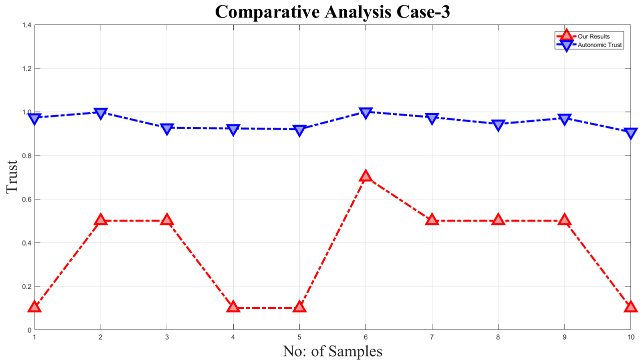


Fig. 11: Comparative Analysis Case-3

5.5.4 Comparative Analysis $(< V_{min})$

In third case, the parameter values less than V_{min} are considered. Fig. 11 illustrates the CPS trust $T_{cps \to fog}$ values in case-3. It can be observed in Fig. 11 that our proposed model can detect the data anomalies and therefore compute accurate CPS trust. However, in case of [10], all trust values are equal to 1 which is not a correct trust quantification.

Overall it is maintained that the normalization introduced in [10] does not take into consideration the parameter reports sent by compromised CPS devices. The anomalous parameter values do not compute an accurate and precise trust scores. However, our proposed trust credibility evaluation model takes care of all these aspects and therefore computes CPS trust with an improved accuracy and precision.

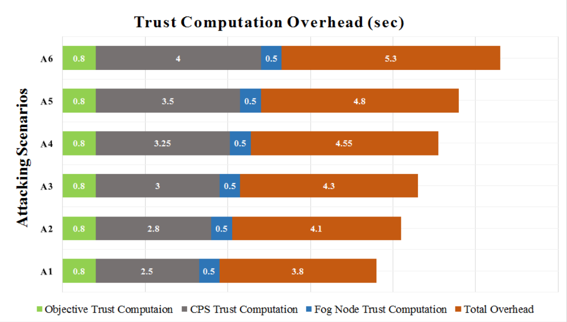


Fig. 12: Trust Computation Overhead

5.6 Trust Overhead Results

Fig. 12 reports the overhead of objective $T_{fa \to fog}$, CPS $T_{cps \to fog}$, and fog node T_{fog} trust computations in all attacking scenarios from A_1 to A_6. It is noted that the overhead of objective trust $T_{fa \to fog}$ and fog node T_{fog} in all attacking scenarios is 0.8 and 0.5 seconds respectively. However, the CPS $T_{cps \to fog}$ trust computations are incurring different overhead in each attacking scenario. The CPS trust computation overhead is the summation of time required for data anomalies detection, random forest regression training and testing, and trust credibility evaluation. The timing are different because the random forest regression training and testing is taking different time in each attacking scenario. Precisely, $T_{cps \to fog}$ takes 2.5 sec in A_1, 2.8 sec in A_2, 3 sec in A_3, 3.25 sec in A_4, 3.5 sec in A_5, and 4 sec in A_6. Overall, trust computation in all attacking scenarios $[A_1, A_2, \dots, A_6]$ takes 3.8, 4.1, 4.3, 4.5, 4.8, and 5.3 seconds respectively.

The trust parameters overhead on CPS devices is measured as follows. Every CPS device sends 20 reports (consisting of three parameters namely, energy consumption, bandwidth and response time) to FA in one time unit. Each report requires 6 bytes for storing three parameters and subsequently for 20 reports the overhead is 120 bytes. The above results demonstrate that our proposed TMS is lightweight and incurs small computation overhead, hence suitable for large scale and dynamic Fog-CPS.

6 Conclusion

In this paper, we proposed a TMS for Fog-CPS systems. The trustworthiness of CPS devices and fog nodes is evaluated based on QoS and network communication features by employing the random forest regression model. A credibility evaluation model is designed to countermeasure the malicious behaviour (i.e. collusion, Sybil, self-promotion and bad-mouthing) of compromised entities. The experimental results are compared with an existing model [10] which cannot detect and therefore prevent the data anomalies attack. Our results demonstrate that the proposed TMS can not only detect the data anomalies but also prevent other malicious behaviours of compromised entities. Lastly, considering the recent endeavours to urbanization, more specifically the research in smart cities, our TMS proposal is timely and important.

Acknowledgment

The authors would like to thank the anonymous reviewers for their helpful and constructive comments. Special thanks to Erasmus Mundus (INTACT project) for funding this research.

References

[1] A. Taherkordi and F. Eliassen, "Towards independent in-cloud evolution of cyber-physical systems," in *2014 IEEE International Conference on Cyber-Physical Systems, Networks, and Applications*, Aug 2014, pp. 19–24.

[2] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the ukrainian power grid," SANS ICS, Tech. Rep., Mar. 2016. [Online]. Available: https://ics.sans.org/

[3] D. H. McKnight and N. L. Chervany, "What is trust? a conceptual analysis and an interdisciplinary model," in *AMCIS 2000 Proceedings*, 2000. [Online]. Available: https://aisel.aisnet.org/amcis2000/382

[4] B. K. Jayaswal and P. C. Patton, *Design for Trustworthy Software: Tools, Techniques, and Methodology of Developing Robust Software*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2006.

[5] X. Li, H. Ma, F. Zhou, and X. Gui, "Service operator-aware trust scheme for resource matchmaking across multiple clouds," vol. 26, no. 5, pp. 1419–1429, 2015.

[6] W. Fan and H. Perros, "A novel trust management framework for multi-cloud environments based on trust service providers," Nov 2014.

[7] N. Ghosh, S. K. Ghosh, and S. K. Das, "Selcsp: A framework to facilitate selection of cloud service providers," vol. 3, no. 1, pp. 66–79, Jan 2015.

[8] X. Li, H. Ma, F. Zhou, and W. Yao, "T-broker: A trust-aware service brokering scheme for multiple cloud collaborative services," *IEEE Transactions on Information Forensics and Security*, pp. 1402 –1415, 2015.

[9] A. Nagarajan and V. Varadharajan, "Dynamic trust enhanced security model for trusted platform based services," vol. 27, no. 5, May 2011.

[10] S. Namal, G. Hasindu, G. Myoung Lee, and T.-W. Um, "Autonomic trust management in cloud-based and highly dynamic iot applications," in *ITU Kaleidoscope: Trust in the Information Society (K-2015)*. Barcelona, Spain: IEEE, dec 2015.

[11] M. Nitti, R. Girau, and L. Atrozi, "Trustworthiness management in the social internet of things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1253 – 1266, may 2014.

[12] W. Li and H. Song, "Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2017.

[13] Y. Wang, Y.-C. Lu, I.-R. Chen, J.-H. Cho, A. Swami, and C.-T. Lu, "Logittrust: A logit regression-based trust model for mobile ad hoc networks," in *6th ASE International Conference on Privacy, Security, Risk and Trust*, 2014.

[14] A. M. Shabut, K. P. Dahal, S. K. Bista, and I. U. Awan, "Recommendation based trust model with an effective defence scheme for manets," *IEEE Transactions on Mobile Computing*, vol. 14, no. 10, pp. 2101–2114, 2015.

[15] H. Xia, G.-d. Wang, and Z.-k. Pan, "Node trust prediction framework in mobile ad hoc networks," in *IEEE TrustCom/BigDataSE/ISPA*, 2016.

[16] F. Bao, I. Chen, and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based internet of things systems," in *2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, March 2013, pp. 1–7.

[17] A. Josang and R. Ismail, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 42, no. 3, pp. 618– 644, 2007.

[18] B. Li, L. Liao, H. Leung, and R. Song, "Phat: A preference and honesty aware trust model for web services," vol. 11, no. 3, pp. 363–375, 2014.

[19] T. H. Noor, Q. Z. Sheng, L. Yao, S. Dustdar, and A. H. Ngu, "Cloudarmor: Supporting reputation-based trust management for cloud services," *IEEE Transactions on Distributed Systems*, pp. 367 – 380, 2016.

[20] D. Ferraris, C. Fernandez-Gago, and J. Lopez, "A trust-by-design framework for the internet of things," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Feb 2018, pp. 1–4.

[21] T. Wang, Y. Li, Y. Chen, H. Tian, Y. Cai, W. Jia, and B. Wang, "Fog-based evaluation approach for trustworthy communication in sensor-cloud system," *IEEE Communication Letters*, vol. 21, no. 11, pp. 2532–2535, 2017.

[22] T. Wang, L. Qiu, G. Xu, A. K. Sangaiah, and A. Liu, "Energy-efficient and trustworthy data collection protocol based on mobile fog computing in internet of things," *IEEE Transactions on Industrial Informatics*, 2019.

[23] A. Rein, R. Rieke, M. Jäger, N. Kuntze, e. A. Coppolino, Luigi", N. Cuppens-Boulahia, F. Cuppens, S. Katsikas, and C. Lambrinoudakis, "Trust establishment in cooperating cyber-physical systems," in *Security of Industrial Control Systems and Cyber Physical Systems*. Cham: Springer International Publishing, 2016, pp. 31–47.

[24] J. Pawlick and Q. Zhu, "Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control," *IEEE Transactions ON Information Forensics and Security*, vol. 12, no. 12, pp. 2906– 2919, 2017.

[25] Y. Wang, "Trust quantification for networked cyber-physical systems," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2055– 2070, 2018.

[26] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2018.

[27] C. Perera, Y. Qin, J. C. Estrella, S. Reiff-Marganiec, and A. V. Vasilakos, "Fog computing for sustainable smart cities: A survey," *ACM Computing Surveys*, vol. 50, no. 3, Jun. 2017.

[28] Z. Wen, R. Yang, P. Garraghan, T. Lin, J. Xu, and M. Rovatsos, "Fog orchestration for internet of things services," *IEEE Computer Society*, pp. 16 – 24, jun 2017.

[29] 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. 19 293 – 19 304, Oct. 2017.

[30] N. Constant, D. Borthakur, M. Abtahi, H. Dubey, and K. Mankodiya, "Fog-assisted wiot: A smart fog gateway for end-to-end analytics in wearable internet of things," in *IEEE Symposium on High Performance Computer Architecture HPCA*, editor, Ed., Feb.

[31] A. Criminisi, J. Shotton, and E. Konukoglu, "Decision forests: A unified framework for classification, regression, density estimation, manifold learning and semi-supervised learning," vol. 7, no. 2-3, p. 81–227, 2011.

[32] H. Kim, H. Lee, W. Kim, and Y. Kim, "A trust evaluation model for qos guarantees in cloud systems," *International Journal of Grid and Distributed Computing*, vol. 3, no. 1, 2010.

[33] L.-q. Tian, C. Lin, and Y. Ni, "Evaluation of user behaviour trust in cloud computing," in *International Conference of Computing and Applied System Modelling*, editor, Ed., 2010.

[34] L. Xiaoyong and Y. Yuehua, "Trusted data acquisition mechanisms for cloud resource scheduling based on distributed agents," *China Communications*, vol. 8, no. 6, pp. 108–116, 2011.

[35] H. Gupta, A. V. Dastjerdi, S. K. Ghosh, and R. Buyya, "ifogsim: A toolkit for modeling and simulation of resource management techniques in the internet of things, edge and fog computing environments," *Cloud and Fog Computing, Wiley Online Library*, pp. 1275–1296, May 2017.

A. K. Junejo received her B.S. in Software Engineering and M.S. in Information Technology from Mehran University of Engineering and Technology, Pakistan. She received Ph.D. in 2019 from City, University of London, UK. Since 2008 to present she has been working as a visiting lecturer and software engineer in Mehran University of Engineering and Technology, Pakistan. Her research interest include fog computing, cyber physical systems, security and privacy of cloud computing, applied cryptography, and trust management.

N. Komninos received his Ph.D. in 2003 from Lancaster University (UK) in Information Security. He is currently a senior Lecturer (US System: Associate Professor) in Cyber Security in the Department of Computer Science at City, University of London. Since 2000, he has participated, as a researcher or principal investigator, in a large number of European and National R&D projects in the area of information security, systems and network security. He has authored and co-authored more than ninety journal publications, book chapters and conference proceedings publications in his areas of interest.

Mithileysh has been working as a Research Scientist at Red Sift, London and carrying out research at the City, University of London, UK. His expertise in communication systems – at both theoretical and application levels – ranges from industrial projects to academic ones. His major research focuses on Smart Technologies, Communication Systems, Forensic Science, Data Science, Human-computer Interaction, Visualisation, and Social Informatics.

Bhawani Shankar Chowdhry (SM'87) received the Ph.D. degree from the Renowned School of Electronics and Computer Science, University of Southampton, Southampton, U.K., in 1990. He has teaching and research experience of more than 30 years. He is a leading person at MUET of several EU funded Erasmus Mundus Program including "Mobility for Life," "StrongTies," "INTACT," and "LEADERS."