Wireless Networks (2020) 26:2339–2351
https://doi.org/10.1007/s11276-019-02106-3

A trust computed framework for IoT devices and fog computing environment

Geetanjali Rathee[1] · Rajinder Sandhu[1] · Hemraj Saini[1] · M. Sivaram[2] · Vigneswaran Dhasarathan[3,4]

Published online: 29 July 2019

Abstract
In this paper, we have demoralized the transmission processing concerns of fog nodes and IoT device layer attack during the handoff (mobility) of IoT devices in the fog environment. A secure routed and handoff mechanism is proposed in order to avoid the attack by exploring the trust value and rating of each fog IoT and fog nodes/devices based on their communication behaviour. A trust manager is established between fog layer and IoT layer that keeps the record of all fog nodes in its look-up table and detects the malicious fog and IoT nodes. Further, the fog nodes computes rating of their service requested IoT layer and routed the services through highly trusted possible path. The proposed mechanism is validated against conventional security approaches over certain networking parameters.

Keywords Trust manager · Social impact theory optimizer · Fog environment · Handoff IoT devices security · Fog devices/nodes · IoT security

1 Introduction

The rapid proliferation of distributed technologies and emergence of new wireless deployment models have resulted in an increasing number of smart applications to be involved with cloud computing. Cloud computing is an information technology (IT) paradigm that collects and analyzes the real time fine-grained data over the internet [1]. However, due to significant physical distance amongst cloud data centres and End Users (EUs)/Internet of Things (IoT) devices, smart applications users from timely processing of data, sustainable traffic congestion, end-to-end delay and high communication cost. Therefore, in order to overcome these is issues, Fog computing [2] has been emerged as an extension to traditional cloud computing infrastructure for supporting low latency, high mobility and geographically distributed IoT based applications. Fog layer is a virtualized platform between cloud layer and IoT device layer that offers the storage, computation and networking services to IoT layer through network devices. The key motivation behind the vision of Fog computing is to offer low latency for processing of data from various unknown/known IoT devices. However, this opportunistic accessing of network services by various devices may increase the probability of several security attacks in fog layer [3, 4]. Further, from the security perspective, it is possible that at fog layer and IoT layer, the intruder may introduce number of malicious activities which will affect the overall performance of smart applications. An attacker may imitate the legitimate IoT device during the communication between the routers (at the fog layer) and during the mobility (handoff) or upon the new entry of device [5, 6]. Handoff process occurs when the IoT device moves from one place to another and searches for a new Fog Node/Fog Device (FN/FD) due to decrease of SNR ratio of the current FN. During this process, intruder may incorporate a Malicious User (MU) to involve some malicious

✉ Vigneswaran Dhasarathan
vigneswaran.d@tdtu.edu.vn

[1] Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, Solan, H.P. 173234, India

[2] Department of Computer Networking, Lebanese French University, Erbīl, Kurdistan Region, Iraq

[3] Division of Computational Physics, Institute for Computational Science, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[4] Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam

activities in order to access or consume the network resources. While in the fog layer, the network devices may act maliciously with intent to degrade the network performance. Figure 1 represents the relationship between TCP/IP and different phases of Fog computing by highlighting the inherited and specific security threats at each layer of Fog environment [7]. In the conventional communication procedures, all the IoT devices and network devices such as routers, bridges, hubs, switches are often assumed to be trusted and cooperative. However, in practice, where the number of known/unknown devices communicated in colossal domain, there is always high probability of the intruders to gain the unauthorized network access. Figure 1 presents the various security threats specific at different layers such as application layer, network and internet layer and network interface layer.

1.1 Research significance

IoT objects/devices may badly affect the society in other way when compromised by various intruders. Despite a lot of IoT application such as healthcare, industries, smart home/society, many business organizations are afraid to opt this technique because of its security concerns. Any organization that may benefit the use of IoT devices, number of intruders may hack the system or record mechanism for benefiting their own concerns. Further, a group of technical experts may forge the network systems and increase or decrease their business growth in order to continue their misbehaviour with the users. In addition, due to the wireless nature and communication procedures of FN there may be a possibility where the FN can be compromised by the intruders to behave maliciously. As soon as the organizations using IoT devices/sensors, its necessary information must be registered somewhere and the each and every activity of sensors must be tracked for user safety. Therefore, there is need to propose some security methods based on cryptographic and trust computing mechanism to identify the authenticity and legitimacy of the devices. The sensors that provide the services to their respective users must be recorded and analyzed regularly to check their behaviour in the network while providing the services. Any intruder that compromised number of IoT devices should be under recognition immediate to prevent huge loss to the firms. Furthermore, at the EU/IoT layer, a New User (NU) or a Handoff EU (HEU)/IoT device can deny the legitimate devices to access the services by authenticating itself to the FNs. The secure communication and transmission process among IoT devices will leads the various organizations to these technologies.

1.2 Motivation

Though several works have proposed number of cryptographic security/privacy mechanisms during the message transmission or mobility of the devices in different environments such as VANETS, MANETS, WSN and WMN [8–10].These mechanisms cannot be directly adopted in Fog environment because of its unique characteristics. The cryptographic schemes may increase number of storage, communication and computation overheads which will further increase the transmission latency. These security issues encourage the author's to provide the security through other methods/frameworks. Now days, the legitimacy of the applications or IoT devices can be measured through the value of trust [11, 12]. A trust in the network is defined as a measuring parameter that computes the

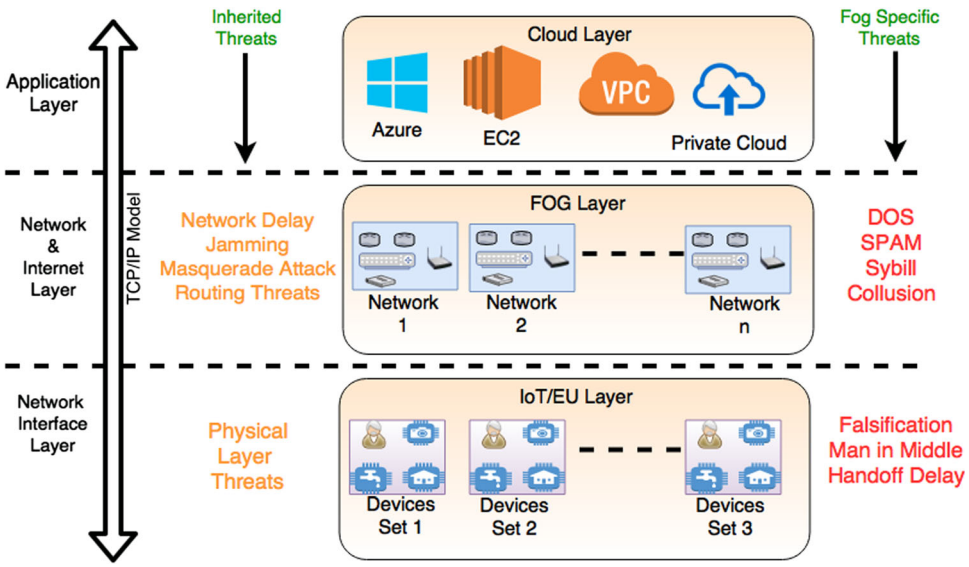

Fig. 1 The relationship between TCP/IP model and fog environment including inherited and specific security threats

legitimacy of a particular node depending upon its existing or previous interactions without enhancing the cryptographic issues.

So, according to the best of author's acquaintance, the potential method to ensure a secure communication mechanism is trust based method. Trust based techniques enhance the security without degrading the communication overhead and increasing the network metrics in comparison to the cryptographic techniques. Unfortunately, trust based security mechanism/frameworks in fog computing and IoT layer has not been systematically recognized and is still in its early stages. Therefore, to study and propose trust based security mechanisms in Fog environment is quite critical prior to the design and implementation of fog-assisted IoT applications.

The paper's objective of this paper is to propose a security mechanism that effectively detects the legitimate FN and IoT devices by computing the Trust Value/Trust Factor (TV/TF) of individual nodes and rating of each neighbouring node by introducing a Trust Manager (TM) between Fog and IoT layer. The task of TM is to verify the legitimate of FN in the network by computing the rating and TV/TF of all the FN depending upon their previous history interactions using the Social Impact Theory Optimizer (SITO). Further, the FN route the services through a highly trusted path for IoT devices that computes the level wise trust of each FN using tidal trust algorithm. In IoT layer, if an IoT device wants to access some network services, the FN will compute the TV of the requesting IoT device and match it with the computed threshold value, if the device's TV is greater than FN rating, then the device is assumed to be trusted and allowed to access the Fog layer services. The TM will keep the record of all the TV/TF and rating of FN into its look-up table including node id, node address, TV/TF and rating. The proposed approach has been verified against malicious number of fog nodes versus network resources, percentage of malicious number of fog nodes versus trusted nodes, malicious fog node versus HEU (handoff IoT device) and fog nodes versus Mobile HEU (MHEU). The potential contributions of the proposed framework are as follows:

- Identifying the role of trusted security framework in fog computing environment.
- Proposing a trusted security framework for fog computing milieu using TV/TF values.

The remaining organization of the paper is as follows. The related work of secure fog environment is presented in section II. The trust based security framework for communication of FN and IoT layer is proposed in section III. Further, section IV analyzed the performance metrics of proposed framework in certain scenarios while the detailed numerically simulated results are illustrated in section V. At last, section VI concludes the work and highlights the future scope.

2 Related work

Although fog plays a central role in delivering a rich portfolio of services more efficiently to the IoT layer, it could impose security challenges during accessing or providing the network services to the IoT devices and between the FN. Due to the wireless nature of IoT and FN, the Fog computing inherits the traditional wireless security threats as well as its own security issues due to its own unique property of providing computation at network devices. Table 1 depicts the inherited and specific security issues of fog environment. Authentication [13], rogue node detection [14], falsification [15] and trusted FN/EU are the key factors that need to be verified before accessing the services of FN by the IoT device. Authentication is to be considered as an essential requirement for the security of IoT devices. There exist certain cryptographic operations to authenticate the IoT device within or during the device's mobility. Various researchers have proposed several authentication schemes based on users' identities to realize the authenticity of the users in ad-hoc cloud-based or cloud-based networks. Various efficient authentication approaches [16–18] have been intended to support IoT services such as face identification and erect secure mechanism based on fog computing, however, none of these schemes consider the mobility of IoT devices (EU). A number of anonymous authentication schemes have been enabled in the FN to confirm the legitimacy EU without exposing their identities, however due to this property, various secrecy techniques, e.g., k-anonymity [19], group signatures [20] and pseudonyms [21, 22] are widely used to sever the links between authentication messages and EUs' identities. With these secrecy techniques, the other users and cloud cannot distinguish the target users. Unfortunately, it is firm to keep the connections action because of the EU mobility in reality, such as driverless cars in a high speed.

In order to address this issue in vehicular communications, Ni et al. [23, 24] exploits the data retrieval scheme to attain the consequences of parking navigation services from roadside entity for drivers. Due to the discrete kinds of Fog and varied needs of real-time facilities, whether this approach can be used in Fog computing is still an open issue. Moreover, the users may be further recognized under security threats [25–27], as the unidentified information is cross-referenced with other information from diverse sources, e.g., purchase records, trajectory and social graphs. Therefore, the defensive technique is not adequate for securing the user's privacy and security in Fog

Table 1 Security attacks in fog and cloud computing environment

Inherited attacks	
Jamming [3]	The jamming attack goal is to obstruct in radio frequencies that are used through the transmission
Eavesdropping [4]	The broadcasting environment of wireless network leads to several eavesdropping threats that lies within the range of communicating nodes
Tampering [5]	A tampering assailant could nastily delay, drop or modify transmitting data to interrupt fog computing and degrade its efficiency
Message alteration [6]	The attacker aim is to alter the routed message in order to consume the network services
Forgery [9]	The intruder not only forges the profiles but also hack the identities of all entities
Network delay [9]	The intruders may increase the network jamming by coding the fake request messages in the network in order to delay the packet transmission
Routing threats [9]	The intruders may reroute the packets or compromise some of intermediate nodes between source and destination
Fog specific	
Spam [3]	It refers to the generation of false collection of data gathering and interrupts by the intruders
Collusion [8]	More than two parties collude to mislead, defraud or deceive the legal entities
Man-in-middle [4]	It presents among two communicating parties by the mean of modifying or altering ongoing messages
DoS [4]	It broadcasts the useless traffic in the network by affecting the network metrics
Sybill [5]	It either exploits pseudonyms or manipulates the fake id by compromising the fog nodes
Falsification [6]	Where the attacker hacks the address of trusted nodes by means of disrupting the network metrics
Handoff attack [9]	Where, the MU tries to authenticate itself during the handoff process

computing. Further, these IoT devices (EUs) don't have enough memory or power to accomplish the security operations needed for an authentication protocol. Even though numbers of cryptographic mechanisms have been proposed to secure the FD from intruders, however, the key management and storage overhead may enhance the communication cost and latency issue in Fog environment. First of all these techniques enhances the key management, computational/communication overhead in the decision making process of smart applications. Secondly most of the proposed approaches ensure the integrity that are effectual for external threats and are found completely infeasible besides internal threats. So, according to the best of author's knowledge, the prospective method to certify a secure decision making process or delivering of messages is trust based method. Trust based techniques improve the security by decreasing the communication overhead and increasing the network performance in comparison to cryptographic methods. A number of trust management mechanisms have been proposed by various researchers under two trust models [28] which are (1) evidence based trust model where a third party is involved in order to prove the trust relationship among two EUs and (2) monitoring based trust model that ascertains the trust among the users based upon their previous history interactions. Wei et al. [29] anticipated a trust management mechanism to estimate the trustworthiness of the users from the negative and positive feedback based on their direct verification. In case where direct verification is not available, indirect verification such as third-party evidence should also be used for ensuring the users trust. Further, Su et al. [30] offers an end-to-end trust based on the security parameters of all participating nodes consisting audit-based factors and security properties of the system. The trusted parameters that are considered as computing the reputation of each user and seeing the data usage actions through past history. Several works have been considered for aggregating the trust verifications from various sources and filtering out biased evidences. Nitti et al. [31] distinct a subjective trusted model to facilitate every user to compute the trust of its neighbours on the basis of users in common with the potential servers and opinion of its own experience. Moreover, reputation is a significant metric to appraise the trust level of the user and various reputation management schemes have been projected to appraise the users' trustworthiness in vehicular ad hoc network (VANET), mobile ad-hoc network (MANET) [32], delay tolerant network and mobile crowd sensing [33–35]. However the proposed trust management framework/schemes/methods need to be improved for Fog environment due to decentralized, mobile and wireless nature of EU and FD. The number of attacking strategies introduced various security issues in fog environment (device and fog layer) where MU compromised the FD or EU by concussing or mimicking the legitimate FD or EU. However, there is a need to ensure the security procedures at fog as well as EU (IoT) layer by resolving the above issues. The researchers have proposed number of cryptographic procedures/mechanisms but only

few researchers have proposed number of trust based mechanisms in fog and IoT environment. However, there exist some challenges that need to be focussed such as for HEU (mobile IoT devices) security and the mechanism to identify the trusted FD [36, 37]. Wazid et al. [38] have proposed a light weight authentication mechanism based on three factors such as password, smart card and personal identity. The proposed mechanism is validated and analyzed thoroughly against real time environment. Further the proposed phenomenon is validated through formal and informal security schemes against various functionality features. The out performance of this mechanism is compared against traditional authentication scheme over communication and computation costs and overheads. Das et al. [39] have proposed a two phase such as node authentication and key agreement procedure for ensuring a secure communication process among two sensing nodes. The proposed mechanism proposed a light weight security scheme using elliptic curve cryptography algorithm. The proposed phenomenon is validated efficiently against informal and formal security concerns over traditional cryptographic schemes. Further, a practical demonstration is analyzed against computation and communication cost results over existing technique.

3 Proposed framework

In order to ease the readability of our proposed approach, the IoT devices layer is called as EU layer where the number of IoT devices layer will be known as EU layer. However, the Fog nodes layer will be specified as same FN layer. An analytical description of the proposed framework has been presented in this section by categorizing the approach into two different cases which are: (1) when the FN is identified as Malicious Node (MN) and (2) when the Malicious User (MU) is identified during the handoff process or upon the entry of New User (NU) in the environment of legitimate EU (IoT device). A system model is categorizing them into 2 sub-levels as discussed in seceding subsections. The proposed framework is described for two different aspects which are (1) at the EU layer where the HEU or NEU is introduced by the intruders and (2) at the fog layer where the FNs are compromised to behave maliciously. The framework is depicted in Fig. 2 which comprises of a TM, a decentralized fog environment including n number of fog nodes among which some may be the MN and an EU layer having HEU, NU.

As depicted in Fig. 2, the numbers of nodes are divided at different levels such as node A at level 0 and B, C, D at level 1 and so on. A number of EUs, HEU and NU may enter and request for the network services from their domains FNs. Initially, during the network establishment all the nodes are assumed to be trusted and legitimate. However, the threat of security increases with the increase in the communication process between the FN and EU-FN. Therefore, the network is considered to be an ideal and trusted at the time of establishment. In order to degrade the security measure of fog environment, the MUs may get randomly deployed during the HEU or entry of NU and during the processing of requested information by the FN's. The intent of the MU is to decrease the performance of the network by restricting the trusted EU or FN to access or provide the services. The TM working at fog layer that keeps the record of TV/TF and rating computed for all the FN using SITO [36] and tidal trust approach [37]. Initially the trust of all FN is computed based on their liveliness and previous history interactions. Further the trust at each level will be computed using tidal trust algorithm. The tidal trust approach is generally works at two different phases: (1) In the first phase, the level wise trust and rating of all the FNs will be computed. The FN at level i + 1 will be computed by the FN at level i (2) In the second phase, FN computes the trust of its EU before providing the services and choose the best trusted intermediate nodes to transmit the requested service to the EU. In this paper, the Ist phase of tidal trust will work at fog level where the record of all the FD will be stored by TM and the second phase will work at EU layer where EU requests for services from the FD. The detailed description of both the phases is discussed below.

3.1 At fog level

The fog layer is a graph based phenomenon where each node may communicate with another node and has a bidirectional relationship with other nodes. In this paper, we have considered unidirectional relation in order to better understand the proposed framework. Now, in order to compute the trust, initially the SITO technique is used where the nodes will compute and assign some trust values between 0 and 1 to their neighbours depending upon its previous history interactions. The record of all FNs rating and TV/TF will be consequently updated in the TM into its look up table. As the communication proceeds, the first part of tidal trust algorithm begins from a randomly chosen FN by computing the TV of its neighbouring nodes by dividing into certain level. All nodes are placed based on certain predefined level such as first fog node at level 0 and so on as depicted in Fig. 3. This procedure prolongs in recursive manner for every level, and computes the TV of their neighbours using their previous history interactions. Figure 3 depicts the state of the graph after the first step of Tidal Trust approach where the neighbours of the nodes, on level 1, are rated based on the value of nodes at level 0. For example in Fig. 3 node B is rated 0.45 because node A has its trust valued at 0.45.

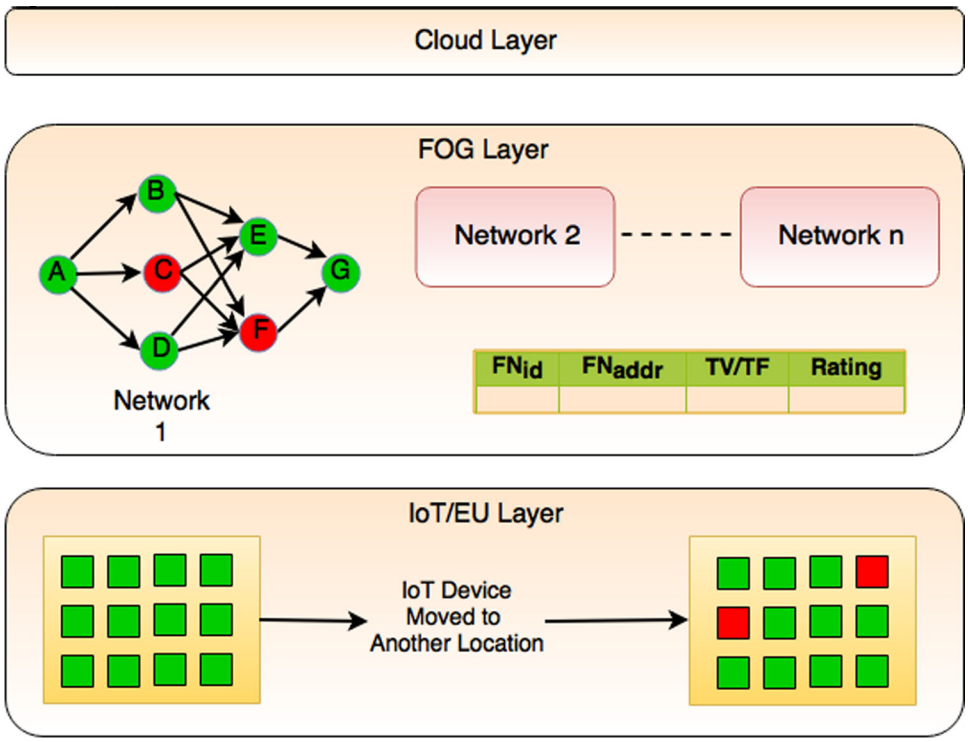

Fig. 2 Layers of proposed framework

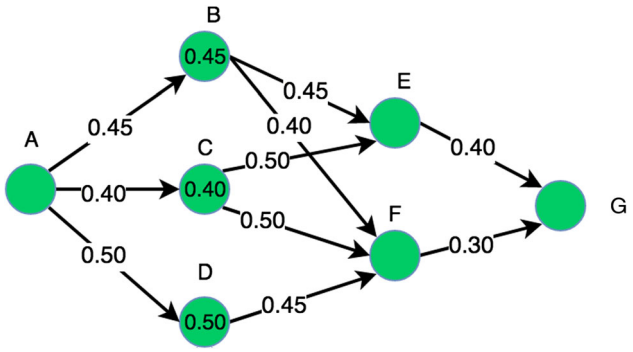

Fig. 3 Fog nodes before attack

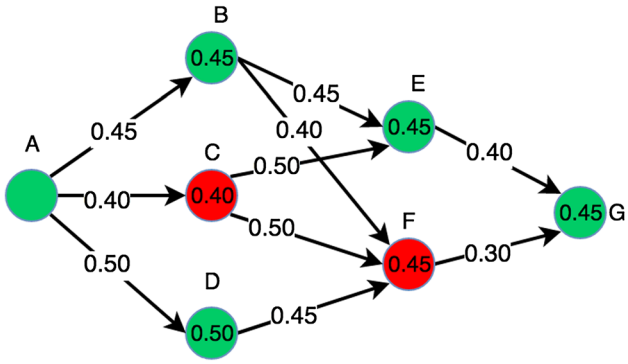

Fig. 4 Fog nodes after attack

Similarly, node C and D are rated 0.40 and 0.50 by node A. Subsequent to every node at level 1 has been rated, the tidal trust algorithm continues to the next step till all the nodes are rated. Every node from level 1 will further gives its rating to their neighbour in level 2 and the value of that rating is the minimum among its rating and its trust towards that neighbour. If any node from level 2 has more than one ancestor at level 1, then its rating would be the maximum of the ratings that its predecessors gave it. Figure 4 shows the graph state after step-to-of the algorithm are finished. In this example, node E has been rated by its predecessors C and B. Further, C rated E with the minimum of its ratings (0.40) and his trust towards E (0.50) that is 0.40. Similarly, B rated E with the minimum of its ratings (0.45) and its trust towards E (0.45) is 0.45. The final rating of E is the maximum among these two ratings and its value is 0.45. This first portion of algorithm prolong in recursive manner as Breadth First Search (BFS). The aim of step of the tidal trust algorithm is to dynamically establish the threshold value of the trust between FN (source) and EU (destination). The threshold value is determined once all the nodes are assigned with TV and rating. This value is determined as the maximum rating of the nodes in the final level of the graph which are associated to the EU, that have some trust to the EU.

Now if a node is compromised by an intruder as depicted in Fig. 4 and starts behaving malicious, in that case, the TV and rating of that node would be very less. Therefore, the low rated node would be discarded and may never be considered for communication. The stepwise description of the above process is depicted in Algorithm 1.

Algorithm 1 Computing the TV/TF and rating of all FN's at each level

Require: Level of all the Nodes in the Graph

1: Initially each node FN_i computes the TV/TF of its neighbouring nodes using SITO by computing following parameters:
2: **function** TV
3: if liveliness and DDR > Assumed Threshold Value
Then
4: Trusted FN
5: **else**
6: Malicious FN
7: **end if**
8: **function** Compute liveliness
9: Count ← 0
10: if NU transmits number of requests (hello) messages to CCU then
11: Count ← Count + 1
12: if Count >= $Count_{Thresholdvalue}$ **then**
13: NU ← MU
14: **else**
15: NU ← Trusted CU
16: **end if**
17: **end if**
18: **end function**
19: **function** Compute DDR
20: DDR ($Indegree_{packets-Outdegree_{packets}} \times 100$
1: **if** DDR <= $DD_{thresholdvalue}$ **then**
22: NU ← MU
23: **else**
24: NU ← Trusted CU
25: **end if**
26: **end function**
27: **end function**
28: Apply tidal trust algorithm at each level in order to compute or Initialize the level wise trust and rating of each FN_i.
29: **function** Level_trust
30: Initially the FN_i at level i assign the TV and rating to FN_i at level i.
31: if FN_i has more than one input from Level i then
32: Trust of FN_i at Level i + 1 ← min(FN_i(TV); FN_i(rating))
33: Trust of FN_i ← max(TV (FN_1; FN_2; ::::::::; FN_i))
34: **end if**
35: **end function**
36: **function** Rating
37: At level i, FN_i assign TV that will rate the FN_i at level i + 1
38: level i + 1 rating would bemin(leveli(FN_i(rating); FN_i(TV))
39: **end function**
40: Level i FN_i assign the TV and rating to level i + 1 FN_i.
41: Recursion is done for calculating the trust and rating of all FN_i.
42: Termination of the recursion Step 40 until all the FN_i have TV and rating

3.2 At IoT device/EU level

In the second algorithm of proposed framework, trust towards the EU is computed through number of intermediate FNs. In this every FN in the graph calculate their trust values towards the EU by Eq. 1:

$$t_{n_i,eu_i} = \frac{t_{n_{i,j}} \times t_{j,eu_i} \| t_{i,j} > max}{t_{n_{i,j}} | t_{i,j} \geq max} \quad (1)$$

where trust threshold is max, t_{n_i} is the trust between the nodes n_i and eu_i, and j are all neighbours of node n_i. Nodes which are associated to the EU have their values towards the EU. Nodes having them as neighbours will compute their TV's in direction of the EU using above formula. The trust threshold is worn to filter out the nodes having low rating. Further, in these computations only the nodes with rating value above threshold trust are worn. This procedure is recursively prolonged for every level of nodes, until the source is reached and its trust value towards the sink is calculated. In that case, the FD will compute the trust over its HEU/NU using the above process and choose the best path to provide the network services as depicted in Fig. 3. If HEU request network services from a FD, then FD will compute the rating and trust using the Eq. 1 as defined and will provide the services if the trust is above the thresh-old by choosing the most trusted path. The complete execution of proposed mechanism is presented in Algorithms 1 and 2.

Algorithm 2 Computing the TV/TF and rating of all FN's at each level

1: e_{ui} communicate with FN_i
2: FN_i compute threshold rating using Level Trust()
3: FN_i compute multiple paths to e_{ui} by comparing each FN_i (rating) with threshold rating
4: **if** FN_i rating > Threshold rating then Include that node FN_i in the path
5: **else** Discard that node from the path
6: **end if**
7: FN_i will compute the best trusted path using Equation

4 Performance and experimental evaluation

There is no as such simulator or environment available in the current market space to test the trust-based identification of malicious EU(IoT device) and FN in fog environment. So, to conduct the performance analysis of proposed framework a synthetic testbed has been developed.

Figure 5 shows the abstracted view of the developed testbed with major components and links. Three virtual machines are provisioned from Microsoft Azure cloud DS2 V2 instance with 2 cores, 4 data disks, 7 GB of memory, 14 GB of SSD drive and 6400 max IOPS. These virtual machines are running a version of NS2 tool with pre-defined network of fog device and initial trust values has been also assigned to each node. A 700 m × 700 m network area is created with small and big network sizes, with 25 and 500 number of nodes, respectively. The nodes are portable in nature, that is, they can abandon their IoT environment and join another network at any time, NS2 version running on three virtual machines have different fog environment with configuration provided in Table 2.

Proposed algorithm has been coded in all three NS2 instances so to calculate the trust values of fog nodes. Initially 6000 virtual micro instances are created which act as IoT device for our proposed testbed which are equally distributed to all the three virtual machines. A synthetic data generator is used which generated data and send to these virtual machines using a Normal distribution pattern and based on the data received at virtual machine configuration of NS2 are changed. Malicious nodes are added into the environment based on the probability distribution during assignment and handoff process. Handoff process is when any IoT device changes its sink node from one virtual machine to another virtual machine. Addition of malicious nodes, handoff nodes and conversion of node to malicious node during handoff is based on the probabilities listed in Table 3. Addition of malicious node probability means that out of 100 deployed micro-instance (acting as IoT) device and fog nodes 15 are malicious.

Table 2 Configuration of NS2 for different virtual machines

S. no.	Virtual machine	Nodes	Edge nodes	Levels
1	VM1	100	10	20
2	VM2	150	15	30
3	VM3	200	20	40

Handoff probability represents that on single unit of time 10 out of 100 nodes change their fog environment due to movement or other reason. Conversion to malicious during handoff state that out of 100 handoff processes 10 nodes will be converted from legitimate to malicious. Taking all these initial assumptions performance analysis is conducted for 60 min. Conversion to malicious node and handoff process take place after each minute based on the probability distribution stated in Table 3.

4.1 Existing approach

For validating the proposed trust framework, the mechanism is compared against existing security technique proposed by Das et al. [39]. They have proposed a two phase such as node authentication and key agreement procedure for ensuring a secure communication process among two sensing nodes. The proposed mechanism proposed a light weight security scheme using elliptic curve cryptography algorithm. The proposed phenomenon is validated efficiently against informal and formal security concerns over traditional cryptographic schemes. Further, a practical demonstration is analyzed against computation and communication cost results over existing technique. However,

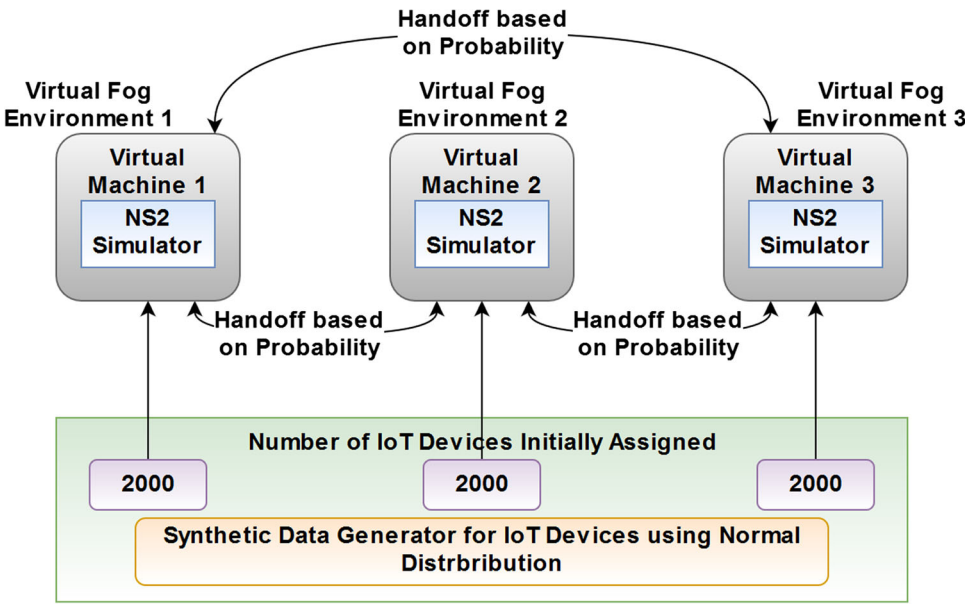

Fig. 5 Testbed for performance analysis of proposed framework

Table 3 Different probabilities used for performance analysis of proposed framework

S. no.	Activity	Probability of attack (%)
1	Addition of malicious nodes	15
2	Handoff nodes	10
3	Conversion to malicious during handoff	10

in our proposed mechanism, the computation and communication cost, key management and storage overhead is resolved using trust based scheme where the devices legitimacy is computed or validated through its trust value.

4.2 System state

Based on the testbed created in Fig. 5, various parameters related to system state were recorded to study the changes in the system. Figure 6 provides the total number of nodes in the system during the course of 60 min of the experiment.

Initially 2000 nodes are assigned to each fog environment and after each minute 50 more nodes are assigned to test the scalability of proposed framework, as represented in the linear trend of Fig. 6. Addition of malicious node is also done based on the probability mentioned in the Table 3, which also resulted in linear trend with almost same number of nodes in each FE, as shown in Fig. 7. Figure 8 represented the number of handoff happened from each FE to another FE based on the probability mentioned in Table 3. As seen in Fig. 8 large numbers of handoffs are happening in the system, this was done deliberately so as to check the security of FN during the handoff process.

4.3 Performance parameters

Multiple parameters were recorded for performance comparison of proposed framework based on the testbed created for the same. Figure 9 provides the accuracy of the proposed system to detect the MN from large number of IoT devices/nodes connected to respective FEs.

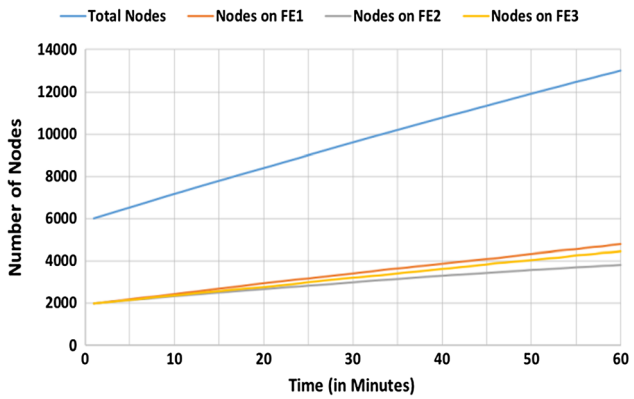

Fig. 6 Total number of nodes in the system

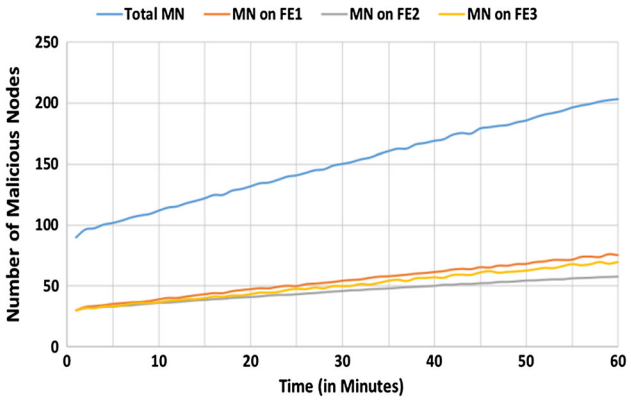

Fig. 7 Total number of malicious nodes in the system

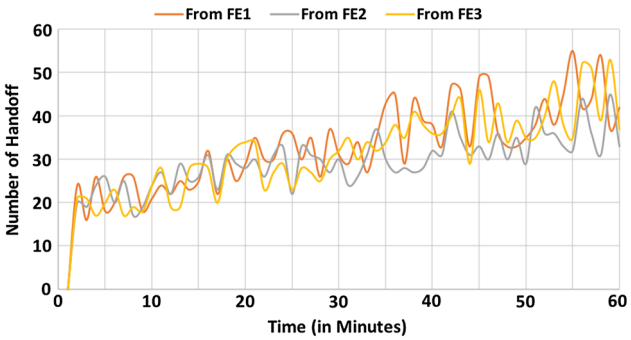

Fig. 8 Total number of handoff happened in system

Proposed framework provides close to 85% accuracy for the prediction of MN this can be further improved if experiment runs for longer period. With this much detection power, it is assumed that response time of the proposed

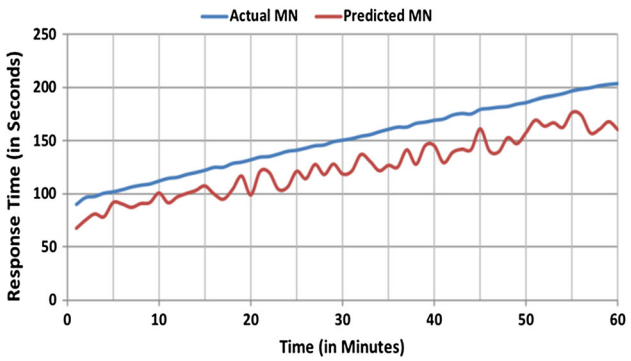

Fig. 9 Accuracy comparison for prediction of malicious nodes

system will increase but as depicted in Fig. 10 proposed framework is better than traditional system.

Here, traditional system is when MN is not detected based on the trust values and they are not removed from the system which causes in the increase in response time of the system. Proposed framework when detects any node as MN it removes it from the system immediately so that it does not further hinder the performance. This results in better response time and utilization of resources as shown in Figs. 11, 12 and 13. Figure 14 provides the number of requests processed by the system and its linear trend for all three FE. It can be observed that as the increase in number of nodes is linear the number of requests to be processed also increases linearly.

4.4 Results and discussion

Proposed framework has been evaluated based on multiple FE and IoT devices for which a customized testbed has been proposed. Experiment evaluation conducted was successful and multiple results regarding various parameters have been recorded. System state and performance parameters results are presented in Sects. 4.1 and 4.2 respectively. The ratings and trust of IoT devices depend entirely upon nodes' communication behaviour that makes the security mechanism more efficient as compared to existing security schemes. Further, during the involvement of malicious nodes in the communication process, the proposed trust based scheme immediately detect the malicious behaviour and block them for future communication. In addition, the detection or identification of malevolent nodes at its early stages improves the network performance by efficiently utilizing the network resources, network congestion, packet loss rate, end to end delay and network throughput. System behaved as desired and all performance parameters were positive for proposed system for any IoT based Fog computing environment. Accuracy was close to 85% which will be further improve with time

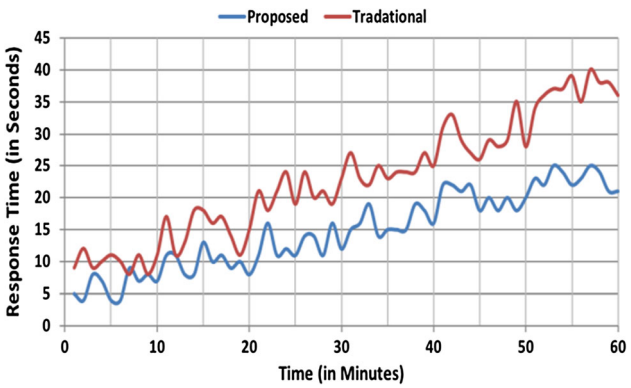

Fig. 10 Response time comparison for prediction of malicious nodes

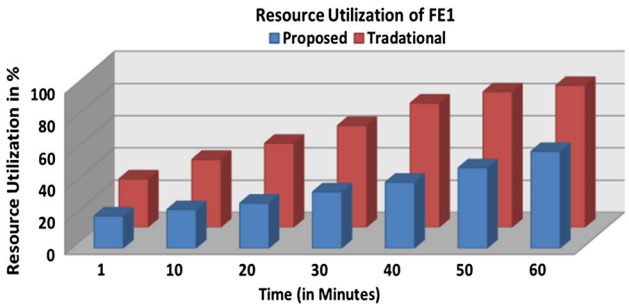

Fig. 11 Resource utilization in fog environment 1

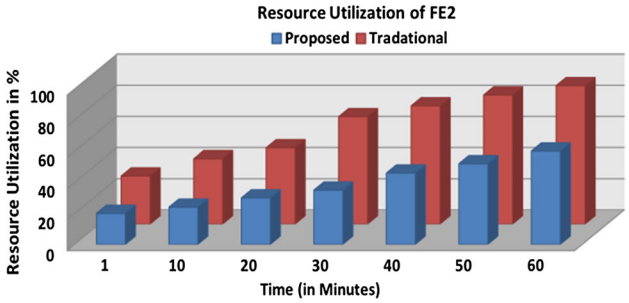

Fig. 12 Resource utilization in fog environment 2

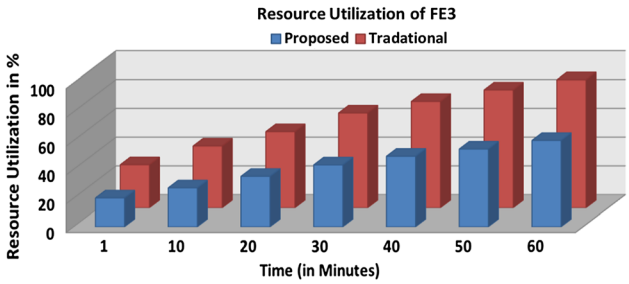

Fig. 13 Resource utilization in fog environment 3

and response time will be fast because of removal of detected MNs from the system. Detection of MNs based on trust and removal of detected MNs did not hinder the performance of other nodes as shown in number of request processed data. Overall proposed system was successful in detection of MNs in fog computing and IoT environment and also achieved the desired performance for all other nodes sending data to Fog computing environment.

5 Conclusion

Addition of malicious nodes in the fog computing and IoT environment affects the fundamental reason of using the fog and IoT layer for computing latency sensitive application. Detection of malicious node is continuous process and depends on connecting nodes for which calculation of trust plays a significant role. In this paper a framework is

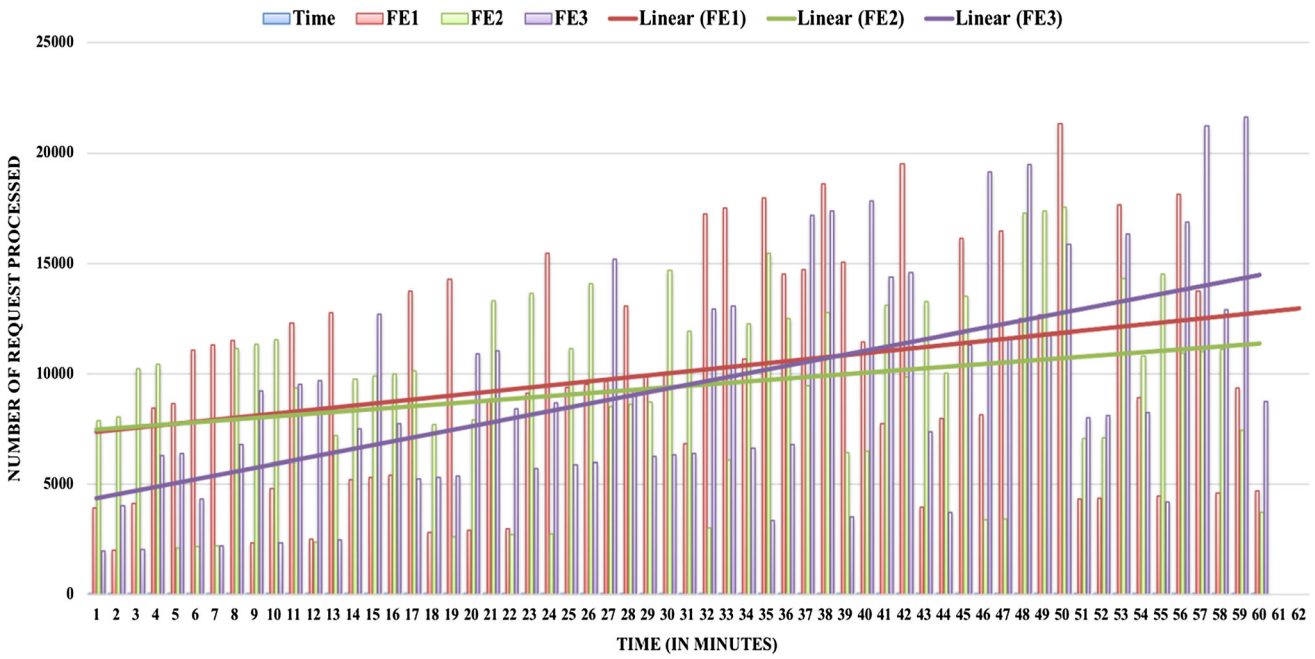

Fig. 14 Number of Request Processed By Each Fog Environment With Linear Trend Line

proposed which calculates tidal trust for each node and detects the malicious nodes based on predefined values. The proposed approach has been successfully verified against various networking parameters such as malicious number of fog nodes versus network resources, percentage of malicious number of fog nodes versus trusted nodes, malicious fog node versus HEU (handoff IoT device) and fog nodes versus Mobile HEU (MHEU). The key point of proposed framework is consideration of handoff and conversion of any fog node and IoT device node to malicious during the handoff process with 85% improvement as compared to existing technique. Future work will include the calculation of trust services running on fog and IoT nodes along with the node trust values against different random and dynamic nature of IoT environment. Further, other types of threats specific to fog environment will be reported in future communications.

Acknowledgements The authors would like to express their sincere thanks to Prof. Dr. Truong Khang Nguyen, Division of Computational Physics, Institute for Computational Science, Ton Duc Thang University, Ho Chi Minh City, Vietnam for giving his value suggestion, comments and support to complete this work as effective.

References

1. Mouradian, C., Naboulsi, D., Yangui, S., Glitho, R. H., Morrow, M. J., & Polakos, P. A. (2018). A comprehensive survey on fog computing: State-of-the-art and research challenges. *IEEE Communications Surveys and Tutorials, 20*(1), 416–464.
2. Hao, P., Wang, X., & Shen, W. (2018). A Collaborative PHY-aided technique for end-to-end IoT device authentication. *IEEE Access, 6,* 42279–42293.
3. Ni, J., Zhang, K., Lin, X., & Shen, X. (2017). Securing fog computing for internet of things applications: challenges and solutions. *IEEE Communications Surveys & Tutorials, 20,* 601–628.
4. Zuo, C., Shao, J., Wei, G., Xie, M., & Ji, M. (2018). CCA-secure ABE with outsourced decryption for fog computing,". *Future Generation Computer Systems, 78,* 730–738.
5. Altisen, K., Devismes, S., Jamet, R., & Lafourcade, P. (2017). SR3: Secure resilient reputation-based routing. *Wireless Networks, 23*(7), 2111–2133.
6. Rathee, G., Sharma, A., Saini, H., Kumar, R., & Iqbal, R. (2019). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimedia Tools and Applications*, 1–23.
7. Chiang, M., Ha, S., Chin-Lin, I., Risso, F., & Zhang, T. (2017). Clarifying fog computing and networking: 10 questions and answers. *IEEE Communications Magazine, 55*(4), 18–20.
8. Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. *IEEE Internet Computing, 21,* 34–42.
9. Rathee, G., Saini, H., & Singh, G. (2018). Aspects of trusted routing communication in smart networks. *Wireless Personal Communications, 98*(2), 2367–2387.
10. Rathee, G., &Saini, H. (2017). Modified AODV (MAODV) against black hole in WMN. In *Proceedings of the national academy of sciences, India section A: Physical sciences* (pp. 1–12).
11. Bertino, E., & Islam, N. (2017). Botnets and internet of things security. *Computer, 2,* 76–79.
12. Zhu, C., Rodrigues, J. J., Leung, V. C., Shu, L., & Yang, L. T. (2018). Trust-based communication for the industrial internet of things. *IEEE Communications Magazine, 56*(2), 16–22.
13. Chandrasekhar, S., & Singhal, M. (2017). Efficient and scalable query authentication for cloud-based storage systems with

multiple data sources. *IEEE Transactions on Services Computing, 10*(4), 520–533.
14. Conti, M., Lal, C., Mohammadi, R., & Rawat, U. (2019). Lightweight solutions to counter DDoS attacks in software defined networking. *Wireless Networks, 25*(5), 2751–2768.
15. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2018). A Sybil attack detection scheme for a forest wildfire monitoring application. *Future Generation Computer Systems, 80,* 613–626.
16. Park, P. (2019). Markov chain model of fault-tolerant wireless networked control systems. *Wireless Networks*, *25*(5), 2291–2303.
17. Wasef, A., & Shen, X. (2013). EMAP: Expedite message authentication protocol for vehicular ad hoc networks. *IEEE Transactions on Mobile Computing, 12*(1), 78–89.
18. Jiang, Q., Ma, J., Wei, F., Tian, Y., Shen, J., & Yang, Y. (2016). An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. *Journal of Network and Computer Applications, 76,* 37–48.
19. Hu, P., Ning, H., Qiu, T., Song, H., Wang, Y., & Yao, X. (2017). Security and Privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. *IEEE Internet of Things Journal, 4*(5), 1143–1155.
20. Pointcheval, D., & Sanders, O. (2016). Short randomizable signatures. In *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)* (Vol. 9610, pp. 111–126).
21. Li, C., Qin, Z., Novak, E., & Li, Q. (2017). Securing SDN infrastructure of IoT–fog networks from MitM attacks. *IEEE Internet of Things Journal, 4*(5), 1156–1164.
22. Martin, D. J., Kifer, D., Machanavajjhala, A., Gehrke, J., & Halpern, J. Y. (2007). Worst-case background knowledge for privacy-preserving data publishing. In *SIGMOD'05: Proceedings of the 2005 ACM SIGMOD international conference on management of data* (pp. 49–60).
23. Ni, J., Lin, X., Zhang, K., & Shen, X. (2017). Privacy-preservingreal-time navigation system using vehicular crowdsourcing. In *IEEE vehicular technology conference*.
24. Ni, J., Zhang, K., Lin, X., Yu, Y., & Shen, X. (2016). *Cloud-based privacy-preserving parking navigation through vehicular communications* (pp. 85–103). Cham: Springer.
25. Jin, R., & Zeng, K. (2018). Physical layer multi-user key generation in wireless networks. *Wireless Networks*, *24*(4), 1043–1054.
26. Weng, J., Miao, C., & Goh, A. (2006). An entropy-based approach to protecting rating systems from unfair testimonies. *IEICE Transactions on Information and Systems, E89-D*(9), 2502–2511.
27. Jain, A. K., Tokekar, V., & Shrivastava, S. (2018). Security enhancement in MANETs using fuzzy-based trust computation against black hole attacks. *Advances in Intelligent Systems and Computing, 625,* 39–47.
28. Li, H., & Singhal, M. (2007). Trust management in distributed systems,". *Computer, 40*(2), 45–53.
29. Wei, Z., Tang, H., Yu, F. R., Wang, M., & Mason, P. (2014). Security enhancements for mobile ad hoc networks withtrust management using uncertain reasoning. *IEEE Transactions on Vehicular Technology, 63*(9), 4647–4658.
30. Su, Z., Biennier, F., Lv, Z., Peng, Y., Song, H., & Miao, J. (2017). Toward architectural and protocol-level foundation for end-to-end trustworthiness in Cloud/Fog computing. *IEEE Transactions on Big Data*, 1–23.
31. Nitti, M., Girau, R., & Atzori, L. (2014). Trustworthiness management in the social internet of things. *IEEE Transactions on Knowledge and Data Engineering, 26*(5), 1253–1266.
32. Cho, J.-H., Swami, A., & Chen, I. R. (2011). A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys & Tutorials Tutorials, 13*(4), 562–583.
33. Xu, Y., Zhu, Y., & Qin, Z. (2019). Urban noise mapping with a crowd sensing system. *Wireless Networks*, *25*(5), 2351–2364.
34. Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems, 1*(2), 99–109.
35. Farris, I., Taleb, T., Khettab, Y., & Song, J. (2018). A survey on emerging SDN and NFV security mechanisms for IoT systems. *IEEE Communications Surveys & Tutorials, 21*(1), 812–837.
36. Macas, M., & Lhotska, L. (2007). Social impact theory based optimizer. *Advances in Artificial Life, Proceedings, 4648,* 635–644.
37. Golbeck, J. A. (2005). Computing and applying trust in web based social networks. *Annals of Physics, 54*(1), 9–19.
38. Wazid, M., Das, A. K., Odelu, V., Kumar, N., Conti, M., & Jo, M. (2017). Design of secure user authenticated key management protocol for generic IoT networks. *IEEE Internet of Things Journal, 5*(1), 269–282.
39. Das, A. K., Wazid, M., Yannam, A. R., Rodrigues, J. J., & Park, Y. (2019). Provably secure ECC-based device access control and key agreement protocol for IoT environment. *IEEE Access, 7,* 55382–55397.

Dr. Geetanjali Rathee is currently working as an Assistant Professor in Computer Science and Engineering Department in Jaypee University, Waknaghat, Solan. She has received B.Tech. Degree in Computer Science and Engineering from Bhagwan Mahavir Institute of Engineering and Technology (BMIET), Haryana in the year 2011. She has completed her M.Tech. in Computer Science and Engineering from Jaypee University, Waknaghat, Solan in the year 2014. She has done her Ph.D. from Jaypee University, Waknaghat, Solan in the year 2017. Her research interest include resiliency in wireless mesh network, routing protocols, network protocols and security in next generation communication systems, security aspects in cognitive radio network.

Dr. Rajinder Sandhu is currently working as Assistant Professor (Senior Grade) in the Department of Computer Science and Engineering at Jaypee University of Information Technology (JUIT) Waknaghat, Solan, Himachal Pradesh-India since November, 2016. He has obtained his Ph.D. from Guru Nanak Dev University, Amritsar in 2017 and M.E. with honours from Thapar University, Patiala in 2013. He was research fellow in CLOUDs Laboratory, University of Melbourne, Australia in 2016–2017. He has published his research work in Scientific Citation Index journals of Elsevier, John Wiley and Springer. He also filed two patents in Indian Patent Office. He is also consultant to Gigabyte Pvt. Ltd. and Nihon

Communication, Bangalore for Cloud Computing and Big Data. He is reviewer of many reputed SCI journals of Elsevier, Wiley and Springer. Starting from his M.E., he has delivered multiple expert talks on cloud computing for various workshops and FDPs of reputed universities like JNU-Delhi, PEC-Chandigarh and IIT-Kharakpur. His current working research areas are cloud computing, Big Data and Internet of Things (IoT). Currently, He is working with Prof. Rajkumar Buyya from Australia and Dr. Victor Chang from China on various projects and research papers.

Dr. Hemraj Saini is currently working as Associate Professor in the Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat-173234. Prior to that he has worked in AIET, Alwar (2011–2012); OEC, Bhubaneswar (2008–2011); HIE, Baniwalid (Libya) (2007–2008); BITS, Pilani (2005–2007); IET, Alwar (2001–2005); REIL, Jaipur (2000–2001) and Dataman System, Delhi (1999–2000) for almost 19 years in Academics, Administration and Industry. Three (03) Ph.D. degrees have been awarded and two (02) Ph.D. Thesis are submitted under his valuable guidance. He is an active member of various professional technical and scientific associations such as IEEE (Mem. No. 92738007), ACM (Mem. No. 5156611), IAENG (Mem. No. 133186), etc. Presently he is providing his services in various modes like, Editor, Member of Editorial Boards, Member of different Subject Research Committees, reviewer for International Journals and Conferences including Springer, ScienceDirect, IEEE, Wiely, IGI Global, Benthem Science etc. and as a resource person for various workshops and conferences. He has published more than 100 research papers in International/National Journals and Conferences of repute. He has also organized various conferences and workshops including—NCRTDM 2011, OEC, BBSR (AICTE, DST and CSIR sponsored) and BSSCAD 2009, OEC, BBSR (DST and CSIR sponsored, INSPIR CAMP under the DST Internship, funded by DST in August 2012, IEEE PDGC-2012 as member of International TPC, 2013-IEEE ICIIP as Technical Program Co-Chair, 2015-IEEE ICIIP as Conference Chair, PDGC-2016 as the Publicity Committee Chairs and ICIIP-2017 as registration Chair.

Dr. M. Sivaram has completed his B.E. (CSE) at Bharat Niketan Engineering College, Madurai Kamaraj University, Madurai in 2002. He has awarded M.Tech. (CSE) degree from National Institute of Technology, Trichy in 2007. He has Completed Ph.D. degree in Information and Communication Engineering from Anna University, Chennai in 2014. He has nearly 18 years of experience in teaching both UG and PG program. He is presently working as a Professor in Department of Information Technology in Lebanese French University, Erbil. His field of interest are Data Mining, Image retrieval, Information retrieval, Data fusion, Image Processing and Artificial intelligence. He has published more than 30 papers in International, journals and conferences.

Vigneswaran Dhasarathan has completed his B.E. in electronics and communication from Kamaraj College of Engineering and Technology and Master of Engineering in optical communication at Alagappa Chettiar College of Engineering and Technology, Anna University, He has published five papers in refereed national/international journals and more than 15 papers in conferences. His research interest includes few-mode fiber design (LP ring core fiber and OAM fiber), few-mode amplifier system design and sensing using ring core fiber and PCF.