Information Fusion 78 (2022) 149–157

Contents lists available at ScienceDirect

Information Fusion

journal homepage: www.elsevier.com/locate/inffus

Data fusion and transfer learning empowered granular trust evaluation for Internet of Things

Hui Lin [a,b], Sahil Garg [c], Jia Hu [d], Xiaoding Wang [a,b,*], Md. Jalil Piran [e,*], M. Shamim Hossain [f,*]

[a] College of Computer and Cyber Security, Fujian Normal University, Fuzhou, Fujian, 350117, China
[b] Engineering Research Center of Cyber Security and Education Informatization, Fujian Province University, Fuzhou, Fujian, 350117, China
[c] École de technologie supérieure (ETS), Montreal, Canada
[d] University of Exeter, UK
[e] Department of Computer Science and Engineering, Sejong University, Seoul 05006, South Korea
[f] Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

ARTICLE INFO

Keywords:
Data fusion
Trust evaluation
Transfer learning
Deep reinforcement learning
Privacy preservation
Internet of Things

ABSTRACT

In the Internet of Things (IoT), a huge amount of valuable data is generated by various IoT applications. As the IoT technologies become more complex, the attack methods are more diversified and can cause serious damages. Thus, establishing a secure IoT network based on user trust evaluation to defend against security threats and ensure the reliability of data source of collected data have become urgent issues, in this paper, a Data Fusion and transfer learning empowered granular Trust Evaluation mechanism (DFTE) is proposed to address the above challenges. Specifically, to meet the granularity demands of trust evaluation, time–space empowered fine/coarse grained trust evaluation models are built utilizing deep transfer learning algorithms based on data fusion. Moreover, to prevent privacy leakage and task sabotage, a dynamic reward and punishment mechanism is developed to encourage honest users by dynamically adjusting the scale of reward or punishment and accurately evaluating users' trusts. The extensive experiments show that: (i) the proposed DFTE achieves high accuracy of trust evaluation under different granular demands through efficient data fusion; (ii) DFTE performs excellently in participation rate and data reliability.

1. Introduction

With the rapid development of edge computing and smart terminal technology, a large number of Internet of Things (IoT) applications have emerged one after another, greatly expanding data sources and bringing massive amounts of valuable data [1]. In a "data-driven" society, various IoT networks contribute to the diversity of user roles, which inevitably leads to unreliable data sources [2]. For example, data sources range from legitimate data collection nodes of heterogeneous systems and networks to malicious users or attackers. Due to the lack of security protection, these data sources are vulnerable to multiple attacks, namely node replication attacks, denial of service attacks, replay attacks, spoofing attacks, etc., causing unreliable data to seriously deviate from real data [3].

Data security threats faced by IoT applications can generally be divided into two categories: one is the external threat, i.e., malicious monitoring of transmission data, impersonating registered users to inject wrong data or launching man-in-the-middle attacks to tamper with data; the other is the internal threat, i.e., legitimate users Provide wrong data to the network to influence decision-making [4]. Generally, external threats can be prevented by methods based on signatures, authentication, and encryption, while internal threats are widely prevented by trust management [5]. Trust management mainly includes four steps: credit evidence collection, credit evaluation, trust evaluation and trust value update. Specifically, the trust management center first collects credit evidence for the trust evaluation object; then, it computes the credit value of the object based on the collected evidence by using the credit computation model; next, the trust level of object is evaluated based on the trust-related factors such as network security status, object area and object engagement time; eventually, according to the credit evidence provided by the user and the trust level of the object, the credit value of the user who provides the credit evidence is updated [6].

As an important supplement to cryptographic methods, trust management can guarantee the authenticity and validity of IoT data. Trust evaluation is a process of quantifying trust by analyzing relevant data,

* Corresponding authors.
E-mail addresses: linhui@fjnu.edu.cn (H. Lin), sahil.garg@ieee.org (S. Garg), j.hu@exeter.ac.uk (J. Hu), wangdin1982@fjnu.edu.cn (X. Wang), piran@sejong.ac.kr (M.J. Piran), mshossain@ksu.edu.sa (M.S. Hossain).

https://doi.org/10.1016/j.inffus.2021.09.001
Received 2 December 2020; Received in revised form 5 July 2021; Accepted 15 September 2021
Available online 24 September 2021
1566-2535/Published by Elsevier B.V.

and it plays a decisive role in trust management. Trust assessment has been widely used in many fields, such as social networks, digital communications, e-commerce, cloud services, and peer-to-peer networks. With the rapid development of network systems accompanied by a large influx of data, trust evaluation is shifting from model-based trust evaluation to data fusion-based trust evaluation [7]. Compared with traditional methods, data fusion has irreplaceable advantages in intelligent trust assessment. First, data fusion can reduce the size and dimensions of data and extract useful information from it. Secondly, data fusion can accurately simulate human decision-making evaluation on trust, so the evaluation results can be easily interpreted and accepted by humans. However, the processing and processing of massive data in the process of data fusion has become a key challenge [8]. To solve the above challenges, transfer learning [9], as a revolutionary breakthrough in artificial intelligence, can transfer models trained on one data set to another, so it has advantages in model training based on data fusion.

Considering the characteristics of massive, multi-modal and heterogeneous data collected from various sources for trust evaluation, in this paper, a Data Fusion and transfer learning empowered granular Trust Evaluation model, named DFTE, is proposed. The major contributions of our work are as follows.

1. To meet granular demands of trust evaluation, two time–space empowered trust evaluation models are built utilizing Deep Reinforcement Learning (DRL) methods based on data fusion, which are the fine-grained trust evaluation model constructed using the Deep Deterministic Policy Gradient algorithm (DDPG) and the coarse-grained trust evaluation model constructed based on the Deep Q-learning Network (DQN). In addition, the Transfer Learning (TL) algorithm is employed to reduce the model training time.
2. To encourage honest users, a dynamic reward–punishment mechanism is developed, in which the scale of reward and punishment is dynamically adjusted utilizing DRL methods.
3. The extensive experiments show that the proposed DFTE achieves high accuracy in trust evaluation under different granular demands and it performs excellently in participation rate and data reliability.

The rest of this paper is organized as follows. The related work is introduced in Section 2. The system architecture and attack model are given in Section 3. The proposed DFTE method is presented in Section 4. The performance evaluations are given in Section 5. We conclude this paper in Section 6.

2. Related work

In order to ensure the validity and reliability of data collected from various data sources in different fields, the topic of trust evaluation has recently attracted widespread attentions. This section introduces a systematic literature review in the field of trust evaluation based on data fusion and machine learning.

2.1. Data fusion based trust evaluation schemes

In [10], Qiu et al. defined data fusion trust architectures with different trust levels, and then proposed an efficient and practical data fusion trust system for multi-source and multi-format data exchange in heterogeneous networks. In [11], Liang et al. proposed a reliable trust computing mechanism based on multi-source feedback and data fusion in fog computing to reduce trust computing overhead, communication overhead and communication delay in the trust evaluation process. In [12], Lv et al. proposed a data security collection trust evaluation scheme based on wireless sensor networks to deal with threats in the data collection process and ensure data quality. In [13], Wang et al. designed an effective trust evaluation strategy to calculate the credibility of users in data collection during the data fusion process in the context of big data. In [14], Yu et al. made full use of the universally relevant characteristics of the data fusion process, evaluated the reliability of the ordinary group by measuring the number of communications between the ordinary group and the absolute trust group, and measured different similarities of group attributes. In [15], Gao et al. proposed a multi-criteria trust evaluation mechanism for information sources, which combined identity-based trust, behavior-based trust, relationship-based trust and feedback-based trust factors, to present information sources. In [16], Yao et al. used the weights related to vehicle nodes and their corresponding data as the main indicators for calculating trust, and analyzed the relationship between the reporter's location and time through traffic experience and utility theory, so as to achieve an effective trust assessment. In [17], Tang et al. proposed a reputation-aware data fusion mechanism to ensure data integrity by using the Gompertz function to evaluate the credibility of the data reported by the participants.

2.2. Trust evaluation schemes using machine learning

In [18], Chen et al. proposed a trust evaluation framework based on machine learning, which promotes policy by considering multiple user characteristics and standards related to trust. In [19], Hesham et al. proposed a new entity-centric trust evaluation framework, which used decision trees and artificial neural networks to ensure reliable data transmission between vehicles during the data fusion process. In [20], Karmakar et al. proposed an innovative trust evaluation model based on deep learning, which measured the trust score of IoT sensor values through time correlation to improve accuracy and reliability. In [21], Mayadunna et al. proposed a general trust evaluation framework, which selected some characteristics of social networks for training, and then designs training models and recommendation algorithms to calculate node trust values. In [22], Wang et al. used logistic regression to combine the node's own information to propose an improved algorithm for calculating the trust value of social network nodes.

Although these works contribute to trust evaluation in IoT applications, there are still the following challenges: 1) How to overcome the efficiency difficulties of trust evaluation model training based on data fusion; 2) How to meet the different granular requirements of trust evaluation; 3) How to satisfy the privacy and security requirements of trust evaluation; 4) How to overcome the problem of data collected from different but related domains, resulting in low efficiency and reliability of data fusion, and thus unable to provide effective collaborative cross-domain reputation evaluation. In this paper, a granular trust evaluation model for data fusion and transfer learning is developed to solve these four problems.

3. System architecture and attack model

3.1. System architecture

In this paper, a granular trust evaluation model DFTE for data fusion and transfer learning is developed. Specifically, the historical data collected in each area will be gathered in the data fusion center to extract the user's trust evidence, i.e., the user's trust and task completion status, and use different DRL algorithms to train a unified trust evaluation model to meet the granularity demand. After the training is completed, the unified trust evaluation model is distributed to each local trust evaluation center. For some local trust evaluation centers that cannot train a trust evaluation model, a unified trust evaluation model is directly used, while for local trust evaluation centers with model training capabilities, migration learning can be used on the basis of the unified model to reduce local model training time. Based on the above analysis, three entities should be considered, namely users, local trust evaluation centers, and the data fusion center.

1. *Users*: Each user belongs to a specific area, so the trust evaluation of users can minimize the potential security risks of non-local users (i.e, unauthorized access to sensitive information, deliberately sabotage tasks, etc.). In addition, the trust value of each user determines what kind of tasks the user can accept. For example, users with a high degree of trust can apply for high-level tasks. If the user completes the task well, his trust will increase significantly. Therefore, it is necessary to design a reasonable incentive mechanism to reward honest users and punish malicious users.
2. *Local Trust Evaluation Centers*: Each local trust evaluation center is deployed on a specific area, which assesses the trust of each user within. Since the security risks imposed by malicious users can result in significant damage, the trust of each user should be properly evaluated. For a local trust evaluation center, which is capable of implementing high-performance computations (e.g., running deep reinforcement learning based algorithms), the local trust evaluation model can be trained individually based on trust evidences, i.e., users' trusts and corresponding task completions. In addition, each local trust evaluation center can make a use of the unified trust evaluation model trained by the data fusion center to reduce the local model training time. In addition, the local trust assessment center also dynamically adjusts the user's trust level according to the areal security level.
3. *The Data Fusion Center*: The historical data collected from each area will be gathered in the data fusion center, and a unified trust evaluation model will be trained through the edge data fusion server, the edge trust evaluation server and the edge security level evaluation server. Note that the security level of an area directly affects the trust of users. For example, for areas with high security levels, users' trust levels should be evaluated more rigorously, which will result in relatively low user trust levels, while for areas with low security levels, The user's trust is relatively high. Therefore, the data fusion center must also evaluate the security level of each area. Since the security level of the area is gradually changing and the evaluation of the security level is directly related to the user's trust evidence, the frequency of execution of this evaluation is lower than that of the user. This implies the importance of trust evaluation for time–space empowered trust evaluation.

In this article, we aim to design a trust evaluation model based on data fusion to meet granular requirements. For fine-grained trust evaluation, we choose the deep reinforcement learning algorithm DDPG to determine whether the user is honest, normal or malicious, and for coarse-grained trust evaluation, we use the deep reinforcement learning algorithm DQN to determine whether the user is honest or malicious of. The reason is as follows. Both DDPG and DQN can be used to find the best strategy. However, in order to ensure the accuracy of trust evaluation, the optimal evaluation threshold needs to be found through continuous spatial search. Compared with DDPG, DQN is suitable for searching in discrete space. The system model of the proposed DFTE is given in Fig. 1.

3.2. Attack model

In this paper, we assume both data fusion center and local trust evaluation centers are honest, while users are either honest or malicious. Traditional trust evaluation often uses local trust evidence only, so a local honest user may be malicious in other areas. Therefore, this article considers privacy leakage attacks and mission destruction attacks caused by malicious users.

1. *Privacy Leakage Attack*: Malicious users launch privacy attacks on the local trust evaluation center by leaking sensitive information about tasks or sharing this information with other malicious users. This indicates that the trust evaluation mechanism should be able to dynamically adjust the user's trust to prevent malicious users from accessing sensitive tasks.
2. *Task sabotage Attack*: Once malicious users accept the task, they deliberately sabotage the attack by providing unreliable data tasks. In order to prevent such attacks, incentive mechanisms will be introduced to reward honest users and punish malicious users.

4. The proposed DFTE method

Data fusion-based trust evaluation is realized in two stages. In the first stage, the data fusion center uses different DRL algorithms to calculate a unified trust evaluation model based on the historical data provided by each area and send the model to each local trust evaluation center. In the second stage, the unified trust evaluation model is either directly used to evaluate user trust, or transfer learning is used to reduce the training time of the local trust evaluation model.

4.1. The unified trust evaluation model

The trust evaluation of users in each area depends on the user's trust evidence and cross-areal related information. The data fusion center can collect all historical data in each area and analyze and process it, so as to find the appropriate relationship between the user and the completion of the corresponding local/foreign tasks, and finally build users' trust evidences, which is considered as the data fusion process of the entire trust evaluation. the In addition, the data fusion center manages to obtain the security level of each area. This is because the security level is related to users' trusts, i.e., users of a high trust level can accept tasks in the areas of a low security level, while users of a low trust level can hardly accept tasks in the areas of a high security level.

4.1.1. Areal security level calculation

The security level of an area directly affects the trust of internal users, but how to evaluate the security level of each area is an open question. On the other hand, the completion of the user's task will affect the security level of the area. For example, the long-term outstanding task completion of an area indicates that the security level of the area is high, and vice versa. Thereby, we evaluate the security level of the ith area by

$$area_i\_securitylevel \propto \sum_{j}^{m} data_j\_reliability, \tag{1}$$

where m denotes the number of task released from the area, and $data_i\_reliability$ denotes the data reliability for the ith task. Then, the normalized value, i.e.,

$$area_i\_securitylevel = \frac{area_i\_securitylevel}{\max\{area_j\_securitylevel | j \le n\}}, \tag{2}$$

where n denotes the number of areas, is considered as the security level of the ith area. Once the security level of each area is calculated, we can adjust the trust level of each user according to the security level of the area.

4.1.2. User credit calculation

We evaluate the credit of users by evaluating the completion of local tasks and the completion of external tasks. This indicates that the user's credit is the integration of the local credit $user\_localcredit$ and the foreign credit $user\_foreigncredit$, that is,

$$user\_credit = \alpha \times user\_localcredit + (1-\alpha) \times user\_foreigncredit, \tag{3}$$

where $\alpha \ge 0.5$. Since the user's credit is closely related to the task completion, we can calculate the local credit and the foreign credit by

$$user\_localcredit = \beta \times localtask\_completion, \tag{4}$$

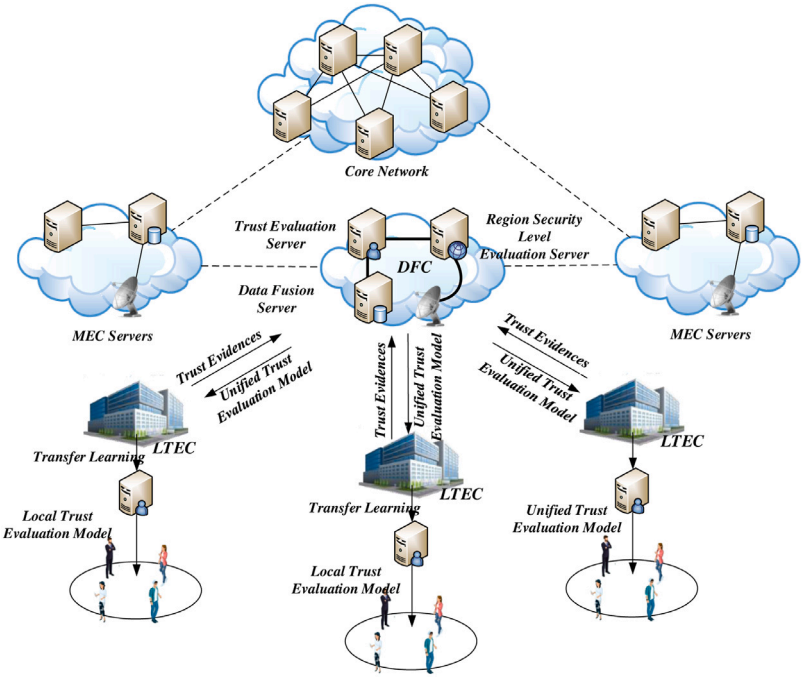

Fig. 1. The system model of the proposed DFTE.

$$user\_foreigncredit = (1-\beta)\times foreigntask\_completion, 0<\beta<1. \quad (5)$$

In this paper, either the local task completion or the foreign task completion of a user is measured by the data reliability $data\_reliability$ provided by the user. Once the user accepts a task, only when he provides reliable data that make either $localtask\_completion$ or $foreigntask\_completion$ reach a certain threshold, can it be considered as qualified to complete the task, then the user's credit will increase. In order to punish a malicious user who provided unreliable data, the user suffered a significant loss in terms of trust level.

4.1.3. User trust calculation

Once the user's credit is obtained, we can evaluate the user's trust $user\_trust$. Considering the case that a area might have a high security level at the beginning and yet ends up with a relative low one, the security level of a specific area is evaluated for the adjustment of users' trusts. In addition, it might be difficult for an honest user within a area of a higher security level to apply for the task with a high trust level constrain, however it is relatively easy for this user to apply for the task of the same trust level constrain in another area of a lower security level. Thereby, we use the security level of each area to dynamically adjust the trust of each user within this area by

$$user\_trust = \frac{user\_credit}{area\_securitylevel}. \quad (6)$$

4.1.4. Dynamic reward–punishment mechanism

Incentive mechanism design should consider rewards/punishment for user trust, that is, users who complete tasks well should be rewarded with trust-enhancing rewards, and malicious users who deliberately sabotage tasks should be severely punished for their trust. Generally speaking, it is a feasible solution to share credit rewards for uncompleted tasks among users who have completed tasks. Since most security problems are caused by malicious users, increasing user trust is much more difficult than reducing trust. Therefore, the reward/punishment for user trust should be implemented based on the trust level of the task, i.e.,

$$user\_trust \leftarrow user\_trust + \zeta \times task\_trustlevel; \quad (7)$$

otherwise, the user's trust drops, i.e.,

$$user\_trust \leftarrow user\_trust - (1-\zeta)\times task\_trustlevel, \quad (8)$$

where $\zeta \le 0.5$.

To sum up, the traditional trust evaluation mechanism is mainly designed based on the trust and task completion of users in a specific area. However, a malicious user in one area may be an honest user in another area. Therefore, all trust evidence should be aggregated to the data fusion center to train a unified trust evaluation model. In order to meet specific granularity requirements, the data fusion center will use DRL algorithms, namely DDPG and DQN, to develop fine-grained trust evaluation and coarse-grained trust evaluation models, respectively.

4.1.5. DRL based granular trust evaluation

In the fine-grained trust evaluation, the DDPG is employed. In DDPG, four networks, namely the critic network Q, the target critic network Q', the actor networks π and the target actor networks π', collaborate to make decisions. And the parameters of these networks are denoted by ϑ^{Q}, $\vartheta^{Q'}$, ϑ^{π} and $\vartheta^{\pi'}$, respectively.

As a DRL, DDPG requires three basic components, i.e., state, action and reward. The action is given at a state to obtain the reward and then the next state is observed from the environment. In the fine-grained trust evaluation, users' trusts consists of the state s. Based on each state, we choose the triple $\langle \alpha, \beta, \zeta \rangle$ as the action a. The reason for that is as follows. Each dimension of the triple determines the scale of impact of a specific factor. Specifically, α represents whether the user's credit values the local credit over the foreign one due to the local credit of a user might be higher than the foreign credit; β reflects the importance of the local task completion considering a user might perform well in local task completion however fails in foreign ones or vice versa; ζ affects the rewards on honest users and the punishments to malicious users in trust value, i.e., if we encourage a user to be an honest one, then ζ should be less than 0.5 to ensure an honest user can have a much higher trust than that of a malicious one. Since the data fusion center aims to find the optimal value for each dimension to accurately evaluate each user's trust, we let each user's trust fall into one of three ranges, i.e., [0, 0.3), [0.3, 0.6), and [0.6, 1] to determine whether the

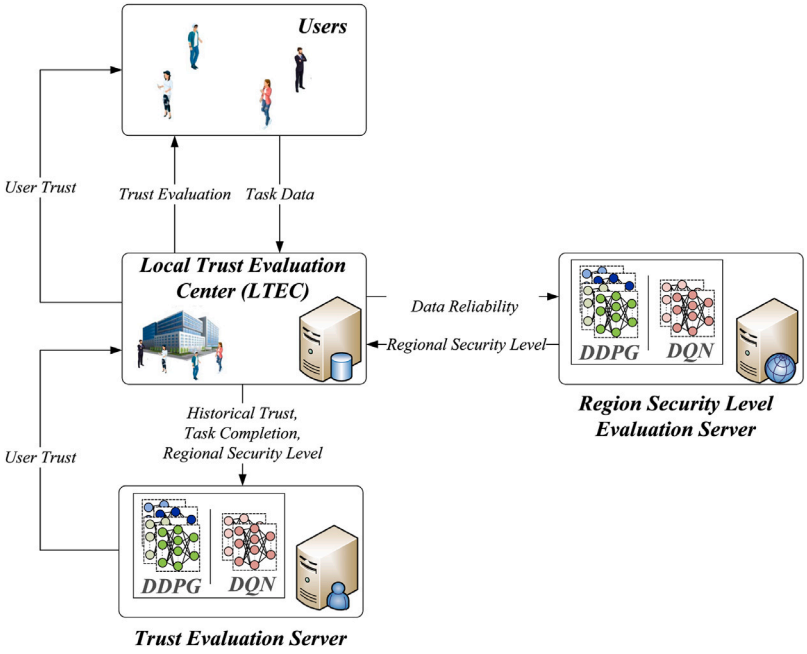

Fig. 2. Granular trust evaluation based on DDPG or DQN.

user is an honest one, a normal one, or a malicious one. Then, we give the reward r by

$$r = \sum_{l} \sum_{m} data\_reliability, \tag{9}$$

where m denotes the number of task posted on each area and then accepted and completed by users, and l represents the number of areas. To maximize the reward r_t in the tth timeslot, the optimal action a_t for each state s_t is given by

$$a_t = \arg\max_{a \in A} Q(s_t, a). \tag{10}$$

Then, experience (s_t, a_t, r_t, s_{t+1}) is stored in experience poor $\mathcal{P}$.

In DDPG's training process, N experiences are randomly sampled from $\mathcal{P}$ to update the critic network utilizing the loss function

$$\mathcal{L}(\vartheta^Q) = \frac{1}{N} \sum_{i}^{N} [Q(s_i, a_i|\vartheta^Q) - \mathcal{Y}_i]^2, \tag{11}$$

where

$$\mathcal{Y}_i = r_i + \gamma(Q(s_{i+1}, \pi(s_{i+1}|\vartheta^{\pi'})|\vartheta^{Q'})), 0 < \gamma < 1. \tag{12}$$

Then, the actor network is updated utilizing policy gradient as

$$\nabla_{\vartheta^\pi} J = \frac{1}{N} \sum_{i}^{N} \left[\nabla_a Q(s, a|\vartheta^Q)|s = s_i, a = \pi(s_i|\vartheta^\pi) \right. \\ \left. \nabla_{\vartheta^\pi} \pi(s|\vartheta^\pi)|s = s_i \right]. \tag{13}$$

Once networks π and Q are updated, the parameters of target networks $\vartheta^{Q'}$ and $\vartheta^{\pi'}$ are updated with a learning rate κ, $0 < \kappa < 1$

$$\vartheta^{Q'} = \kappa\vartheta^Q + (1-\kappa)\vartheta^{Q'}, \tag{14}$$

$$\vartheta^{\pi'} = \kappa\vartheta^\pi + (1-\kappa)\vartheta^{\pi'}. \tag{15}$$

The coarse-grained trust evaluation is implemented by the data fusion center utilizing another DRL algorithm DQN to train the unified trust evaluation model. Similar to DDPG, the DQN still requires three basic components: state, action and reward. The state, action and reward of the DQN are identical to that of the DDPG. However, in coarse-grained trust evaluation, we let each user's trust fall into two ranges, i.e., [0, 0.5) and [0.5, 1] to determine whether the user is an honest one or a malicious one. Specifically, in DQN, a random action a_t in the tth timeslot is chosen with a probability ϵ; otherwise, the action a_t is chosen by

$$a_t = \arg\max_{a \in A} Q(s_t, a; \theta). \tag{16}$$

Then, experience (s_t, a_t, r_t, s_{t+1}) is stored in experience poor $\mathcal{P}'$.

In DQN's training process, we randomly sample minibatch of transitions (s_t, a_t, r_t, s_{t+1}) from $\mathcal{P}'$ to perform the gradient descent using the following loss function on the parameter θ

$$\mathcal{L} = (y_j - Q(s_t, a_t; \theta)^2), \tag{17}$$

where

$$y_j = \begin{cases} r_j, & if\ episode\ terminates\ at\ step\ j+1, \\ r_j + \delta \max_{a'} \hat{Q}(s_{j+1}, a'; \theta^-), 0 < \delta < 1, & otherwise. \end{cases} \tag{18}$$

Then, for each certain number of steps, we set

$$\hat{Q} = Q. \tag{19}$$

The structure of the trust evaluation utilizing DDPG or DQN is given in Fig. 2.

4.2. Transfer learning based user trust evaluation

4.2.1. Fine-grained TL based user trust evaluation

In the fine-grained user trust evaluation, we use TL [23] to construct the trust evaluation model based on DDPG to reduce the training time of the local trust evaluation model. Specifically, the data fusion center trains DDPG to implement a unified trust evaluation, and then uses the trained DDPG network as an initialization model for local training. That is, the parameters of the hidden layer of the DDPG network of the unified trust evaluation are shared as the initialization of the local trust evaluation. We summarize the TL based user trust evaluation utilizing DDPG in Algorithm 1.

Fig. 3 gives the relevant details about the fine-grained TL based user trust evaluation.

4.2.2. Coarse-grained TL based user trust evaluation

In the Coarse-grained user trust evaluation, we use TL to construct the DQN based trust evaluation model to reduce the model training time. That is, the parameters of the hidden layer of the DQN network

Algorithm 1 User Trust Evaluation using DDPG and TL

Input: Local Trust Evidences,Trust Evidences Collection, actor networks π_1 and $\pi_1^{'}$ and critic networks Q_1 and $Q_1^{'}$ of DDPG network 1, actor networks π_2 and $\pi_2^{'}$ and critic networks Q_2 and $Q_2^{'}$ of DDPG network 2, states and actions of DDPG network 1 and 2
Output: User Trust Evaluation Model using DDPG and TL
for $Episode = 1, T_{max}$ **do**
for $t = 1, T$ **do**
An action is chosen using $\pi_1(s_t|\vartheta^{\pi_1})$
Reward r_t is calculated using (9) and next state s_{t+1} is observed after Executing action a_t
Experience poor $\mathcal{P}$ add (s_t, a_t, r_t, s_{t+1})
N experiences are randomly sampled from $\mathcal{P}$
Critic network is updated using (11) and (12)
Actor network is updated using (13)
Target networks are updated using (14) and (15)
end for
end for
Local trust evaluation model (DDPG Network 2) uses the parameters of the unified trust evaluation model (DDPG Network 1)
Start to train the local trust evaluation model (DDPG Network 2)

Algorithm 2 User Trust Evaluation using DQN and TL

Input: Local Trust Evidences,Trust Evidences Collection, action–value function Q with weight θ, target action–value function $\hat{Q}$ with weight $\theta^{-} = \theta$
Output: User Trust Evaluation Model based on DQN and TL
for $Episode = 1, T_{max}$ **do**
for $t = 1, T$ **do**
A random action a_t is chosen with probability ϵ
Otherwise, a_t is selected using (16)
Reward r_t is calculated using (9)and next state s_{t+1} is observed after Executing action a_t
Experience poor $\mathcal{P}^{'}$ add (s_t, a_t, r_t, s_{t+1})
N experiences are randomly sampled from $\mathcal{P}^{'}$
Parameter θ is updated using gradient descent through (17) and (18)
Target net is updated for every C steps using (19)
end for
end for
Local trust evaluation model (DQN Network 2) uses the parameters of the unified trust evaluation model (DQN Network 1)
Start to train the local trust evaluation model (DQN Network 2)

of the unified trust evaluation are shared as the initialization of the local trust evaluation. We summarize the TL based user trust evaluation utilizing DQN in Algorithm 2.

Fig. 4 gives the relevant details about the coarse-grained TL based user trust evaluation.

5. Performance evaluation

5.1. Simulation setup

The simulation is implemented to validate the performance of the proposed strategy DFTE in Python on a computer equipped with Intel Core i7 processor, 64G running memory, CPU frequency 6.4GHZ 64-bit win7 system. We use the similar experimental scenario given in [24]. To be specific, the trust evaluation center publishes the image recognition task. If the user's trust is higher than the task's trust level constrain, then the user can accept the task and complete the task through federated learning. The trust evaluation center evaluates the

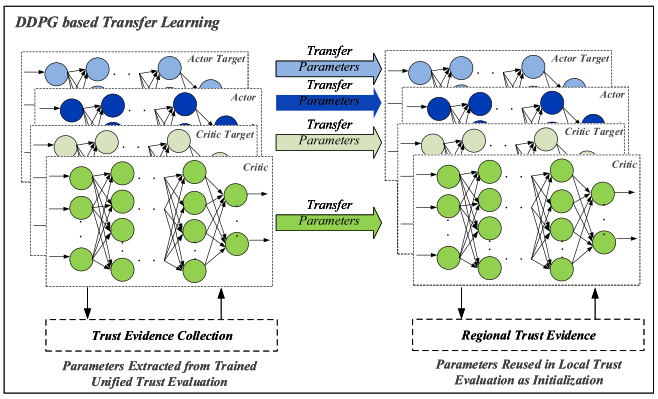

Fig. 3. TL based Fine-grained trust evaluation utilizing DDPG.

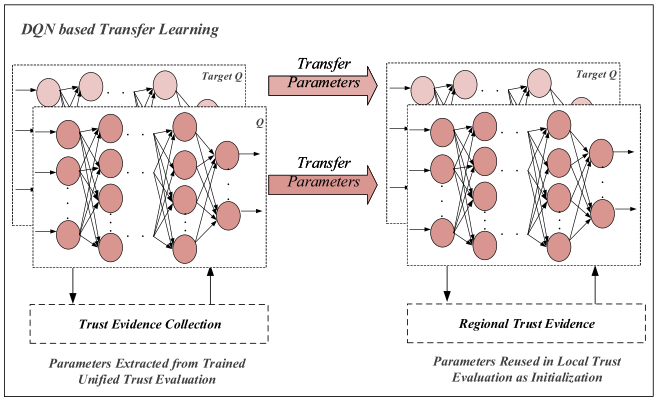

Fig. 4. TL based Coarse-grained trust evaluation utilizing DQN.

user's trust by measuring the accuracy of the model provided by the user. In order to distinguish users with different capabilities, we let each user have a part of images of the Mnist [25] dataset. In addition, in order to achieve the transferability of the trust evaluation model between different areas, we set the number of areas with resemblances equals to 10. The number of users are varying from 50 to 300 as that of the tasks. We let all users have the same initial trust value, and give each task a trust level constrain. In the DRL based trust evaluation, the discount factors γ and δ are set to 0.9 and 0.7 respectively, while the learning rate κ is set to 0.1.

5.2. Performance metrics

We validate the performance of DFTE by comparing with baseline approaches BSDA [26] and BPDC [27] in terms of trust evaluation accuracy, data reliability and participation rate, while considering different number of tasks and users, respectively.

- *Trust Evaluation Accuracy*: Both false alarm rate (FAR) and miss detection rate (MDR) consist of the trust evaluation accuracy.
- *Data Reliability*: The deviation between the provided data and the reference is used to measure the data reliability.
- *Participation Rate*: The percentage of users who participate the data fusion tasks.

Note that although both BSDA and BPDC can evaluate user's trust in the task release scenario, they cannot meet different granular demands on trust evaluation. In addition, they do not combine the dynamic reward and punishment mechanism with the trust evaluation, which will affect the participation rate and the data reliability.

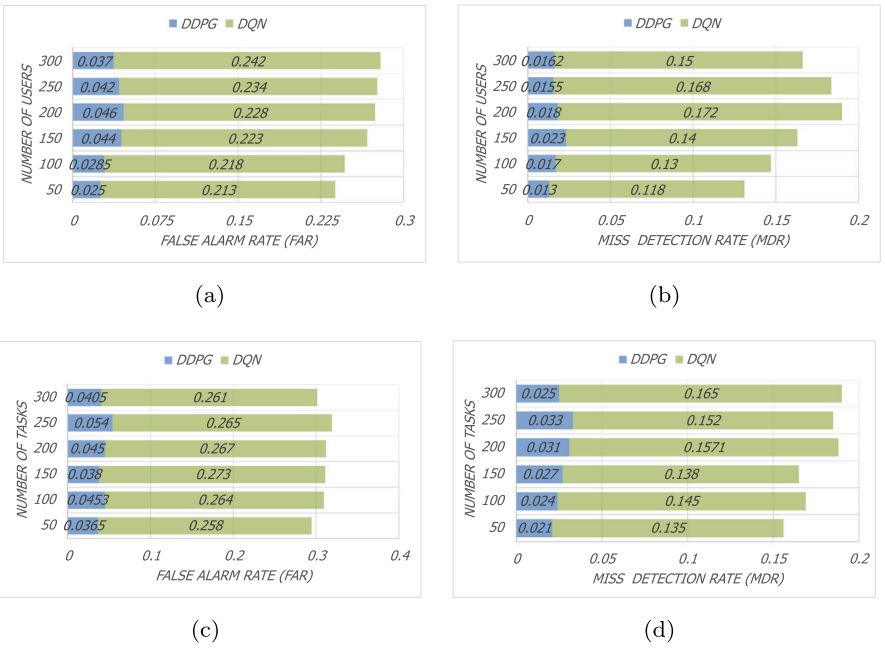

Fig. 5. False Alarm Rate (FAR) and Miss Detection Rate (MDR), while varying number of users.

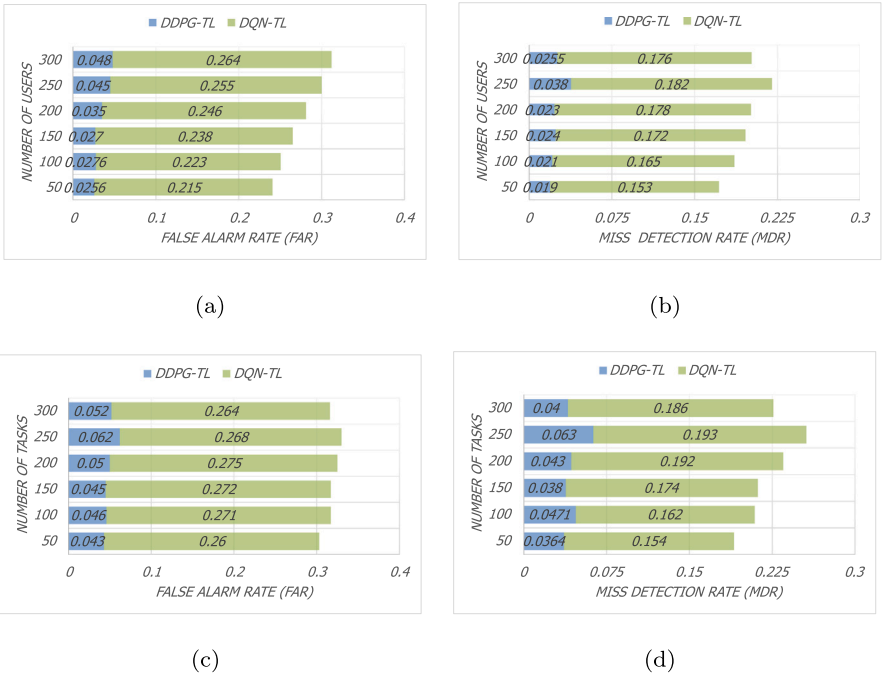

Fig. 6. False Alarm Rate (FAR) and Miss Detection Rate (MDR), while varying number of tasks.

5.3. Experiment results

5.3.1. Trust evaluation accuracy

As shown in Fig. 5, we find that as the number of users grows, the trust evaluation based on DDPG reaches 3.7% FAR and 1.7% MDR, while the trust evaluation based on DQN has higher FAR and MDR which are 22.3% and 14.6% respectively on average. In addition, as the number of tasks increases, the trust evaluation based on DDPG reaches 4.3% FAR and 2.7% MDR, while the trust evaluation based on DQN has higher FAR and MDR which are 26.5% and 14.9% respectively on average. The reason is as follows. Whether the user accepts the task depends on the security level and credit reward of the task. In the initial stage, the user's credibility is low and can only receive low-level tasks. Due to the limited number of tasks, the samples required for trust evaluation are insufficient, resulting in low evaluation accuracy. With the increase in the number of users, users can obtain higher credit through rewards and punishments based on completing more low-level tasks, so that they can accept high-level tasks. This makes the trust evaluation model to be trained on sufficient trust evidence. Therefore, the accuracy of trust evaluation is improved. In addition, compared to DQN-based credit evaluation, DDPG-based trust evaluation can achieve fine-grained user credit evaluation. This avoids the problem of insufficient trust evidence due to the user's inability to complete high-level tasks, which reduces the credit rating and thus cannot receive low-level tasks.

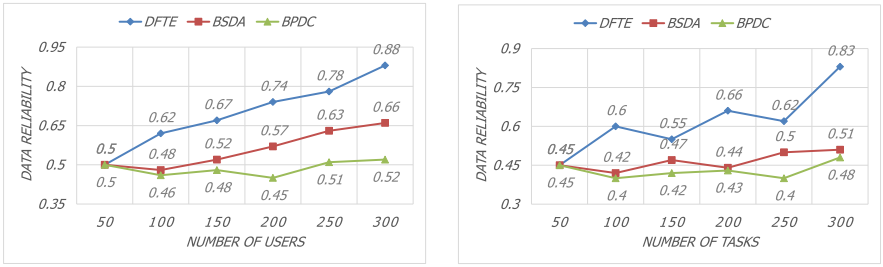

Fig. 7. Data reliability, while varying number of users and number of tasks.

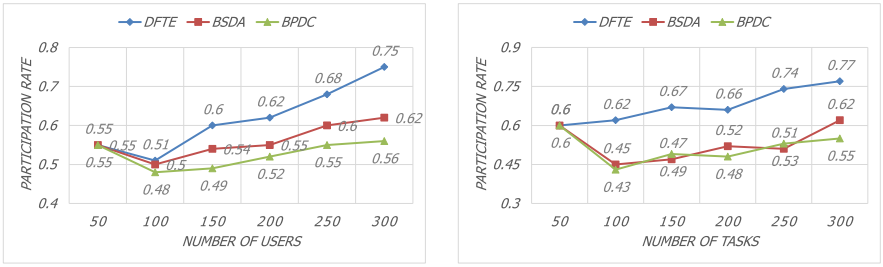

Fig. 8. Participation rate, while varying number of users and number of tasks.

As shown in Fig. 6, as the number of users increases, the trust evaluation based on DDPG and TL reaches 4.8% of FAR and 2.55% of MDR, while the trust evaluation based on DQN and TL has 24% of FAR and 17.1% of MDR. Moreover, with the increase in the number of tasks, the trust evaluation based on DDPG and TL reached 5.2% of FAR and 4% of MDR on average, while the trust evaluation based on DQN and TL has 26.8% of FAR and 17.6% of MDR. The reason is as follows. We introduce transfer learning to reduce model training time. Using a unified credit evaluation model for initialization in the training process of the local credit evaluation model through the transfer learning method between similar areas, not only can greatly reduce the model training time, but the accuracy of the credit evaluation model can also be guaranteed.

5.3.2. Data reliability

As shown in Fig. 7(a), we know that the data reliability of all strategies increases as the number of users increases. The proposed DFTE achieves the highest data reliability, up to 88%, while BSDA and BPDC are 66% and 52%, respectively. The reason is as follows. Honest users will accept the task if their trust reaches the trust level of the task. Since the proposed DFTE uses machine learning to dynamically adjust data reliability factors and trust evaluation criteria to reward honest users and punish malicious users, DFTE defeats BSDA and BPDC in terms of the highest data reliability for any number of users. In Fig. 7(b), it is obvious that the proposed DFTE performs better than the baseline strategy, that is, as the number of tasks increases, the data reliability of DFTE is about 62% on average, compared to 53% of BSDA and 43% of BPDC. The reason is as follows. If all tasks are completed reliably, more tasks will bring more credit rewards. However, some users may not be able to complete the tasks they accept, so trust rewards and punishments will be shared by other users who complete the tasks, and these users can apply for more tasks.

5.3.3. Participation rate

Observing from Fig. 8(a) and Fig. 8(b), we find that the number of users and the number of tasks have similar effects on the participation rate. For example, as the number of users grows, the participation rate fluctuates. The highest participation rate of DFTE is as high as 75%, while the participation rates of BSDA and BPDC are both lower than 65%. On the other hand, as the number of tasks increases, DFTE has a higher participation rate of 77%, while both BSDA and BPDC are lower than 65%. There is no doubt that the proposed DFTE is superior to the baseline strategy. The reason is as follows. Once users complete their tasks well, they can obtain credit rewards with a scale dynamically adjusted using the DRL algorithm. By continuously and reliably completing tasks, additional trust enhancement can enable users to be rated as honest users, so that they can apply for tasks with higher trust constraints. Compared with DFTE, neither BSDA nor BPDC can provide accurate trust assessment or dynamically adjusted rewards/penalties. In general, whether it is BSDA or BPDC, when considering different numbers of users or tasks, the participation rate is nearly 10% lower than that of DFTE.

6. Conclusion

The development of big data, edge computing, and smart terminal technologies promotes the rapid development of IoT applications, and generates a large number of valuable data. However, in the Internet of Things, users usually lack security protection and are susceptible to multiple attacks, especially internal attacks such as privacy attacks and data reliability. As a result, the results of data analysis are quite different from the actual situation, which ultimately affects the application of the Internet of Things. To overcome these problems, in this paper, a Data Fusion and transfer learning empowered granular Trust Evaluation mechanism (DFTE) is proposed. In DFTE, time–space empowered fine/coarse grained trust evaluation models is built based on DRL algorithms, i.e., DDPG and DQN, to implement the different granularity trust evaluation. And then, to prevent privacy leakage and task sabotage, a DRL based dynamic reward punishment mechanism is developed by dynamically adjusting the reward and punishment scale for accurate evaluation on users' trusts. Experimental results show that the proposed DFTE achieves high accuracy of trust evaluation under different granular demands through efficient data fusion, and it performs excellently in user participation rate and data reliability.

CRediT authorship contribution statement

Hui Lin: Conceptualization, Methodology, Software. **Sahil Garg:** Data curation, Writing – original draft. **Jia Hu:** Visualization, Investigation. **Xiaoding Wang:** Writing. **Md. Jalil Piran:** Software, Validation. **M. Shamim Hossain:** Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors extend their appreciation to the Researchers Supporting Project number (RSP-2021/32), King Saud University, Riyadh, Saudi Arabia for funding this work.

References

[1] C. Brewster, I. Roussaki, N. Kalatzis, K. Doolin, K. Ellis, IoT in agriculture: Designing a europe-wide large-scale pilot, IEEE Commun. Mag. 55 (9) (2017) 26–33.
[2] J. Sengupta, S. Ruj, S.D. Bit, A comprehensive survey on attacks, security issues and blockchain solutions for IoT and iIoT, J. Netw. Comput. Appl. 149 (2020) 102481.
[3] W. Ding, X. Jing, Z. Yan, L.T. Yang, A survey on data fusion in internet of things: Towards secure and privacy-preserving fusion, Inf. Fusion 51 (2019) 129–144.
[4] M.B.M. Noor, W.H. Hassan, Current research on Internet of Things (IoT) security: A survey, Comput. Netw. 148 (2019) 283–294.
[5] A. Sharma, E.S. Pilli, A.P. Mazumdar, P. Gera, Towards trustworthy Internet of Things: A survey on trust management applications and schemes, Comput. Commun. 160 (2020) 475–493.
[6] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for Internet of Things, J. Netw. Comput. Appl. 42 (2014) 120–134.
[7] W. Najib, S. Sulistyo, Widyawan, Survey on trust calculation methods in Internet of Things, Procedia Comput. Sci. 161 (2019) 1300–1307.
[8] T. Meng, X. Jing, Z. Yan, W. Pedrycz, A survey on machine learning for data fusion, Inf. Fusion 57 (2020) 115–129.
[9] S.J. Pan, Q. Yang, A survey on transfer learning, IEEE Trans. Knowl. Data Eng. 22 (10) (2010) 1345–1359.
[10] Q.I.U. Han, Q.I.U. Meikang, L.U. Zhihui, G. Memmi, An efficient key distribution system for data fusion in V2X heterogeneous networks, Inf. Fusion 50 (2019) 212–220.
[11] J. Liang, M. Zhang, V.C. Leung, A reliable trust computing mechanism based on multisource feedback and fog computing in social sensor cloud, IEEE Internet Things J. 7 (6) (2020) 5481–5490.
[12] D. Lv, S. Zhu, S, Achieving secure big data collection based on trust evaluation and true data discovery, Comput. Secur. 96 (2020) 101937.
[13] T. Wang, Y. Li, W. Fang, W. Xu, J. Liang, Y. Chen, X. Liu, A comprehensive trustworthy data collection approach in sensor-cloud system, IEEE Trans. Big Data (2021) http://dx.doi.org/10.1109/TBDATA.2018.2811501.
[14] J. Yu, K. Wang, P. Li, R. Xia, S. Guo, M. Guo, Efficient trustworthiness management for malicious user detection in big data collection, IEEE Trans. Big Data. http://dx.doi.org/10.1109/TBDATA.2017.2761386.
[15] Y. Gao, X. Li, J. Li, Y. Gao, S.Y. Philip, Info-trust: A multicriteria and adaptive trustworthiness calculation mechanism for information sources, IEEE Access 7 (2019) 13999–14012.
[16] X. Yao, X. Zhang, H. Ning, P. Li, Using trust model to ensure reliable data acquisition in VANETs, Ad Hoc Netw. 55 (2017) 107–118.
[17] Y. Tang, S. Tasnim, N. Pissinou, S.S. Iyengar, A. Shahid, Reputation-aware data fusion and malicious participant detection in mobile crowdsensing, in: 2018 IEEE International Conference on Big Data, Big Data, IEEE, pp. 4820–4828.
[18] X. Chen, Y. Yuan, L. Lu, J. Yang, A multidimensional trust evaluation framework for online social networks based on machine learning, IEEE Access 7 (2019) 175499–175513.
[19] H. El-Sayed, H.A. Ignatious, P. Kulkarni, S. Bouktif, Machine learning based trust management framework for vehicular networks, Veh. Commun. 25 (2020) 100256.
[20] G.C. Karmakar, R. Das, J. Kamruzzaman, IoT sensor numerical data trust model using temporal correlation, IEEE Internet Things J. 7 (4) (2019) 2573–2581.
[21] H. Mayadunna, L. Rupasinghe, A trust evaluation model for online social networks, in: 2018 National Information Technology Conference, NITC, IEEE, 2018, pp. 1–6.
[22] W. Yuji, The trust value calculating for social network based on machine learning, in: 2017 9th International Conference on Intelligent Human–Machine Systems and Cybernetics, Vol. 2, IHMSC, IEEE, 2017, pp. 133–136.
[23] Q. Chen, Z. Zheng, C. Hu, D. Wang, F. Liu, On-edge multi-task transfer learning: Model and practice with data-driven task allocation, IEEE Trans. Parallel Distrib. Syst. 31 (6) (2020) 1357–1371, http://dx.doi.org/10.1109/TPDS.2019.2962435.
[24] W. Liu, et al., D2MIF: A malicious model detection mechanism for federated learning empowered artificial intelligence of things, IEEE Internet Things J. (2021) http://dx.doi.org/10.1109/JIOT.2021.3081606.
[25] Y. Lecun, L. Bottou, Y. Bengio, P. Haffner, Gradient-based learning applied to document recognition, Proc. IEEE 86 (11) (1998) 2278–2324.
[26] X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu, M.S. Hossain, A secure data aggregation strategy in edge computing and blockchain empowered internet of things, IEEE Internet Things J. (2021) http://dx.doi.org/10.1109/JIOT.2020.3023588.
[27] H. Lin, S. Garg, J. Hu, G. Kaddoum, M. Peng, M.S. Hossain, A blockchain-based secure data aggregation strategy using 6g-enabled nib for industrial applications, IEEE Trans. Ind. Inf. (2021) http://dx.doi.org/10.1109/TII.2020.3035006.