PPCS: An Intelligent Privacy-Preserving Mobile-Edge Crowdsensing Strategy for Industrial IoT

Xiaoding Wang, Sahil Garg, *Member, IEEE*, Hui Lin, Georges Kaddoum, Jia Hu, and M. Shamim Hossain, *Senior Member, IEEE*

***Abstract*—Mobile-edge crowdsensing is capable of providing a large amount of data via pervasive mobile terminals for Industrial Internet of Things (IIoT). However, the generated data often contain users' sensitive information, which suggests the significance of privacy preserving in data aggregation and analysis for IIoT. Privacy preserving in mobile-edge crowdsensing have conflicting objectives, i.e., the edge fusion center (FC) requires data of better quality for data fusion with higher accuracy whereas participatory users (PUs) desire better privacy preserving by larger noise injection. Therefore, how to select proper noises to achieve the tradeoff between accuracy and privacy is a challenging problem. In addition, FC is subject to data tempering due to the lack of data reliability validations and incentive mechanisms. To tackle these problems, we propose a novel privacy-preserving mobile-edge crowdsensing strategy (PPCS) for IIoT. Specifically, PPCS provides a Kullback–Leibler privacy-preserving data aggregation using a reputation-based incentive mechanism. On the other hand, PPCS offers hypothesis test-based data reliability validation and PU's reputation update, which collaborate to ease the impact of tampered data. Meanwhile, a reinforcement learning algorithm, the expected Sarsa, is applied to obtain the optimal test threshold. Theoretical analysis and experimental results show that PPCS is an energy-efficient strategy and the data provided by PPCS has a better aggregation accuracy than certain baseline strategies.**

***Index Terms*—Crowdsensing, edge computing, industrial Internet of Things (IIoT), privacy preserving, reinforcement learning (RL).**

Manuscript received June 7, 2020; revised August 8, 2020 and September 13, 2020; accepted October 8, 2020. Date of publication October 21, 2020; date of current version June 23, 2021. This work was supported by the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, through the Vice Deanship of Scientific Research Chairs: Chair of Pervasive and Mobile Computing. *(Corresponding authors: Hui Lin; Jia Hu.)*

Xiaoding Wang and Hui Lin are with the College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, China (e-mail: wangdin1982@fjnu.edu.cn; linhui@fjnu.edu.cn).

Sahil Garg is with the Electrical Engineering Department, École de technologie supérieure, Montreal, QC H3C 1K3, Canada (e-mail: sahil.garg@ieee.org).

Georges Kaddoum is with the Department of ECE, École de technologie supérieure, Montreal, QC H3C 1K3, Canada (e-mail: georges.kaddoum@etsmtl.ca).

Jia Hu is with the Department of Computer Science, University of Exeter, Exeter EX4 4QJ, U.K. (e-mail: j.hu@exeter.ac.uk).

M. Shamim Hossain is with the Chair of Pervasive and Mobile Computing and the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia (e-mail: mshossain@ksu.edu.sa).

Digital Object Identifier 10.1109/JIOT.2020.3032797

I. Introduction

With the rapid development of mobile devices, i.e., smartphone, smartwatch, tablet, etc., the mobile crowdsensing has aroused many interests in Industrial Internet of Things (IIoT). Via edge computing, the public cloud center can employ IoT terminals to obtain useful information [1]. Specifically, the data collected by the terminal devices is integrated by the edge fusion centers (FCs), and the public cloud center can get the aggregated information from the encrypted data of FC. However, FC could be untrustworthy, i.e., compromised by malicious attackers [2]. On the other hand, it is costly for participatory users (PUs) to contribute sensing data to FC that make PUs reluctant in crowdsensing without a compensating mechanism.

To tackle this problem, a number of works have been proposed [3], [4], [14]–[19] based on specific incentive mechanisms. The basic idea of these works is that PUs contribute perturbed data by injecting noise to preserve privacy and FC pays for PUs' privacy loss. However, it immediately raises two other problems: 1) how to select a reasonable amount of noise to preserve desired privacy and 2) how to achieve an efficient data reliability and eventually minimize the impact of tampered data. These problems should be addressed by quantifying the privacy-preserving degree (PPD) first and then simultaneously optimizing aggregation accuracy as well as providing acceptable PPDs for PUs. In fact, designing an incentive mechanism, which ensures honest PUs contributing perturbed private data with respect to (w.r.t.) their PPD to be well compensated by FC, is crucial. That suggests the payment from FC to PUs is somehow related to PUs' reputations, which is obtained from the reliability of their contributed data through an efficient validation process.

This article proposes an efficient reinforcement-learning (RL)-based privacy-preserving mobile-edge crowdsensing strategy (PPCS) for IIoT to solve the above problems. PPCS consists of three important components. The first provides Kullback–Leibler (KL) privacy-preserving data aggregation, which achieves the tradeoff between PPD and aggregation accuracy. The second accounts for data reliability validation. The third is responsible for PU reputation update and corresponding aggregation weight calculation. We summarize the contributions of this article as follows.

1) To achieve privacy-preserving edge crowdsensing for IIoT, the proposed PPCS offers a weighted data aggregation, in which data are perturbed by noise. Especially, the data perturbation is designed based on the KL privacy. Compared with differential privacy, privacy attackers are hard to recognize the original data with samples of highly similar distributions. To solve the noise selection problem, the PPD is quantified and the relation between PPD and aggregation accuracy is obtained. Then, an incentive mechanism is developed to calculate the payment for FC to each PU w.r.t. his/her PPD and reputation as well. Thus, the tradeoff between accuracy and privacy is accomplished.
2) To efficiently validate data reliability and further minimize the impact of tampered data, a hypothesis test is constructed. Since the test accuracy depends on the corresponding threshold, we employ an on-policy RL algorithm, the expected Sarsa, to learn the optimal threshold to detect unreliable data. Based on test results, PUs' reputations are updated to calculate aggregation weights of corresponding data for mitigating the impact of data tampering, i.e., the reliable data provided by an honest PU should be given a significant weight and a relatively low weight is given for unreliable data provided by a malicious PU. As the payment is related to each PU's reputation, malicious PUs will be paid less than honest ones as a punishment. Thus, the quality of the aggregated data should be further improved.
3) Theoretical analysis and experiment results show that the expected Sarsa outperforms Myopic policy and Random policy not only in the convergence rate but in the energy cost as well. That results in an energy-efficient PPCS. More importantly, the weighted average of aggregated data calculated by PPCS has a better aggregation accuracy than that of the average obtained by two other privacy-preserving data aggregation strategies PPCC [3] and REAP [4].

The remainder of this article is organized as follows. Related work is covered in Section II. We introduce the system model in Section III. The details of the proposed strategy PPCS are elaborated in Section IV. The experiments are presented in Section V. We conclude this article in Section VI.

II. Related Work

There has been a growing research interest in privacy-preserving mobile-edge crowdsensing. Zhao *et al.* [5] achieved the reputation management of privacy preserving and the prevention of users' malicious behaviors. In [6], a crowdsensing mechanism utilizing the dubbed blockchain is developed for location privacy protection. Shen *et al.* [7] integrated the machine learning and the blockchain for privacy-preserving mechanism design. Liang *et al.* [8] utilized the deep learning (DL) on embedded sensors to protect users' privacy. In [9], the data trustworthiness is introduced to design the crowdsensing mechanism of enhanced privacy against internal attacks. In [10], a framework that aims to achieve the tradeoff between guaranteeing system stability and minimizing data aggregation error w.r.t. the participants' privacy, the sensing task randomness, and the cost of the platform. Xiong *et al.* [11] studied the privacy-preserving crowdsensing problem in industrial IoT. Then, they [12] adopt machine learning and game theory to achieve data privacy in mobile-edge crowdsensing. In [13], a mobile-edge crowdsensing based on the blockchain is developed to verify data and design a dynamic incentive mechanism.

Plenty of incentive mechanisms have been proposed in mobile-edge crowdsensing for privacy preserving. Wang *et al.* [3] proposed the PPCC to compute the average for heterogeneous privacy preserving. Zhang *et al.* [4] designed a contract incentive REAP to pay for PUs' privacy losses with a limited budget. In [14], the privacy preference is introduced for the incentive mechanism design. In [15], the participation level is considered to design incentive utilizing the Stackelberg game. In [16], the programming of multiple stages is employed for users' participation motivation. In [17], both deep RL and Stackelberg game are adopted in the incentive mechanism design. In [18], the time varying demands on privacy preserving and the Q learning are adopted for dynamic pricing. In [19], a payment-PPD game is formulated to decide the payment w.r.t. different PPDs, where the Q learning is employed.

Although these works contribute to privacy-preserving mobile-edge crowdsensing, there still remain two challenges: 1) how to select proper noise to preserve desired privacy and 2) how to accomplish a highly efficient data reliability validation to ease the impact of tampered data. In this article, a novel RL-based PPCS is proposed for IIoT to address these two problems.

III. System Model

In this article, we consider the mobile-edge crowdsensing system, which is composed of a single fusion center FC and a number of PUs $V = \{v_1, v_2, \ldots, v_N\}$ (see Fig. 1). All N PUs contribute data, $X = \{x_1, x_2, \ldots, x_N\}$, to the FC, where $x_i \in R$ is a real number. Inspired by [20] and [21], we rate each PU v_i as either a honest one, the normal one, or the malicious one w.r.t. v_i's normalized reputation $r_i \in [0, 1]$ as shown in Table I. Then, the FC calculates the average, i.e., $y = (1/N) \sum_{i=1}^{N} x_i$. The data contributed by PUs is further analyzed for IIoT applications. For example, in healthcare, PUs' daily exercise data are collected by FC and average aggregation is conducted for public health monitoring. Since PUs provide sensitive information, there exist some threats against PUs' privacy [22].

A. Threat Model

An untrusted FC is considered in this article. In addition, there exist two types of PUs. One are honest while the others are malicious. That implies two types of threats should be considered. The first one is the deterioration of the quality of aggregated data [23]. Unlike honest PUs, malicious ones may upload tampered data to reduce the usability of the aggregated result. The second one is privacy compromise, i.e., FC may try to infer the private information from uploaded data,

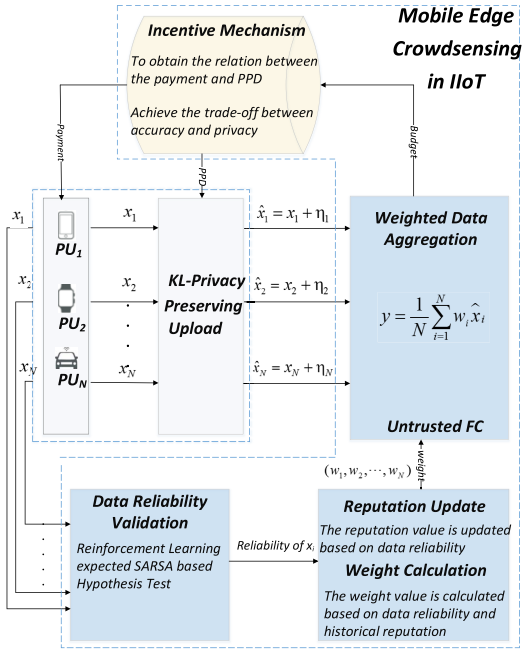


Fig. 1. Illustration of the proposed PPCS for mobile-edge crowdsensing in IIoT.

TABLE I
PU REPUTATION RATING

Reputation Range	*Rank*
[0, 0.3)	Malicious
[0.3, 0.6)	Normal
[0.6, 1)	Honest

sophisticated malicious attackers might launch eavesdropping attack, etc.

B. KL-Privacy

Due to the privacy concern, each PU uploads perturbed data instead of the raw one. In order to quantify the PPD, the KL privacy, developed from differential privacy, is employed. In general, data perturbation is implemented w.r.t. the KL divergence by adding original data with noise to measure PPDs [24].

Definition 1 [25]: The α-adjacent, $\alpha \geq 0$, of two vectors x and $x' \in R^n$ is defined as

$$|x_i - x_i'| \leq \begin{cases} \alpha, & \text{if } i = i_0 \\ 0, & \text{if } i \neq i_0. \end{cases}$$

Definition 2 [24]: For any pair of α-adjacent vectors x and x', we define the ε-KL privacy through a randomized function $\mathcal{M}(x) : R^n \to R$ as

$$\frac{\mathcal{D}_K\left[\mathcal{P}_{\mathcal{M}(x)} || \mathcal{P}_{\mathcal{M}(x')}\right] + \mathcal{D}_K\left[\mathcal{P}_{\mathcal{M}(x')} || \mathcal{P}_{\mathcal{M}(x)}\right]}{2} \leq \varepsilon$$

where the pdf of $\mathcal{M}(x)$ and $\mathcal{M}(x')$ is denoted by $\mathcal{P}_{\mathcal{M}(x)}$ and $\mathcal{P}_{\mathcal{M}(x')}$, respectively; the KL divergence of $\mathcal{P}_1$ w.r.t. $\mathcal{P}_2$ is represented by $\mathcal{D}_K[\mathcal{P}_1||\mathcal{P}_2]$; and the PPD provided by $\mathcal{M}(x)$ is denoted by ε.

A randomized function $\mathcal{M}$ preserves the ε-KL privacy if $\mathcal{M}$ preserves the ε-differential privacy [24].

C. Aggregation Model

Both privacy model and threat model suggest the weighted average is a better alternative to ease the impact of tampered data. Thus, the aggregated data y^k is calculated utilizing the data of the ith PU in the kth time x_i^k and the corresponding weight w_i^k as

$$y^k = \sum_{i=1}^{N} w_i^k x_i^k \tag{1}$$

where w_i^k is calculated by (28).

IV. PROPOSED STRATEGY

The proposed PPCS consists of three important components, each of which is responsible for 1) KL privacy-preserving data aggregation; 2) data reliability validation; and 3) PU reputation update and aggregation weight calculation, respectively.

A. KL-Privacy-Preserving Data Aggregation

Each PU v_i adds original data x_i a Gaussian noise η_i due to privacy concern, i.e.,

$$\tilde{x}_i = x_i + \eta_i$$

where $\eta_i \sim N(0, \sigma^2)$. Thus, we can rewrite (1) as

$$\hat{y}^k = \sum_{i=1}^{N'} w_i^k \tilde{x}_i^k \tag{2}$$

where N' denotes the number of reliable ones among N uploaded data.

Note that the noise perturbation in (2) is implemented utilizing a randomized function $M(.) : R \to R$ to data x_i, i.e., $\tilde{x}_i = M(x_i) = x_i + \eta_i$. Cuff and Yu [24] proved that if $\eta_i \sim N(0, (\sigma_i)^2)$ then the randomized function $M(x_i)$ preserves the ε_i-KL privacy for x_i, where $(\sigma_i)^2 = (\alpha^2/2\varepsilon_i)$. Compared with differential privacy [26], privacy attackers are hard to recognize the original data with samples of highly similar distributions. However, the noise perturbation process brings about another problem which is how to achieve the tradeoff between accuracy and privacy. To address this problem, we first define the aggregation accuracy radius γ.

Definition 3: The deviation γ from the true average $\bar{y}$ to the computation result $\hat{y}$ is defined as the aggregation accuracy radius

$$\gamma = |y - \hat{y}|.$$

That implies the smaller γ the better aggregation accuracy. For PU v_i, if the weight w_i and the PPD ε_i are given, then we can obtain the aggregation accuracy radius γ with Theorem 1.

Theorem 1: The computation result $\hat{y}$ converges to the true average $\bar{y}$ within γ for any $p \in (0, 1)$ as

$$\gamma = \frac{\alpha}{\sqrt{1-p}} \sqrt{\sum_{i=1}^{N'} \left(w_i^k\right)^2 \frac{1}{\varepsilon_i}}.$$

Proof: Consider the aggregated data without perturbation noise

$$y = \sum_{i=1}^{N'} w_i x_i$$

and the perturbed one

$$\hat{y} = \sum_{i=1}^{N'} w_i^k (x_i + \eta_i) = y + \sum_{i=1}^{N'} w_i^k \eta_i.$$

Since $\mathrm{Var}(\eta_i) = 2\sigma_i^2$, we obtain

$$\mathrm{Var}\left(\sum_{i=1}^{N'} w_i^k \eta_i\right) = 2\sum_{i=1}^{N'} \left(w_i^k\right)^2 \sigma_i^2.$$

For $\forall \gamma > 0$, utilizing Chebyshev's inequality yields

$$\Pr\left[|\hat{y} - y| \geq \gamma\right] \leq \frac{2}{\gamma^2} \sum_{i=1}^{N'} \left(w_i^k\right)^2 \sigma_i^2. \tag{3}$$

Substituting $\Pr[|\hat{y} - y| < \gamma] = p$ into (3) yields

$$\frac{2}{\gamma^2} \sum_{i=1}^{N'} \left(w_i^k\right)^2 \sigma_i^2 = 1 - p.$$

Then, it follows that:

$$\gamma = \frac{\sqrt{2}}{\sqrt{1-p}} \sqrt{\sum_{i=1}^{N'} \left(w_i^k\right)^2 \sigma_i^2}. \tag{4}$$

Substituting $\sigma_i^2 = (\alpha^2 / 2\varepsilon_i)$ into (4) yields

$$\gamma = \frac{\alpha}{\sqrt{1-p}} \sqrt{\sum_{i=1}^{N'} \left(w_i^k\right)^2 \frac{1}{\varepsilon_i}}.$$

■

On the other hand, although the noise perturbation provides data privacy, both privacy cost and rationality constraint affect privacy and accuracy as well.

Definition 4 [27]: The privacy cost c_i of each PU v_i is defined as

$$c_i = \mu_i (\varepsilon_i)^2$$

where the cost parameter μ_i is a nonnegative real number.

It is obvious that if v_i values his/her privacy more than he/she might set a larger μ_i with a fixed ε_i.

Definition 5 [27]: The rationality constraint is defined as the relation between the payment pa_i and a PPD ε_i of the following form:

$$pa_i - \mu_i (\varepsilon_i)^2 \geq 0 \quad \forall i \in [1, N].$$

A rational PU v_i must report perturbed data w.r.t. PPD ε_i, only if he/she receives a reasonable payment pa_i as expected.

Observed from Theorem 1, we know that to minimize γ we should obtain the minimum $\sum_{i=1}^{N} ([(w_i^k)^2]/\varepsilon_i)$. In addition, the FC is assumed to have a budget B to cover the payment for PUs' privacy loss. Then, we design an *incentive mechanism* based on the following optimization problem w.r.t. privacy cost and rationality constraint in order to find the optimal ε_i and the optimal pa_i for the tradeoff between accuracy and privacy.

Problem 1:

$$\begin{aligned} \min_{\varepsilon_i, pa_i} \ & \sum_{i=1}^{N'} \frac{\left(w_i^k\right)^2}{\varepsilon_i} \\ \text{s.t.} \ & pa_i - \mu_i (\varepsilon_i)^2 \geq 0, \ \ i \in \left[1, N'\right] \\ & \sum_{i=1}^{N'} pa_i \leq B \\ & pa_i \geq 0, \varepsilon_i > 0. \end{aligned}$$

The following theorem is given for solving the above optimization problem. Thus, each PU uploads perturbed data based on the optimal solution to Problem 1, which is given in (5) and (6) of Theorem 2.

Theorem 2: Problem 1's optimal solution is

$$\varepsilon_i^* = \sqrt{\frac{\left(w_i^k\right)^2 (\mu_i)^{-\frac{2}{3}}}{\sum_{j=1}^{N'} \left(w_j^{k-1}\right)^2 \left(\mu_j\right)^{\frac{1}{3}}} B} \tag{5}$$

$$pa_i^* = \frac{\left(w_i^k\right)^2 (\mu_i)^{\frac{1}{3}}}{\sum_{j=1}^{N'} \left(w_j^{k-1}\right)^2 \left(\mu_j\right)^{\frac{1}{2}}} B. \tag{6}$$

Proof: Recall that $\sum_{i=1}^{N'} \mu_i \varepsilon_i^2 = pa_i$. Thus, we have

$$\sum_{i=1}^{N'} \mu_i \varepsilon_i^2 = B. \tag{7}$$

We optimize Problem 1 by introducing the Lagrangian $L : R^N \times R \to R$ first as

$$L(\varepsilon_i, \lambda) = \sum_{i=1}^{N'} \left(w_i^k\right)^2 \frac{1}{\varepsilon_i} + \sum_{i=1}^{N'} \lambda \left(\mu_i \varepsilon_i^2 - B\right)$$

where the Lagrange multiplier is denoted by λ. Then, we take the derivatives of L for optimal ε_i discovery as

$$\frac{\partial \mathcal{L}}{\partial \varepsilon_i} = -\frac{\left(w_i^k\right)^2}{\varepsilon_i^2} + 2\lambda \mu_i \varepsilon_i = 0$$

which yields

$$\varepsilon_i = \left(\frac{\left(w_i^k\right)^2}{2\lambda \mu_i}\right)^{\frac{1}{3}}. \tag{8}$$

Substituting (8) into (7), we obtain

$$\left(\frac{1}{2\lambda}\right)^{\frac{2}{3}} = \frac{1}{\sum_{i=1}^{N'} \left(w_i^k\right)^2 (\mu_i)^{\frac{1}{3}}} B.$$

Then, it follows that:

$$\varepsilon_i^* = \sqrt{\frac{\left(w_i^k\right)^2 (\mu_i)^{-\frac{2}{3}}}{\sum_{j=1}^{N'} \left(w_j^k\right)^2 \left(\mu_j\right)^{\frac{1}{3}}} B} \tag{9}$$

$$pa_i^* = \frac{\left(w_i^k\right)^2 (\mu_i)^{\frac{1}{3}}}{\sum_{j=1}^{N'} \left(w_j^k\right)^2 \left(\mu_j\right)^{\frac{1}{2}}} B. \tag{10}$$

■

In fact, Theorem 2 provides the solution to the problem that how much the FC should pay for the privacy loss of the PU. That suggests each PU only provides a perturbed data based on his/her privacy-preserving degree. Without the perturbation noise, the FC is not able to restore the original data from the perturbed one no matter the FC is untrustworthy or not. In addition, Theorem 2 is deemed as a reward-and-punishment mechanism. Observed from (9) and (10), we know that the optimal PPD ε_i^* and reward pa_i^* are determined by FC's budget B, cost parameter μ_i, and the number of PUs n. Once FC offers a higher budget B, ε_i^* increases as well as pa_i^*. Thus, each PU reports perturbed data with larger PPD and then receives more payment, which enables the accuracy radius γ to be narrowed down. That indicates increasing budget facilitates aggregation accuracy. On the other hand, ε_i^* decreases as μ_i increases, while pa_i^* increases with μ_i. Recall that the extent of v_i caring about personal privacy is represented by μ_i, i.e., a larger u_i results in more privacy cost for v_i with a specific PPD ε_i. Thus, FC should pay enough for each PU's privacy. Note that the optimal solution can be computed offline due to each PU v_i sends ε_i before data aggregation. Compared with honest PUs, malicious ones should receive less payment as a punishment w.r.t. (10) due to their *bad* reputations. However, such punishment is not permanent, e.g., if a malicious PU v_i starts to upload reliable data to improve his/her reputation r_i then the payment pa_i increases referring to (28). It is worth to mention that Theorem 2 gives a solution to incentive mechanism design under the constraint that the budget B of the FC is limited. However, if the FC owns an unlimited budget B', then the solution given by Theorem 2 still applies. This is because the payment pa_i is given w.r.t. the PPD ε_i for the ith PU. In addition, as for the PUs, who contribute unreliable data, the corresponding payments prepared for whom are shared by those reliable data contributors as a supplement to the incentive mechanism as the further punishment for malicious PUs.

B. Data Reliability Validation

The significance of data reliability validation depends on the quality of data aggregation which is vulnerable to tampered data uploaded by malicious PUs. Thereby, contributing unreliable data is not tolerated. That suggests we should introduce an effective mechanism to facilitate the FC to detect unreliable data as many as possible. To this end, we formulate the data reliability validation into a zero-sum game implemented by a hypothesis test with the optimal test threshold learned by the RL.

1) Data Reliability-Based Hypothesis Test: We denote H_0 as the null hypothesis, i.e., the data are reliable, while the alternative hypothesis H_1 denotes otherwise. Accordingly, we give the false alarm rate (FAR) P_f indicating a reliable data misjudged as an unreliable one as

$$P_f = P(H_1|H_0). \tag{11}$$

Similarly, we give the missing detect rate P_m suggesting an unreliable data is mistaken as a reliable one as

$$P_m = P(H_0|H_1). \tag{12}$$

Then, the test static is constructed as

$$L = ||x_i^k - \hat{x}_i^k||^2. \tag{13}$$

Note that (13) gives the deviation between the input data x_i and the reference one $\hat{x}_i$. Consider the data $x_i = (x_i^1, x_i^2, \ldots, x_i^n)$, the Mahalanobis distance is utilized to calculate the reasonable deviation between x_i and the reference due to the advantage in eliminating the deviations between features. According to (11)–(13), we give the hypothesis test as

$$L \underset{H_1}{\overset{H_0}{\lessgtr}} \theta. \tag{14}$$

Note that if the data are reliable, then the reference $\hat{x}_i^k$ is updated, i.e., $\hat{x}_i^k \leftarrow x_i^k$; otherwise, $\hat{x}_i^k \leftarrow x_i^{k-1}$.

Let C represent the energy costs factor. The gain of receiving a reliable data is denoted by G_1, while the gain of receiving an unreliable data is denoted by G_0 with $G_1 > G_0 > 0$. Let the probability of the malicious attack is denoted by $\mathbf{p}$. Thus, we give the Bayesian risk $R(\theta, \mathbf{p})$ of the data reliability validation under a prior distribution of malicious attacks as

$$\begin{aligned} R(\theta, \mathbf{p}) = &\big(G_1\big(1 - P_f(\theta)\big) - CP_f(\theta)\big)\left(1 - \sum_{i=1}^{N_m} p_i\right) \\ &+ \left(G_0(1 - P_m(\theta)) - CP_m(\theta)\right)\sum_{i=1}^{N_m} p_i. \end{aligned} \tag{15}$$

Let the utility of the FC is denoted by $u_{fc}(\theta, \mathbf{p})$. Thus, we have $u_{fc}(\theta, \mathbf{p}) = R(\theta, \mathbf{p})$.

2) Nash Equilibrium of the Data Reliability Validation Game: The Nash equilibrium of a game suggests the utility of any player will not increase if other strategies rather than the optimal one is chosen. We denote the NE of the data reliability validation game as $(\theta^*, \mathbf{p}^*)$. The threshold θ^* is chosen by the FC for utility $u_{fc}(\theta, \mathbf{p}^*)$ maximization in the data reliability validation, while the malicious PU aims to maximize its utility $u_{mp}(\theta^*, \mathbf{p})$. Therefore, we have

$$\begin{aligned} \theta^* &= \arg\max_{\theta > 0} u_{fc}\big(\theta, \mathbf{p}^*\big) \\ \mathbf{p}^* &= \arg\max u_{mp}\big(\theta^*, \mathbf{p}\big). \end{aligned}$$

Theorem 3: The unique NE of the data reliability validation game is given by

$$\theta^* = s\big(G_1 - G_0 - P_f(\theta)(G_1 + C) + P_m(\theta)(G_0 + C) = 0\big) \tag{16}$$

where

$$\mathbf{p}^* = \frac{1}{1 + e^{-\frac{\lambda}{2}} \frac{G_0 + C}{G_1 + C}\ {}_0\tilde{F}_1\big(1;\ \frac{\theta\lambda}{4}\big)} \tag{17}$$

and the equation is solved by $s(\cdot)$.

Proof: Note that each data uploaded consists of both real part and imaginary part of dimension 2. Thus, we have

$$P_f(\theta) = 1 - F_{\chi_2^2}(\theta) \tag{18}$$

$$P_m(\theta) = F_{\chi_{2,\lambda}^2}(\theta) \tag{19}$$

where $F_{\chi_2^2}(\cdot)$ and $F_{\chi_{2,\lambda}^2}(\cdot)$ are the cumulative distribution function of the chi-square distribution and noncentral chi-square

distribution with a noncentrality parameter λ with 2 degrees of freedom, respectively. Thus, we have $\lim_{\theta\to\infty} P_f(\theta) = 0$, $P_m(0) = 0$, $P_f(0) = 1$, $\lim_{\theta\to\infty} P_m(\theta) = 1$, and

$$\frac{dP_f(\theta)}{d\theta} = -\frac{1}{2}e^{-\frac{\theta}{2}} \tag{20}$$

$$\frac{dP_m(\theta)}{d\theta} = \frac{1}{2}e^{-\frac{\theta+\lambda}{2}}\ {}_0\tilde{F}_1\left(1;\frac{\theta\lambda}{4}\right). \tag{21}$$

By (15), we have

$$\frac{\partial u_{mp}(\theta,\mathbf{p})}{\partial \mathbf{p}} = G_1 - G_0 - P_f(\theta)(G_1 + C) + P_m(\theta)(G_0 + C) \tag{22}$$

indicating that $u_{mp}(\theta,\mathbf{p})$ is a linear function of $\mathbf{p}$. By (22), we have $\partial u_{mp}(0,\mathbf{p})/\partial\mathbf{p} = -G_0 - C < 0$ and $\lim_{\theta\to\infty} \partial u_{mp}(\theta,\mathbf{p})/\partial\mathbf{p} = G_1 + C > 0$. By (20)–(22), we have

$$\frac{\partial^2 u_{mp}(\theta,\mathbf{p})}{\partial\mathbf{p}\partial\theta} = \frac{1}{2}e^{-\frac{\theta}{2}}(G_1 + C) + \frac{1}{2}e^{-\frac{\theta+\lambda}{2}}(G_0 + C)_0\tilde{F}_1\left(1;\frac{\theta\lambda}{4}\right) \geq 0$$

indicating that $\partial u_{mp}(\theta,\mathbf{p})/\partial\mathbf{p}$ increases with θ. As $\partial u_{mp}(0,\mathbf{p})/\partial\mathbf{p} < 0$ and $\lim_{\theta\to\infty} \partial u_{mp}(\theta,\mathbf{p})/\partial\mathbf{p} > 0$, the solution of $\partial u_{mp}(\theta,\mathbf{p})/\partial\mathbf{p} = 0$ denoted by $\hat{\theta}$, which is given by (16), is unique and positive. If $0 \leq \theta \leq \hat{\theta}$, we have $\partial u_{mp}(\theta,\mathbf{p})/\partial\mathbf{p} < 0$; otherwise, we have $\partial u_{mp}(\theta,\mathbf{p})/\partial\mathbf{p} > 0$.

Then, by (15), (20), and (21), we have

$$\frac{\partial u_{fc}(\theta,\mathbf{p})}{\partial\theta} = \frac{1}{2}e^{-\frac{\theta}{2}}\Big[(G_1 + C)(1 - \mathbf{p}) - (G_0 + C)\mathbf{p}e^{-\frac{\lambda}{2}}\ {}_0\tilde{F}_1\left(1;\frac{\theta\lambda}{4}\right)\Big]. \tag{23}$$

As $\partial u_{mp}(\hat{\theta},\mathbf{p})/\partial\mathbf{p} = 0$, $u_{mp}(\hat{\theta},\mathbf{p})$ is constant for any $\mathbf{p} \in [0,1]$. Let $\hat{\mathbf{p}}$ be the solution of $\partial u_{fc}(\hat{\theta},\mathbf{p})/\partial\theta = 0$, which is given by (17). If $\mathbf{p} = \hat{\mathbf{p}}$, we have $\partial u_{fc}(\theta,\hat{\mathbf{p}})/\partial\theta > 0$ for $0 < \theta < \hat{\theta}$ and $\partial u_{fc}(\theta,\hat{\mathbf{p}})/\partial\theta < 0$ for $\hat{\theta} < \theta$, indicating that $\hat{\theta} = \theta^*$, if $\hat{\mathbf{p}} = \mathbf{p}^*$. Thus, we have $(\hat{\theta},\hat{\mathbf{p}}) = (\theta^*,\mathbf{p}^*)$.

The uniqueness of the NE is proved by contradictions. Assume that there exists another NE $(\theta_1,\mathbf{p}_1) \neq (\theta^*,\mathbf{p}^*)$. If $\theta_1 < \theta^*$, we have $\partial u_{mp}(\theta_1,\mathbf{p})/\partial\mathbf{p} < 0$ and thus $\mathbf{p}_1 = 0$. By (23), we have $\partial u_{fc}(\theta,0)/\partial\theta \geq 0$, i.e., $u_{fc}(\theta,\mathbf{p}_1)$ increases with θ. Thus, $u_{fc}(\theta_1,\mathbf{p}_1) < u_{fc}(\theta^*,\mathbf{p}^*)$, contradicting the assumption that $(\theta_1,\mathbf{p}_1)$ is NE. If $\theta_1 > \theta^*$, we have $\partial u_{mp}(\theta_1,\mathbf{p})/\partial\mathbf{p} > 0$ that yields $\mathbf{p}_1 = 1$. By (23), we have $\partial u_s(\theta,1)/\partial\theta \leq 0$, i.e., $u_{fc}(\theta,1)$ decrease with θ. Thus, $u_{fc}(\theta_1,\mathbf{p}_1) < u_{fc}(\theta^*,\mathbf{p}^*)$, contradicting to the assumption. Thus, the unique NE is $(\theta^*,\mathbf{p}^*)$ in this game. ■

3) Reinforcement-Learning-Based Threshold Estimation: The machine learning technologies, i.e., DL [28], [29] and RL [30], [31], are proved to be efficient in discovering the optimal strategy. Usually, the attacking frequency remains unknown to FCs, therefore the optimal test threshold should be discovered for data reliability validation.

As an RL algorithm, the expected Sarsa is chosen in this article. The reason behind that is as follows. The expected Sarsa, which computes the 1-step expected reward, is more stable while compared with Q-learning. That suggests the expected Sarsa tends to converge faster than Q-learning such that less energy cost is required. As any privacy-preserving algorithm designed for mobile-edge crowdsensing in IIoT should be energy efficient, the expected Sarsa is more suitable than Q-learning. While applying the expected Sarsa to data reliability validation, FC employs the hypothesis test in (14) to determine the reliability of each one of N data received in each time slot.

Let the FAR and miss detection rate (MDR) of authentication in the $k-1$th time slot, i.e., $s_k = [\alpha_{k-1},\beta_{k-1}]$, constitute the state s_k in the kth time slot. Consider the threshold estimation a continuous space Markov decision process, we quantize both of the state space and the action space into different levels for complexity reduction. To be specific, we quantize error rates into $\mathcal{X}+1$ levels. Similarly, the test threshold θ is chosen from $\mathcal{Y}+1$ level. Note that the number of levels, i.e., $\mathcal{X}$ and $\mathcal{Y}$, determines the accuracy of data reliability validation. That is a larger $\mathcal{X}$ or $\mathcal{Y}$ contributes to a better validation accuracy and a higher computational complexity as well due to more actions θs will be taken on each state s. Thereby, we verify the validation accuracy in simulation in terms of average error rates, i.e., the FAR and the MDR. The simulation results show that the proposed PPCS outperforms baselines with both FAR and MDR less than 2% when the $\mathcal{X}$ and $\mathcal{Y}$ are set to 29 and 9, respectively. FC chooses its action θ_k based on the state s_k to maximize the utility, denoted by U_k, which is given by $U_k = u_r^k(\theta,\mathbf{p})$. No doubt that malicious PUs will affect the result of data reliability validation such that the utility of the FC drops. Although a growing number of malicious PUs will compromise the performance of the proposed PPCS, the data reliability will be verified eventually due to the effectiveness of the reliability validation and the reward–punishment of the incentive mechanism. Compared with PPCC and REAP, the proposed PPCS obtain a higher FC utility due to the discovery of the optimal threshold. In each timeslot k, by taking the action θ_k, the next state s_{k+1} can be observed from the environment due to the next state, which is the result of the hypothesis test (14), not only depends on the threshold θ_k but the authenticity of input data obtained from the environment as well.

In addition, the reliability validation with expected Sarsa has a learning rate $\tau \in (0,1]$, which accounts for the weight of $Q(s_k,x_k)$. And $\delta \in (0,1]$ denotes the discount factor indicating the uncertainty of future rewards. The $V(s)$ represents the state-value function. Then, the Q-value is updated by the FC as

$$Q(s_k,\theta_k) \leftarrow (1-\tau)Q(s_k,\theta_k) + \tau(U_k + \delta V(s_{k+1})) \tag{24}$$

$$V(s_k) \leftarrow \sum_{\theta\in\left\{\frac{l}{\mathcal{Y}}\right\}_{0\leq l\leq\mathcal{Y}}} \pi(\theta|s_k)Q(s_k,\theta) \tag{25}$$

where $\pi(\theta|s_k)$ denotes the probability of choosing threshold θ based on state s_k. We adopt the ε-greedy for the FC to choose a suboptimal action with the probability ε compared with choosing the optimal action with the probability $1-\varepsilon$.

Eventually, we obtain the θ^* as

$$\theta^* = \arg \max_{\theta \in \left\{\frac{l}{\mathcal{Y}}\right\}_{0 \le l \le \mathcal{Y}}} Q(s_k, \theta). \tag{26}$$

C. PU Reputation Update and Aggregation Weight Calculation

In order to distinguish malicious PUs (i.e., the ones upload tampered data) from honest ones (i.e., the ones upload perturbed data satisfying predetermined PPDs), we decide to update the reputation of the ith PU in the kth time, denoted by r_i^k, for further corresponding weight w_i^k calculation. Let d_i denote the absolute deviation between each data and the reference with $d_{\max} = \max_i\{d_i\}$, while the absolute deviation between each reliable data and the reference is denoted by d' with $d'_{\max} = \max_i\{d'_i\}$. Then, we give the following rules for reputation update.

Rule 1: If $d_i \le d_{\max}$, then the reputation value increases as d_i decreases. Thus, the reputation gradually grows if the ith PU consistently provides reliable sensing data.

Rule 2: If $d_i > d_{\max}$, then the reputation value decreases as the $d_i - d_{\max}$ increases. It suggests that if PU v_i continuingly contributes unreliable data, then the reputation value of v_i will approach 0.

Accordingly, the reputation update function is then given by

$$\begin{aligned} r_i^k \leftarrow r_i^{k-1} &+ \frac{\text{sign}\left(d_i - d'_{\max}\right) + 1}{2} \cdot \left(1 - r_i^{k-1}\right) \cdot \exp\{-\zeta d_i\} \\ &+ \frac{\text{sign}\left(d_i - d'_{\max}\right) - 1}{2} \cdot r_i^{k-1} \\ &\times \left(1 - \exp\{-\eta(d_i - d_{\max})\}\right) \end{aligned} \tag{27}$$

where ζ and eta are negative real numbers to scale r_i^k and $\text{sign}(x) = \begin{cases} -1, & x > 0 \\ 1, & x \le 0. \end{cases}$

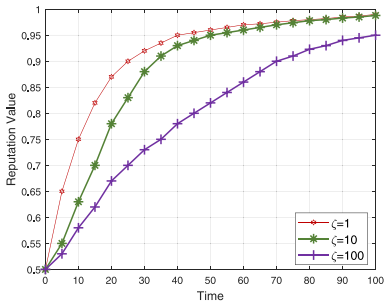
The impact of parameter ζ and η is evaluated in (27) by monitoring the reputation value change of an honest PU or a malicious one with each initial value set to 0.5, respectively. In Fig. 2(a), it is obvious that a smaller ζ results in rapidly growing in the reputation value. On the contrary, a larger η contributes to the great drop in the reputation value as shown in Fig. 2(b).

Note that only the reliable data are utilized to calculate the weighted average. Let $X' = \{x_1, x_2, \ldots, x_{N'}\}$ denote the reliable data set verified by the data reliability validation. Thus, the aggregation weight for data x_i^k is then given by

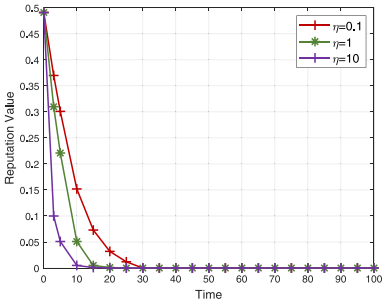
$$w_i^k = \frac{\xi_i^k}{\sum_{i=1}^{N'} \xi_i^k} \tag{28}$$

where $\xi_i^k = [(r_i^{k-1})/(\sum_{i=1}^{N'} r_i^{k-1})] + [(d'_i)/(d'_{\max})]$.

In fact, (10) and (28) guarantee that only reliable data will be utilized to calculate the weighted average for aggregation accuracy improvement. It is worth to mention that malicious PUs are always paid less than honest ones due to their "bad" reputations even if they just contribute reliable data. On the other hand, honest PUs will be paid less than usual and the corresponding reputations drop if they just contribute unreliable data. However, if malicious PUs keep contributing reliable data, then the payment increases with their reputations, and eventually malicious PUs become honest ones. On the contrary, honest PUs become malicious ones if they constantly contribute unreliable data such that the corresponding payment decreases rapidly. It is clear that the collective influence of the incentive mechanism design and the reputation update rule successfully punishes malicious PUs meanwhile rewards honest ones as long as PUs are rational.



(a)



(b)

Fig. 2. Normalized reputation w.r.t. (a) $\zeta \in [1, 10, 100]$ and (b) $\eta \in [0.1, 1, 10]$.

V. Performance Evaluation

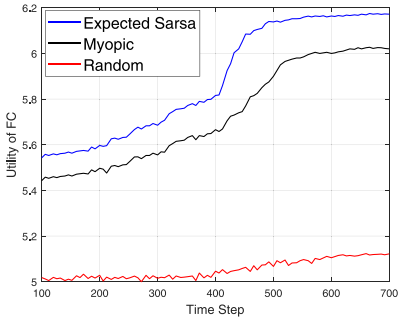
A. Simulation Setup

The performance of the proposed PPCS for mobile-edge computing-assisted IIoT applications has been validated through extensive simulation experiments in Python. The data set we used in this experiment is the Web traffic time-series forecasting of Wikipedia pages [32]. Approximately, $145k$ time series constitutes the training data set, in which daily views of different Wikipedia articles are considered as time series from July 1, 2015 to December 31, 2016. In our experiment, there are up to $N = 50$ PUs, each of which uploads normalized daily views of a unique article per time slot. We set the number N_m of malicious PUs varying from 2 to 8, each of which uploads the tampered daily view that deviates from the real value about 15%. We give the parameters in Table II.

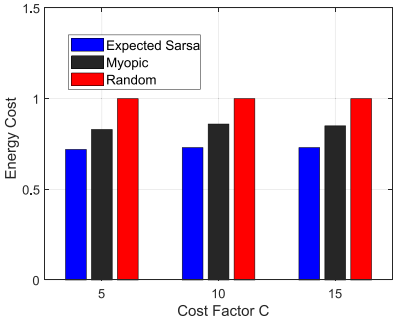
We first give the data reliability validation comparison between the expected Sarsa of PPCS and both baseline policies Myopic and Random in MDR, FAR, Utility of FC, and normalized energy cost. Then, we compare the aggregation accuracy of PPCS with that of PPCC and REAP.

TABLE II
PARAMETERS SETUP

Para.	*Desc.*	*Val.*
Data Radius	Radius of normalized daily views	(0,0.5)
$\mathcal{X}$	Classification level of state set S	29
$\mathcal{Y}$	Classification level of action set A	9
G_1	Gain of receiving a reliable data	15
G_0	Gain of receiving an unreliable data	10
C	Energy cost factor	$\{5, 10, 15\}$
α	Adjacent distances	[0.05,0.5]
B	FC budget	[50,500]
ϵ_i	PPD of the ith PU	(0,1)
μ_i	Cost parameter chosen uniformly	[10,20]

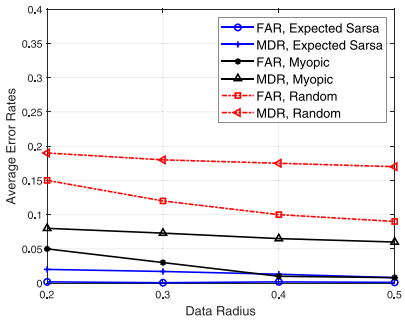


(a)

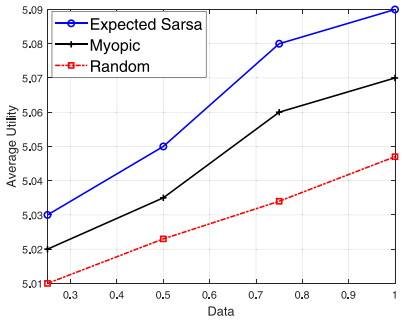


(b)

Fig. 3. Performance comparison between expected Sarsa, myopic, and random in (a) utility of FC and (b) energy cost.



(a)



(b)

Fig. 4. Comparison between expected Sarsa, myopic, and random in (a) average error rates and (b) utility of FC.

B. Data Reliability

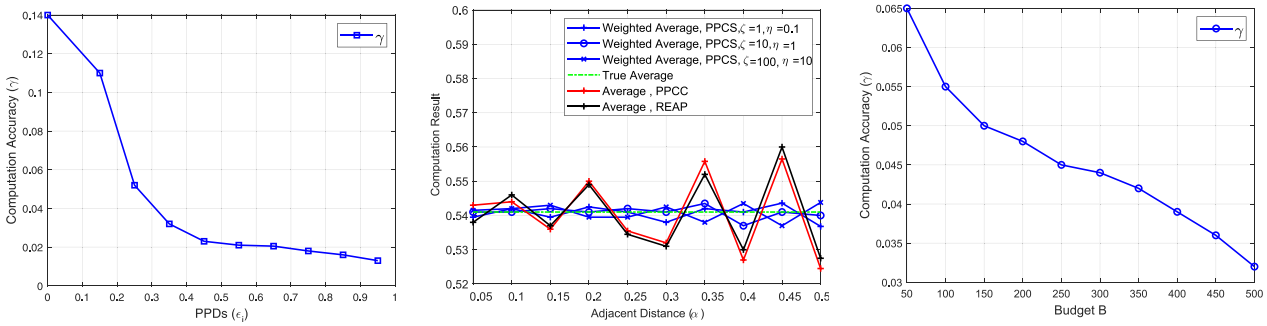
As shown in Fig. 3(a), the data reliability validation with expected Sarsa reaches a stable utility much faster and higher than that of policy Myopic and policy Random. The reason behind that is as follows. Policy Myopic tends to maximize immediate reward, however by doing so future reward can be reduced. Besides, the Random policy can hardly obtain the optimal threshold that results in a lower utility. Since expected Sarsa converges faster than the Myopic policy and the Random policy, the energy cost of expected Sarsa is considerably lower as shown in Fig. 3(b), which is about 75% of that of the Random policy and 90% of that of the Myopic policy. Since the privacy-preserving strategies designed for IIoT should be energy efficient, the performance of mobile-edge crowdsensing could be greatly improved if the PPCS is adopted.

Both FAR and MDR decrease as the data radius increases, as shown in Fig. 4(a). For example, both FAR and MDR are close to 0, if the data radius is approaching 0.5. If the data radius is about 0.4, the FAR and MDR of policy Random are up to 20% and 15%, respectively, while that of expected Sarsa is only 2% and 1%. And policy Myopic performs a little better than Random. The average utility of FC is shown in Fig. 4(b), it is clear that expected Sarsa outperforms policy Myopic and policy Random as well. It is worth to mention that a higher utility often results in a better threshold w.r.t. (26). That explains both FAR and MDR of the expected Sarsa are lower compared with baseline approaches as shown in Fig. 4(a). That suggests the mobile-edge crowdsensing is more robust if the PPCS is employed.

C. Aggregation Accuracy

The ε_i's effects on aggregation accuracy is shown in Fig. 5(a). It is clear that when PUs have a larger ε_i, the weighted average value is close to the true one due to less noise is added if PPDs are higher. Thereby, PUs are encouraged to set higher PPDs for better aggregation accuracy.

Fig. 5(b) shows the weighted average and average with varying adjacent distance α. It is obvious that PPCS achieves much better aggregation accuracy than baseline approaches PPCC and REAP with each pair of reputation scale factors (ζ, η). This is because PPCS give each data a corresponding weight based on data reliability validation and data owner's reputation, i.e., a reliable data provided by an honest PU should be given a significant weight otherwise a relatively low weight is given, while both PPCC and REAP calculate the average of aggregated data disregarding the fact that malicious PUs can upload tampered data. Thanks to the PPCS, the QoS of the mobile-edge crowdsening of IIoT is significantly improved.



(a) (b) (c)

Fig. 5. Aggregation accuracy with varying parameters. (a) Varying PPDs. (b) Varying α. (c) Varying budget.

The impact of FC's budget B is shown in Fig. 5(c). It can be observed that γ decreases as the budget increases. Note that a smaller γ indicates a better aggregation accuracy. Each PU is paid more to set the ε_i with a larger value if the budget of FC is larger. That will result in a higher aggregation accuracy.

VI. Conclusion

This article investigates the privacy-preserving data aggregation problem in IIoT. Most previous studies on this subject have conflicting objectives, i.e., the edge FC requires data of better quality for data fusion of better accuracy whereas PUs desire better privacy preserving by larger noise injection. Thus, how to choose proper noise to achieve the tradeoff between accuracy and privacy is an open problem. In addition, FC is vulnerable to tampered data without efficient data reliability validations and reward–punishment mechanisms. In this article, an efficient RL-based PPCS is proposed to solve these problems. In general, PPCS provides a KL privacy-preserving-based data aggregation utilizing an incentive mechanism to solve the problem of noise selection. Furthermore, the incentive mechanism design is based on PUs' reputations to punish malicious PUs. On the other hand, PPCS offers data reliability validation and PU's reputation update, both of which collaborate to ease the impact of tampered data. Theoretical analysis and validation experiments indicate that the weighted average of aggregated data established by PPCS has a better aggregation accuracy than contemporary strategies.

References

[1] T. Wang, H. Ke, X. Zheng, K. Wang, A. Sangaiah, and A. Liu, "Big data cleaning based on mobile edge computing in industrial sensor-cloud," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1321–1329, Feb. 2020.

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

[3] X. Wang, J. He, P. Cheng, and J. Chen, "Privacy preserving collaborative computing: Heterogeneous privacy guarantee and efficient incentive mechanism," *IEEE Trans. Signal Process.*, vol. 67, no. 1, pp. 221–233, Jan. 2019.

[4] Z. Zhang, S. He, J. Chen, and J. Zhang, "REAP: An efficient incentive mechanism for reconciling aggregation accuracy and individual privacy in crowdsensing," *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 2995–3007, 2018,

[5] K. Zhao, S. Tang, B. Zhao, and Y. Wu, "Dynamic and privacy-preserving reputation management for blockchain-based mobile crowdsensing," *IEEE Access*, vol. 7, pp. 74694–74710, 2019.

[6] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, "A blockchain-based location privacy-preserving crowdsensing system," *Future Gener. Comput. Syst.*, vol. 94, pp. 408–418, May 2019.

[7] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7702–7712, Oct. 2019.

[8] Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, "Deep learning based inference of private information using embedded sensors in smart devices," *IEEE Netw.*, vol. 32, no. 4, pp. 8–14, Jul./Aug. 2018.

[9] J. Hu, H. Lin, X. C. Guo, and J. Yang, "DTCS: An integrated strategy for enhancing data trustworthiness in mobile crowdsourcing," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4663–4671, Dec. 2018.

[10] Y. Liu, T. Feng, M. Peng, J. Guan, and Y. Wang, "DREAM: Online control mechanisms for data aggregation error minimization in privacy-preserving crowdsensing," *IEEE Trans. Depend. Secure Comput.*, early access, Jul. 24, 2020, doi: 10.1109/TDSC.2020.3011679.

[11] J. Xiong *et al.*, "A personalized privacy protection framework for mobile crowdsensing in IIoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4231–4241, Jun. 2020.

[12] J. Xiong, M. Zhao, M. Bhuiyan, L. Chen, and Y. Tian, "An AI-enabled three-party game framework for guaranteed data privacy in mobile edge crowdsensing of IoT," *IEEE Trans. Ind. Informat.*, early access, Dec. 2, 2019, doi: 10.1109/TII.2019.2957130.

[13] J. Huang *et al.*, "Blockchain-based mobile crowd sensing in industrial systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6553–6563, Oct. 2020.

[14] J. He, L. Cai, P. Cheng, J. Pan, and L. Shi, "Distributed privacy-preserving data aggregation against dishonest nodes in network systems," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1462–1470, Apr. 2019.

[15] J. Nie, J. Luo, Z. Xiong, D. Niyato, and P. Wang, "A Stackelberg game approach toward socially-aware incentive mechanisms for mobile crowdsensing," *IEEE Trans. Wireless Commun.*, vol. 18, no. 1, pp. 724–738, Jan. 2019.

[16] B. Cao, S. Xia, J. Han, and Y. Li, "A distributed game methodology for crowdsensing in uncertain wireless scenario," *IEEE Trans. Mobile Comput.*, vol. 19, no. 1, pp. 15–28, Jan. 2020.

[17] Y. Zhan, C. H. Liu, Y. Zhao, J. Zhang, and J. Tang, "Free market of multi-leader multi-follower mobile crowdsensing: An incentive mechanism design by deep reinforcement learning," *IEEE Trans. Mobile Comput.*, vol. 19, no. 10, pp. 2316–2329, Oct. 2020.

[18] M. Zhang, J. Chen, L. Yang, and J. Zhang, "Dynamic pricing for privacy-preserving mobile crowdsensing: A reinforcement learning approach," *IEEE Netw.*, vol. 33, no. 2, pp. 160–165, Apr./May 2019.

[19] Y. Liu, H. Wang, M. Peng, J. Guan, J. Xu, and Y. Wang, "DeePGA: A privacy-preserving data aggregation game in crowdsensing via deep reinforcement learning," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4113–4127, May 2020.

[20] G. Fortino, F. Messina, D. Rosaci, G. M. L. Sarné, and C. Savaglio, "A trust-based team formation framework for mobile intelligence in smart factories," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6133–6142, Sep. 2020.

[21] H. Fang, X. Wang, and L. Hanzo, "Adaptive trust management for soft authentication and progressive authorization relying on physical layer attributes," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2607–2620, Apr. 2020.

[22] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.
[23] R. Casadei, G. Fortino, D. Pianini, W. Russo, C. Savaglio, and M. Viroli, "Modelling and simulation of opportunistic IoT services with aggregate computing," *Future Gener. Comput. Syst.*, vol. 91, pp. 252–262, Feb. 2019.
[24] P. Cuff and L. Yu, "Differential privacy as a mutual information constraint," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 43–54.
[25] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design," *Automatica*, vol. 81, pp. 221–231, Jul. 2017.
[26] P. Zhou *et al.*, "Privacy-preserving and residential context-aware online learning for IoT-enabled energy saving with big data support in smart home environment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7450–7468, Oct. 2019.
[27] A. Ghosh and A. Roth, "Selling privacy at auction," *Games Econ. Behav.*, vol. 91, pp. 334–346, May 2015.
[28] X. Guo, H. Lin, Z. Li, and M. Peng, "Deep-reinforcement-learning-based QoS-aware secure routing for SDN-IoT," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6242–6251, Jul. 2020.
[29] Z. Chen, J. Hu, G. Min, A. Zomaya, and T. El-Ghazawi, "Towards accurate prediction for high-dimensional and highly-variable cloud workloads with deep learning," *IEEE Trans. Parallel Distrib. Syst.*, vol. 31, no. 4, pp. 923–934, Apr. 2020.
[30] J. Wang, J. Hu, G. Min, W. Zhan, Q. Ni, and N. Georgalas, "Computation offloading in multi-access edge computing using a deep sequential model based on reinforcement learning," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 64–69, May 2019.
[31] C. Xu, K. Wang, P. Li, R. Xia, S. Guo, and M. Guo, "Renewable energy-aware big data analytics in geo-distributed data centers with reinforcement learning," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 205–215, Jan.–Mar. 2020.
[32] *Web Traffic Time Series Forecasting*, Google, Mountain View, CA, USA, 2017. [Online]. Available: https://www.kaggle.com/c/web-traffic-time-series-forecasting/data

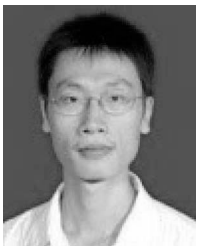
Xiaoding Wang received the Ph.D. degree from the College of Mathematics and Informatics, Fujian Normal University, Fuzhou, China, in 2016.

He is an Associate Professor with the School of Fujian Normal University. His main research interests include network optimization and fault tolerance.

Sahil Garg (Member, IEEE) received the Ph.D. degree from the Thapar Institute of Engineering and Technology, Patiala, India, in 2018.

He is currently a Postdoctoral Research Fellow with École de Technologie Supérieure (ÉTS), Montreal, QC, Canada; and a MITACS Intern with the Global AI Accelerator, Ericsson, Montreal. He was the recipient of a prestigious Visvesvaraya Ph.D. Fellowship from the Ministry of Electronics and Information Technology, Government of India, at Thapar Institute of Engineering and Technology. He is also a Visiting Researcher with the School of Computer Science and Engineering (SCSE), Nanyang Technological University, Singapore. He has over 60 publications in high ranked journals and conferences, including over 40 top-tier journal papers and over 20 reputed conference articles. His research interests are mainly in the areas of machine learning, big data analytics, knowledge discovery, cloud computing, Internet of Things, software defined networking, and vehicular ad-hoc networks.

Dr. Garg has been awarded the IEEE ICC Best Paper Award in 2018. He also serves as the special sessions/workshop chair and publication chair for CCCI 2020 and ICICC 2020. He is also the workshop chair/publicity co-chair for several IEEE/ACM conferences, including IEEE Infocom, IEEE Globecom, IEEE ICC, and ACM MobiCom. He is currently a Managing Editor of *Human-Centric Computing and Information Sciences Journal* (Springer). He is also an Associate Editor of *IEEE Network Magazine*, IEEE SYSTEMS JOURNAL, *Future Generation Computer Systems* (Elsevier), *Applied Soft Computing* (Elsevier), and *International Journal of Communication Systems* (Wiley). In addition, he also serves as the Workshops and Symposia Officer for the IEEE ComSoc Emerging Technology Initiative on Aerial Communications. He guest edited/editing a number of special issues in top-cited journals, including IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE INTERNET OF THINGS JOURNAL, *IEEE Network Magazine*, *Future Generation Computer Systems* (Elsevier), and *Neural Computing and Applications* (Springer). He is a member of ACM and IAENG; and also actively involved in various technical societies, including IEEE Communications Society, IEEE Computer Society, IEEE Industrial Electronics Society, and IEEE Smart Grid Community.



Hui Lin received the Ph.D. degree in computing system architecture from the College of Computer Science, Xidian University, Xi'an, China, in 2013, and the M.E. degree from the College of Mathematics and Informatics, Fujian Normal University, Fuzhou, China, in 2007, and the Ph.D. degree in computing system architecture from the College of Computer Science, Xidian University in 2013.

He is a Professor with the College of Mathematics and Informatics, Fujian Normal University. He has published more than 50 papers in international journals and conferences. His research interests include mobile cloud computing systems, blockchain, and network security.

Georges Kaddoum received the Ph.D. degree (Honor) in signal processing and telecommunications from the National Institute of Applied Sciences, Toulouse, France, in 2008.

He published over 200 journal and conference papers and two pending patents.

Dr. Kaddoum is a recipient of the "Research Excellence Award of the Université du Quebec," and the "Research Excellence Award-Emerging Researcher" from ÉTS in 2019. He is a co-recipient of the Best Papers Awards of the IEEE PIMRC 2017 and the IEEE WiMob 2014. He received the "Exemplary Reviewer Award" from IEEE TRANSACTION ON COMMUNICATION twice in 2015 and 2017. He is currently serving as an Associate Editor for the IEEE TRANSACTION ON INFORMATION FORENSICS AND SECURITY and the IEEE COMMUNICATION LETTERS. He held the ÉTS Research Chair in physical-layer security for wireless networks.

Jia Hu received the B.Eng and M.Eng. degrees in electronic engineering from Huazhong University of Science and Technology, Wuhan, China, in 2006 and 2004, respectively, and the Ph.D. degree in computer science from the University of Bradford, Bradford, U.K., in 2010.

He is a Senior Lecturer of Computer Science with the University of Exeter, Exeter, U.K. He has published over 60 research papers within these areas in prestigious international journals and reputable international conferences. His research interests include edge-cloud computing, resource optimization, applied machine learning, and network security.

Dr. Hu has received the Best Paper Awards at IEEE SOSE'16 and IUCC14. He serves on the editorial board of *Computers and Electrical Engineering* (Elsevier) and has guest-edited many special issues on major international journals (e.g., IEEE INTERNET OF THINGS JOURNAL, *Computer Networks*, and *Ad-Hoc Networks*). He has served as the General Co-Chair of IEEE CIT'15 and IUCC'15, and a Program Co-Chair of IEEE ISPA'20, ScalCom'19, SmartCity'18, CYBCONF'17, and EAI SmartGIFT'2016.

M. Shamim Hossain (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, Ottawa, ON, Canada, in 2019.

He is a Professor with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He is also an Adjunct Professor with the School of Electrical Engineering and Computer Science, University of Ottawa. He has authored and coauthored more than 300 publications, including refereed journals conference papers, books, and book chapters. Recently, he co-edited a book on *Connected Health in Smart Cities Springer*. His research interests include cloud networking, smart environment (smart city, smart health), AI, deep learning, edge computing, Internet of Things, multimedia for health care, and multimedia big data.

Prof. Hossain is on the editorial board of several SCI/ISI-Indexed Journals/Transactions, including the IEEE TRANSACTIONS ON MULTIMEDIA, IEEE MULTIMEDIA, IEEE NETWORK, IEEE WIRELESS COMMUNICATIONS, IEEE ACCESS, *Journal of Network and Computer Applications* (Elsevier), and *International Journal of Multimedia Tools and Applications* (Springer). He also presently serves as a Lead Guest Editor of IEEE NETWORK, *ACM Transactions on Internet Technology*, *ACM Transactions on Multimedia Computing, Communications, and Applications*, and *Multimedia Systems Journal*. He is a Senior Member of ACM.