Toward Secure Data Fusion in Industrial IoT Using Transfer Learning

Hui Lin, Jia Hu, Xiaoding Wang, Mohammed F. Alhamid, *Member, IEEE*, and Md. Jalil Piran, *Member, IEEE*

***Abstract*—As an emerging technology, the industrial Internet of Things (IIoT) can promote the development of industrial intelligence, improve production efficiency, and reduce manufacturing costs. In IIoT, the improvement and progress of industrial production and applications are inseparable from data fusion, a process that realizes the collection, analysis, and processing of the massive IoT data generated by industrial equipment and applications. IIot demands a real-time, effective, and privacy-preserving data fusion process. However, the existing works need to train different learning models for data analysis, which cannot meet real-time requirements in IIoT. Meanwhile, the lack of defense against internal attacks and the difficulty to balance system performance and privacy protection hinder the effectiveness and privacy protection in the data fusion process. To solve the abovementioned problems, in this article, we propose a new transfer learning-based secure data fusion strategy (TSDF) for IIoT. The proposed TSDF consists of three parts, guidance based deep deterministic policy gradient (GDDPG) algorithm for task classification, transfer learning based GDDPG for grouping of task receivers, and a multiblockchain mechanism for privacy preservation. The experiment results show that TSDF can achieve high system throughput and low latency, providing privacy preservation in data fusion under various IIoT application environments.**

***Index Terms*—Blockchain, cyber security, fifth generation (5G), industrial Internet of Things (IIoT), transfer learning (TL).**

Manuscript received October 18, 2020; accepted November 1, 2020. Date of publication November 17, 2020; date of current version June 30, 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 Smart Technologies. Paper no. TII-20-4801. *(Corresponding authors: Jia Hu; Xiaoding Wang.)*

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

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

Xiaoding Wang is with the College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, China (e-mail: wangdin1982@163.com).

Mohammed F. Alhamid is with the Chair of Smart Technologies, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia (e-mail: mohalhamid@ksu.edu.sa).

Md. Jalil Piran is with the Department of Computer Science and Engineering, Sejong University, Seoul 05006, South Korea (e-mail: piran@sejong.ac.kr).

Color versions of one or more of the figures in this article are available at https://doi.org/10.1109/TII.2020.3038780.

Digital Object Identifier 10.1109/TII.2020.3038780

I. Introduction

As a new development of the Internet of Things (IoT) [1] technology, industrial IoT (IIoT) has been rapidly deployed to meet the demand of industrial intelligence [2]. IIoT comprehensively utilizes various IoT devices, and intelligent data analysis technologies to collect, analyze and process massive amounts of data generated in the industrial production process, and return decision information to related equipment and departments, thereby improving production efficiency, and reducing production costs [3].

With the continuous development and popularization of IIoT, the traditional wireless communication technologies and cloud computing architectures cannot meet the requirements for real-time, accuracy, and effectiveness in the process of industrial intelligence, and will restrict the further development of IIoT applications [4]. The mobile edge computing (MEC) [5], [6] and the 5G communication system [7] provide an opportunity to solve the abovementioned problems, and integration of 5G and MEC to support IIoT applications has become a consensus in academia and industry [8]. Therefore, this article aims to propose a new 5G-aided IIoT architecture. As shown in Fig. 1, the proposed 5G-aided IIoT consists of three important components, i.e., intelligent terminals, the 5G edge network, and the remote cloud service center. Specifically, the intelligent terminals are responsible for data collection and fusion. The 5G edge network is composed of multiple MEC servers employed to run various computation tasks. Furthermore, the remote cloud service center is responsible for large-scale data storage and tasks processing.

The 5G-aided IIoT can bring innovation to industrial production, but it will also bring new problems, especially for data fusion. The data fusion in 5G-aided IIoT is as follows: edge servers aggregate collected data from various industrial intelligent terminals, then analyze and process the fused data, to extract useful information, and finally feedback the information to industrial equipment or submit to a cloud service center for further decisions. How to ensure the realtime, accuracy, and effectiveness while providing privacy preservation in data fusion has become a key issue for IIoT [9].

To solve the abovementioned challenges, we propose a new transfer learning-based secure data fusion strategy (TSDF) for Industrial IoT. The transfer learning (TL) [8], [10] is a machine learning technology that transfers trained models for other models' training. In this article, the TSDF employs the TL

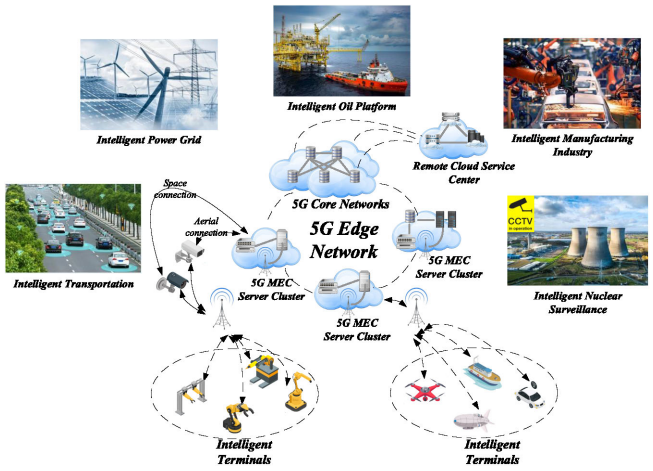


Fig. 1. Architecture of 5G-aided IIoT.

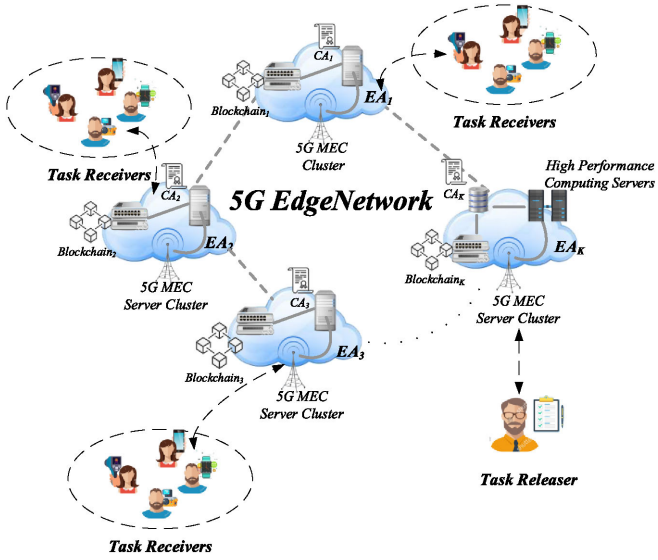


Fig. 2. System model of TSDF.

to accomplish the classification of tasks and the grouping of task receivers. In addition, blockchain [11] a tamper-resistant distributed ledger of blocks has been employed to tackle the privacy security challenge.

The main contributions of this article are outlined as follows.

1) A novel 5G-aided IIoT architecture is proposed based on the integration of 5G, MEC, and IIoT technologies, to meet the new requirements of the IIoT applications in low latency, high-bandwidth connections, high processing power, and large storage capacity.
2) A TL-based classification technology is developed to realize the classification of tasks and the grouping of task receivers according to the security and privacy requirements, to improve the effectiveness and accuracy in the process of data fusion for 5G-aided IIoT.
3) Based on the classification and grouping results, multiple homogeneous blockchains with different privacy and security protection capabilities are established to avoid the collusion attackers obtaining the privacy information during data fusion.
4) Experiment results show that TSDF can achieve high selection rate of trusted task receiver, high system throughput, and low transaction latency, while improving privacy protection capabilities under various application environments.

II. Related Work

Data fusion in IIoT has been studied for decades. Rigazzi *et al.* [12] propose a tunnel based data fusion method for IIoT applications, in which the M2M data collected by industrial intelligent terminal are merged and aggregated toward the gateway/base station. AlQahtani *et al.* [13] propose an M2M data fusion scheme for IIoT that manages to obtain low delay under the power constraints. To reduce the delay of channel access, Bhandari *et al.* [14] propose a cluster based data fusion scheme. A novel model is designed by Qin *et al.* [15] to quantify path duration time in data fusion that employs convergecast in IIoT. Wang *et al.* [16] propose a wireless networks for industrial automation-process automation data packet fusion scheme based on the channel quality and packet fusion mechanism for IIoT to increase the success rate of data transmission and effectively reduce the forwarding time. Wu *et al.* [17] propose a fog computing based privacy aware data fusion scheme for IIoT to aggregate data in a privacy aware manner, utilizing homomorphic encryption. Zhao *et al.* [18] design a privacy-preserving data fusion scheme w.r.t evaluations on data fusion and sensing users in IIoT. The contract theory is used for data fusion strategy design [19] to assure fusion accuracy and user data privacy by providing different privacy preferences based contracts to users. A federated TL-based data fusion mechanism is proposed by Chen *et al.* [20] for the IIoT applications, in which the federated learning is used for data fusion first and the TL is employed to create personalized models. The deep reinforcement learning (DRL) algorithm is applied achieve privacy-aware data transmission by Guo *et al.* [21], in which transmission routes are selected dynamically to avoid privacy leakage. The data coding and k-anonymous techniques based privacy preservation method is proposed by Qiu *et al.* [22] to protect the privacy of multimedia data during data fusion process.

Although existing research results can improve the accuracy of the data fusion process in IIoT applications and provide security and privacy protection to a certain extent, the following challenges still exist: 1) How to further improve the effectiveness and accuracy in the process of data fusion. 2) How to prevent privacy leakage due to the internal attacks such as collusion attack while ensure that the system performance can meet the requirements of IIoT practical applications.

III. System Model

The system model of TSDF, as shown in Fig. 2, consists of task releasers, task receivers, edge authentication (EA) servers, and 5G MEC server clusters. Specifically, the task receivers are

mainly responsible for data collection. The task releasers are responsible for releasing data collection and fusion tasks. EA is responsible for the certification of blockchain workers. 5G MEC server clusters execute the data fusion and computation tasks.

In general, the task releaser posts a series of data fusion tasks on 5G MEC server clusters. Among these servers, the classification server and the task receiver grouping server partition tasks and task receivers into groups, respectively. Accordingly, the multiple homogeneous blockchains are established on blockchain servers and CA servers w.r.t task partition and task receiver grouping. Once task receivers sign the data fusion contracts, they provide data to crowdsensing servers.

In the proposed TSDF, we assume that a task receiver failing to complete the task or performing poorly in task completion should not be allowed to accept new task, especially the new task of a high security level. According to the abovementioned assumption, we use a three-dimension vector $(\mathrm{WL}_i, \mathrm{CH}_i, \mathrm{TR}_i)$ to represent a task Task_i, where WL_i, CH_i, TR_i represent the work load, the completion history, and the information of task receivers of Task_i, respectively. Thereby, the security level of the task Task_i, denoted by $\mathrm{SL}_{\mathrm{Task}_i}$, should consider each dimension factor, i.e., $\mathrm{SL}_{\mathrm{Task}_i} = \alpha \mathrm{CH}_i + \beta \mathrm{WL}_i + \gamma \mathrm{TR}_i$ with $\alpha + \beta + \gamma = 1$. Accordingly, we give the security level of a task receiver $\mathrm{SL}_{\mathrm{TR}_i} = \eta \mathrm{CH}_i + (1-\eta)\mathrm{SL}^{\mathrm{Avg}}_{\mathrm{Task}}$, where $\mathrm{SL}^{\mathrm{Avg}}_{\mathrm{Task}}$ denotes the average security level of tasks the task receiver ever completed. It is evident that $\mathrm{SL}_{\mathrm{Task}}$ and $\mathrm{SL}_{\mathrm{TR}}$ affect each other. Once the task is completed properly, the security level of the task receiver will be raised that eventually results in a rise in that of the task.

In this article, we focus on the privacy disclosure problem. Be specific, if sensitive information of the task is accessed by malicious task receivers, then there is a potential risk of privacy exposure of the task releaser, i.e., malicious task receivers sell sensitive information contained in the task for profit or in exchange for something more valuable. Therefore, we consider the following attack.

Collusion Attack: Task receivers launch collusion attack by sharing partial information obtained by individual after accepting tasks for privacy stealing.

IV. Implementation Details of the TSDF

In this section, we give the implements details of the TSDF, which includes the task classification, the task receiver grouping, and the multiple homogeneous blockchains design.

A. Guiding Based Deep Deterministic Policy Gradient (GDDPG) Design for Task Classification

Due to the privacy concern, the task and task receiver partition is necessary. In addition, we assign each task or task receiver a security level. This is because we only allow task receivers to accept tasks if their security levels are higher than that of the tasks. In fact, how to efficiently and reliably partition sensitive tasks poses a great challenge. In this article, we develop a DRL [23] based sensitive tasks partition mechanism utilizing the GDDPG for sensitive task classification first. And then task receiver grouping is implemented through TL based on the well trained deep neural networks of the GDDPG in the task classification.

Similar to the traditional DDPG, the GDDPG consists of an actor networks π, a critic network Q, a target actor networks π', and a target critic network Q', the parameters of which are denoted by ϑ^{π} ϑ^{Q}, $\vartheta^{\pi'}$, and $\vartheta^{Q'}$, respectively. Note that in the learning process of a DRL, there could exist some high-return trajectories [24], which contain useful information. In order to use these experiences, we introduce a senior experience pool $\mathcal{P}^*$ to store excellent experiences only, i.e., high-return trajectories. Specifically, in each timeslot, we store the experience in the experience pool $\mathcal{P}$ in a quintuple (s_t, a_t, r_t, s_{t+1}), while excellent experiences are stored as an episode experience of length T in $\mathcal{P}^*$, i.e., $[(s_0, a_0), (s_1, a_1), \ldots, (s_T, a_T)]$ under the constrain that the reward of the ith episode r^e_i, $r^e_i = r_1 + r_2 + \cdots + r_T$, should be greater than the average reward of the latest m episodes, which have already been stored in $\mathcal{P}^*$ as $r^e_i \geq \frac{r^e_1 + r^e_2 + \cdots + r^e_m}{m}$. It is worth to mention that compared with DBDDPG [25] the proposed GDDPG is more stable in the learning process. Specifically, as a supervised learning algorithm, the stability of GDDPG depends on the guiding network, while DBDDPG adopts a so-called confidence network to stabilize the learning process utilizing the stochastic gradient algorithm. Although the immediate reward can be deemed as an unbiased estimation of the reward function for network update based on unsupervised stochastic gradient, the immediate reward can hardly reflect the capability of stabilizing the learning process of the DBDDPG. Furthermore, GDDPG updates the guiding network with excellent experiences. Thereby, the learning process can be stabilized for convergence acceleration by the GDDPG. The size of the $\mathcal{P}^*$ is fixed such that if a new episode experience is added, the one of the least reward is eliminated. Similar to the literature [24], a guiding network $G(s|\vartheta^G)$ is developed based on this experience pool.

To partition sensitive tasks into groups, we choose K group centers such that Task_is fall into a group G_i if the group center Center_i is the closest one than other group centers. That indicates the distance between a task Task_i and a group center Center_i is the key for task partition. Since each task is presented in a three-dimension vector, the scale-invariant distance is required. In fact, as a scale-invariant distance, the Mahalanobis distance can eliminate the scale influences. We then give the Mahalanobis distance between the Task_j and Center_i as $\mathrm{dist}(\mathrm{Task}_j, \mathrm{Center}_i) = \sqrt{(\mathrm{Task}_j^{\rightarrow} - \mathrm{Center}_i^{\rightarrow})^T \sum^{-1} (\mathrm{Task}_j^{\rightarrow} - \mathrm{Center}_i^{\rightarrow})}$, where $\sum$ represents the covariance matrix of task. Since a DRL requires three basic components, i.e., state, action, and reward, in this article, we let the state s_t in timeslot t be the proportion of the distance between all group members and the group center to the overall distance between each pair of tasks as $s_t = \frac{\sum_{i=1}^{K} \sum_{\mathrm{Task}_j \in G_i} \mathrm{dist}(\mathrm{Task}_j, \mathrm{Center}_i)}{\sum_{i \neq j} \mathrm{dist}(\mathrm{Task}_i, \mathrm{Task}_j)}$. Accordingly, we use K group centers chosen in timeslot t as the action, i.e., $a_t = (\mathrm{Center}_{1,t}, \mathrm{Center}_{2,t}, \ldots, \mathrm{Center}_{K,t})$. Different from the traditional DRL, if the action is taken, then the next state s_{t+1} can be calculated based on (s_t, a_t) rather than observing from the environment. Next, according to the total distance from group members to the corresponding group centers, we give

the reward r_t as $r_t = -\sum_{i=1}^{K}\sum_{\text{Task}_j \in G_i} \text{dist}(\text{Task}_j, \text{Center}_i)$. Since the guiding network $G_1(s|\vartheta^{G_1})$ is introduced to improve the learning progress, a potential action a_t can be calculated with an extra guidance, i.e.,

$$a_t = \pi_1(s_t|\vartheta^{\pi_1}) + \zeta(G_1(s_t|\vartheta^{G_1}) - \pi_1(s_t|\vartheta^{\pi_1})) \tag{1}$$

where $0 \le \zeta \le 1$. Then, experience (s_t, a_t, r_t, s_{t+1}) and (s_t, a_t) are stored in experience poor $\mathcal{P}_1$ and trajectory Traj, respectively.

Total N experience will be sampled from $\mathcal{P}_1^*$ to for the guiding network update w.r.t the loss function in the training process

$$\mathcal{L}(\vartheta^G) = \frac{1}{N}\sum_{i}^{N}[G_1(s_i|\vartheta^G) - a_i]^2. \tag{2}$$

Accordingly, the critic network is updated utilizing the following loss function based on experiences sampled from $\mathcal{P}$ by

$$\mathcal{L}(\vartheta^{Q_1}) = \frac{1}{N}\sum_{i}^{N}[Q_1(s_i, a_i|\vartheta^{Q_1}) - \mathcal{Y}_i]^2 \tag{3}$$

where

$$\begin{aligned}\mathcal{Y}_i = r_i + \delta[(1-\zeta)Q_1(s_{i+1}, \pi_i(s_{i+1}|\vartheta^{\pi_1'})|\vartheta^{Q_1'}) \\ + Q_1(s_{i+1}, \pi_i(s_{i+1}|\vartheta^{\pi_1'})|\vartheta^{Q_1'})].\end{aligned} \tag{4}$$

Then, the policy gradient is employed to update the actor network π by

$$\begin{aligned}\nabla_{\vartheta^{\pi_1}} J = \frac{1}{N}\sum_{i}^{N}[\nabla_a Q_1(s, a|\vartheta^{Q_1})|s = s_i, a = \pi_1(s_i|\vartheta^{\pi_1}) \\ \nabla_{\vartheta^{\pi_1}}\pi_1(s|\vartheta^{\pi_1})|s = s_i].\end{aligned} \tag{5}$$

Eventually, target networks $\vartheta^{Q_1'}$ and $\vartheta^{\pi_1'}$ are updated based on a learning rate κ.

B. TL-Based GDDPG Design for Task Receiver Grouping

The task receiver grouping is implemented through TL based on the well trained deep neural networks of the GDDPG in the task classification. Specifically, the task classification is implemented based on the distance from each task to a specific task center, in which two factors of the task (i.e., the completion history and the information of task receivers) are closely related to task receivers. On other hand, task classification can facilitate task receiver grouping. Accordingly, the proportion of the distance between all group members (i.e., task receivers in a group) and the group center to the overall distance between each pair of task receivers represents the state in task receiver grouping referring to that in task classification. Then, it is straightforward to find the similar mapping between either two action spaces or two reward functions correspondingly. We first train the GDDPG networks in the task classification problem and then use the trained networks as initialization of the GDDPG networks in the task receiver grouping problem, which could contribute to a significant reduction in the training time. Furthermore, once parameters are transferred, we can adjust all layers to assess the grouping result as an adaptation (see Fig. 3).

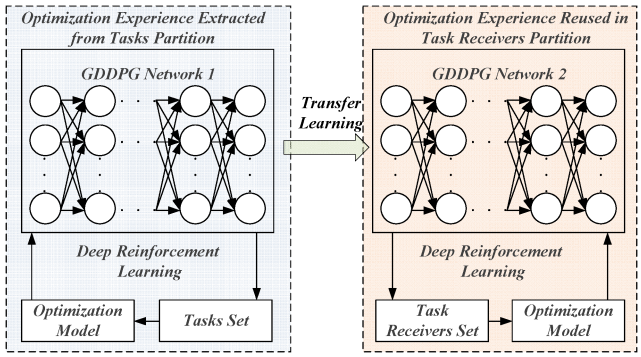


Fig. 3. TL-based task classification and task receiver grouping.

By colluding with each other, task receivers are able to launch the collusion attack to obtain sensitive information. However, such attack can be prevented by the task classification and task receiver grouping of the proposed strategy TSDF. The reason for that is as follows. First, each task receiver is capable of joining in a blockchain, only if the SL_{TR} is higher than that of the task SL_{Task}. That suggests a task receiver whoever possess a higher security level is more trustworthy. Therefore, such task receivers should be less likely to collude with others for sensitive task information discovery. Second, since the task receivers of a specific blockchain is separated from that of another blockchain, the probability of colluding $N/2$ task receivers will be less than $\frac{C_{N/2}^{N}}{N^{N/2}}$, the limit of which is equal to 0 with $N \to +\infty$. That implies the more task receivers TSDF required the less chance of the collusion attack being launched, especially more blockchains are involved.

C. Multiblockchain Design

The proposed task classification and task receiver grouping mechanisms can effectively defense against the collusion attack. However, the privacy security is still a challenge for data fusion in TSDF. In this section, based on the task classification and task receiver grouping results, the multiple homogeneous blockchains implemented on the Hyperledger Fabric [26], [27] with different privacy protection capabilities are established to reduce the possibility of privacy information leakage during data fusion process. Each group of tasks are established in smart contracts on a specific blockchain blockchaini and corresponding certificate authority CA_i deployed on Edge Area EA_i. Moreover, a dynamically reliable workers selection mechanism will be deployed in the CA_i of the blockchain_i to impose the security requirements of the blockchain through authentication.

Once the task receiver posts a data fusion task, task information will be written in the smart contract. Meanwhile, only when the task satisfies a certain condition, can the task be packaged into a block. For example, when the block's security level SL_{Block} should be lower than that of the task's security level SL_{Task}, the task can be packaged into the current block as a transaction, otherwise it will be removed from the current blockchain. This avoids the malicious task releaser to obtain the privacy information of the task receivers through releasing the

TABLE I
PARAMETER SETUP

Parameter	*Description*	*Range*
N_C	classification number	[2,5]
N_R	task releaser number	1
N_M	task receivers number	100
SR	send rate	[200,550] tps
N	number of tasks	[100, 240]
T_N	transaction number	[250,500,750]
TB_N	transaction number in block	[100,800]
BS	size of the block	[1.5,5] mb

task. On the other hand, if task receivers in the current blockchain want to apply for tasks, the security levels of whom should be higher than that of the tasks. By doing so, only a limited amount of sensitive information the task receivers might obtain. That indicates the possibility of selecting trusted task receivers against privacy leakage.

D. Reward-Punishment Mechanism

In TSDF, to avoid the task receivers be reluctant in receiving and completing tasks, a reward-punishment mechanism is designed to reward the honest task receivers and punish malicious ones. In the proposed mechanism, a task receiver will be rewarded if he or she actively participates in the task and completes the task well. Otherwise, whoever fails to complete the task or performs extremely poor in task completion, the payment of the task will be shared by others, and the security level of that task receiver will drop significantly as the reputation value. Thereby, the task receiver will be kept from accepting tasks of higher security level as a further punishment.

V. PERFORMANCE EVALUATION

A. Simulation Setup

To implement performance evaluation on the proposed TSDF, we employ a physical machine of 3.33 GHZ Intel I7 CPU and 64 G memory, in which the Hyperledger Fabric 1.3 is deployed on a virtual machine of four processors, 60 GB of Ubuntu system with 8 GB memory. We give the parameter setup in Table I.

1) Performance Metrics: The performance of TSDF is evaluated in clustering accuracy, system throughput, transaction latency and trusted task receiver selection rate (TSR) considering different T_N, SR, BT_N, and BS, respectively.

1) *Clustering accuracy:* The deviation between cluster centers generated by TSDF, K-means, and support vector machine (SVM), respectively.
2) *System throughput:* System throughput depends on transaction processing speed of the blockchain.
3) *Transaction latency:* Transaction latency relies on transaction processing capacity of the blockchain.
4) *Trusted TSR:* TSR is determined by task completion and task receivers' security levels.
5) *Model training time:* With the TL, the model training time for task receiver grouping is significantly reduced.

B. Experiment Results

1) Clustering Accuracy: We first compare the positions of each pair of group centers generated by the TSDF, K-means, and SVM clustering algorithm, respectively, with the number of group set to two. And the result is shown in Fig. 4. It is obviously that all group centers are closely located. TSDF adopt GDDPG utilizing all attributes of a task and the information of task receivers for task classification such that sensitive tasks are not only accurately partitioned but the privacy disclosure is prevented as well, while compared with K-means and SVM.

The results shown in Fig. 4 verifies that TSDF is more applicable than K-means and SVM in 5G-aided IIoT for privacy-preserving data fusion.

2) System Throughput: Observed from Fig. 5(a), we find that the system throughput approaches 85, 86, and 95 tps, while the number of task T_N equals to 250, 500, and 750, respectively. When $T_N = 750$, the system throughput increases by 30% and reaches 125 tps, compared with 40% and 12.5% when $T_N = 500$ and $T_N = 250$ respectively. Obviously, the more tasks the system processes the higher system throughput we obtain. Fig. 5(a) verifies the efficiency of task processing in multiple blockchains. As shown in Fig. 5(b) and (c), it is evident that the system throughput increase gradually with the growth of either the BS or the TB_N. In addition, once BS $\geq$ 4mb or $\text{TB}_N \geq 700$, the throughput begins to level off. The reason behind that is multiblockchains can provide the efficient partition of both task and task receivers and the capability of task processing as well based on different BS and TB_N.

3) Transaction Latency: Fig. 6 shows the variation tendency of average latency while considering different SR, TB_N, and BS. In Fig. 6(a), it is clear that the average latency increase with SR. And a greater TB_N tends to have a higher average latency. In addition, the average latency is no more than 8.5 s when T_N equals to either 250, 500, or 750. When the SR approaches 450 tps, the curves of average latency tend to stabilize. We then set SR $= 450$ tps, $\text{TB}_N \in [200, 900]$, and BS $\in [1.5\tilde{}\text{MB}, 5\text{MB}]$ in Fig. 6(b) and (c). No doubt that as TB_N and BS increase the average latency grows. Note that the average latency tends to increase gently w.r.t the variation of either SR, TB_N, or BS. Both Figs. 5 and 6 verify the capability of task processing of the proposed multiblockchains based TSDF.

4) TSR: Fig. 7 shows the variation of TSR. Observed from Fig. 7(a), it is clear that TSR curves experience fluctuations as time increases. And the highest TSRs of $T_N = 250$, $T_N = 500$, and $T_N = 750$ reach 85%, 78%, and 60%, respectively. The reason for that is as follows. If task receivers perform well in task completion, then task receivers' reputations are improved. On the other hand, some task receivers might be reluctant in task completion that gradually deteriorates the TSR. Fortunately, the proposed TSDF introduce the reward-punishment mechanism to deal with this case such that even TSR drops at first it will rise eventually. We also consider the case that without the reward-punishment mechanism task receivers might complete the tasks reliably at first and then they fail in next tasks and the simulation result is given in Fig. 7(b). Obviously, even the proposed TSDF can offer task receivers "appealing" contracts,

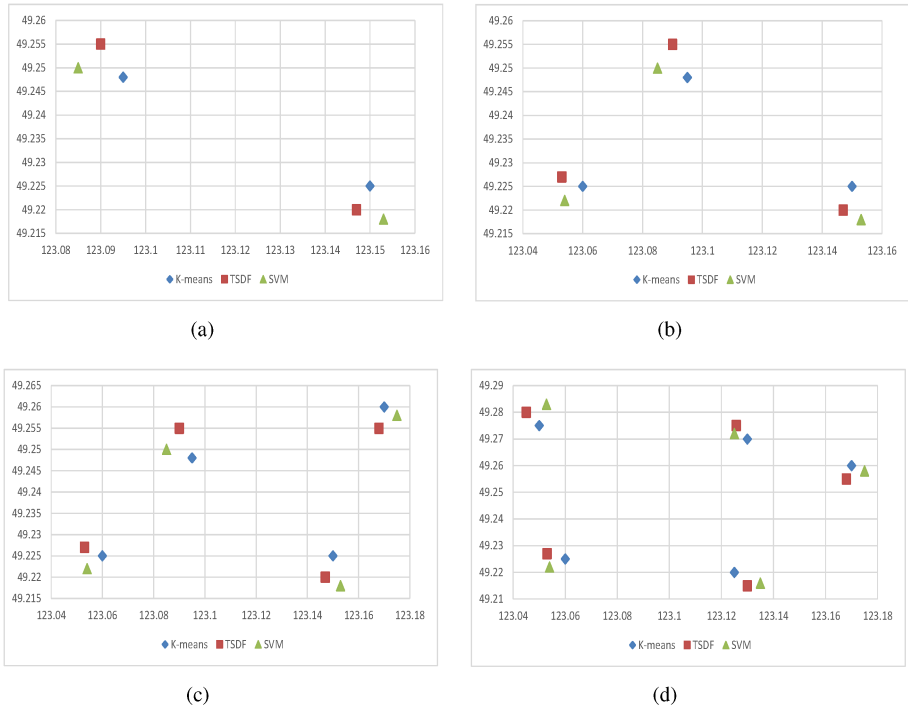


Fig. 4. Clustering accuracy comparison with the classification numbers varying from 2 to 5. (a) $N_C = 2$. (b) $N_C = 3$. (c) $N_C = 4$. (d) $N_C = 5$.

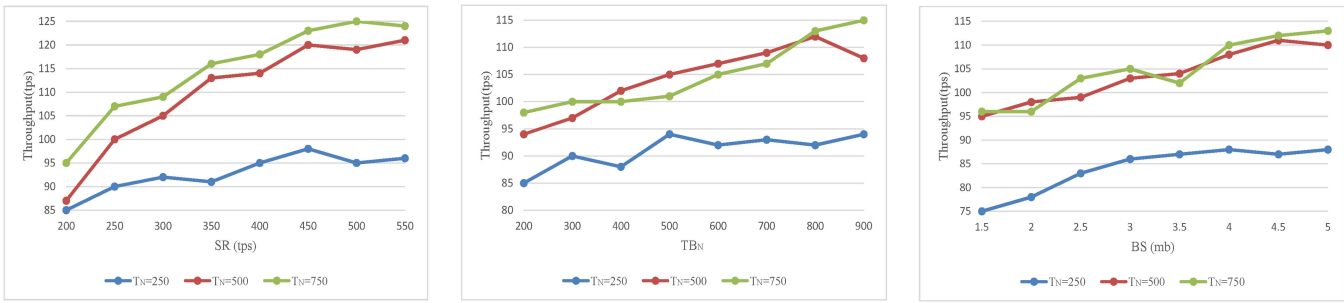


Fig. 5. System throughput of TSDF with different (a) SR, (b) TB_N, and (c) BS.

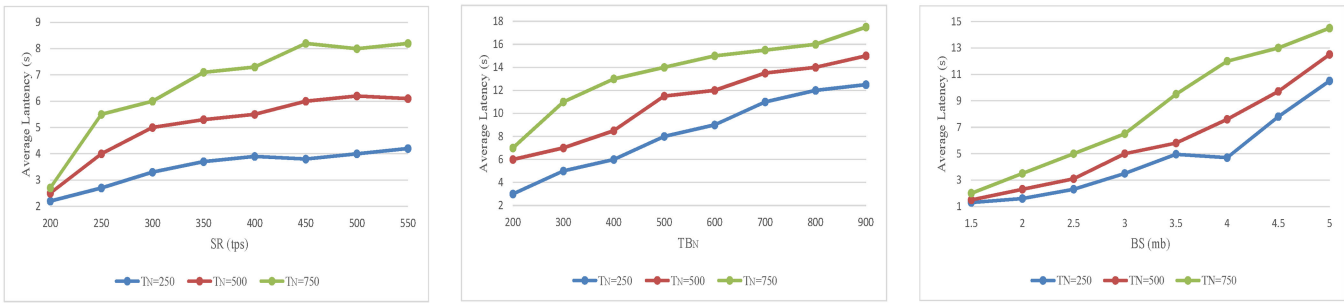


Fig. 6. Transaction latency of TSDF with different (a) SR, (b) TB_N, and (c) BS.

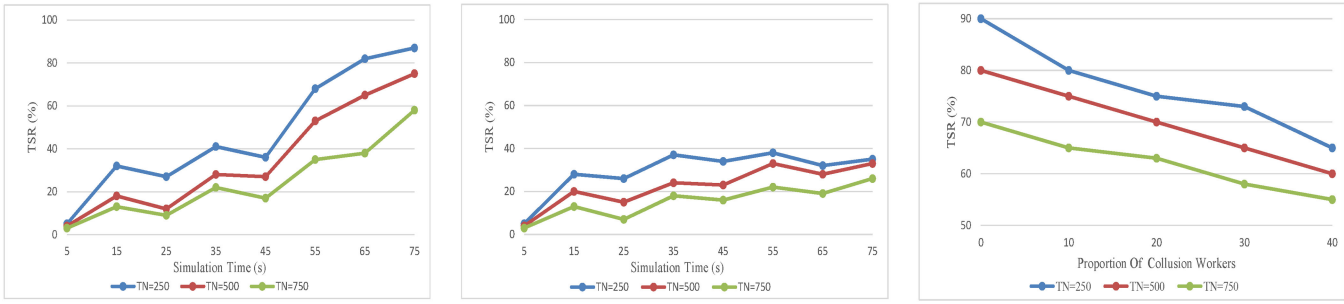


Fig. 7. Trusted TSR comparison. (a) Without collusion attack. (b) Without collusion attack and reward-punishment mechanism. (c) With collusion attacks and reward-punishment mechanism.

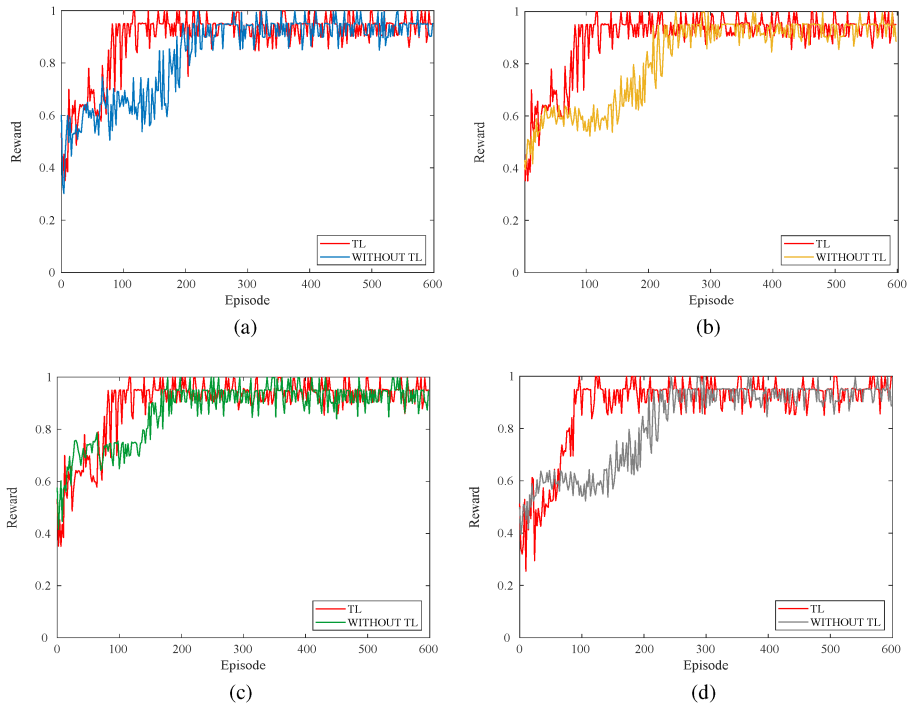


Fig. 8. Model training time of task receiver grouping with the classification numbers varying from 2 to 5. (a) $N_C = 2$. (b) $N_C = 3$. (c) $N_C = 4$. (d) $N_C = 5$.

some task receivers still tend to perform poorly in task completion due to task releaser gives no reward to good task completion as no punishment to poor one. That explains why the highest TSR for either $T_N = 250$, $T_N = 500$, or $T_N = 750$ is less than 40%. As shown in Fig. 7(c), with more task receivers collude with each other, TSR decreases dramatically due to the reason that accepting tasks is for sensitive information recovery through task receivers' collusion. Furthermore, a larger T_N has a lower TSR. This is because more tasks required to be processed bring a greater chance for task receivers colluding with each other such that TSR drops even more.

5) Model Training Time: In order to verify the significance of TL, we first compare the task receiver grouping with/without TL (TRG_TL/TRG) in model training time with the classification number varying from 2 to 5. And the result is shown in Fig. 8.

Fig. 8 verifies that the TL-based task receiver grouping can significantly reduce the model training time. Thereby, with the help of TL, the proposed TSDF is efficient in privacy-preserving data fusion for 5G-aided IIoT applications.

VI. Conclusion

Focusing on the shortage of low-latency, high-bandwidth connections, high processing capabilities, and large storage capacity service guarantees faced by traditional IIoT, and the demand of accurate and realtime data fusion during the development of IIoT applications, in this article, a TSDF for IIoT was proposed. In TSDF, 5G communication technology and MEC were deeply integrated with IIoT, and a novel 5G-aided IIoT was proposed. At the same time, in TSDF, to solve the data privacy issues in data

fusion process, TL technology was used to classify and group tasks and task recipients according to their privacy and security levels. And then, the blockchain technology was adopted to protect privacy during data fusion process by strictly restricting task receivers from participating in receiving tasks and obtaining task information, and also avoided the malicious task releaser to obtain the privacy information of the task receivers through releasing the task. The simulation experiment results show that TSDF can obtain accurate clustering, high throughput, high credible user selection rate, and low latency.

References

[1] C. Brewster, I. Roussaki, N. Kalatzis, K. Doolin, and K. Ellis, "IoT in agriculture: Designing a europe-wide large-scale pilot," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 26–33, Sep. 2017.

[2] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[3] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[4] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K. F. Tsang, and J. Rodriguez, "Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 28–33, Mar. 2017.

[5] X. Hou, Z. Ren, K. Yang, C. Chen, H. Zhang, and Y. Xiao, "IIoT-MEC: A novel mobile edge computing framework for 5G-enabled IIoT," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2019, pp. 1–7.

[6] J. Mills, J. Hu, and G. Min, "Communication-Efficient federated learning for wireless edge intelligence in IoT," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 5986–5994, Jul. 2020.

[7] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, 2018.

[8] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "Edge intelligence and blockchain empowered 5G beyond for the industrial Internet of Things," *IEEE Netw.*, vol. 33, no. 5, pp. 12–19, Oct. 2019.

[9] B. Pourghebleh and N. J. Navimipour, "Data aggregation mechanisms in the Internet of Things: A systematic review of the literature and recommendations for future research," *J. Netw. Comput. Appl.*, vol. 97, pp. 23–34. 2017.

[10] S. J. Pan and Q. Yang, "A survey on transfer learning," *IEEE Trans. Knowl. Data Eng.*, vol. 22, no. 10, pp. 1345C–1359, Oct. 2010.

[11] Q. Chen, Z. Zheng, C. Hu, D. Wang, and F. Liu, "On-edge multi-task transfer learning: Model and practice with data-driven task allocation," *IEEE Trans. Parallel Distrib. Syst.*, vol. 31, no. 6, pp. 1357–1371, Jun. 2019.

[12] G. Rigazzi, N. K. Pratas, P. Popovski, and R. Fantacci, "Aggregation and trunking of M2M traffic via D2D connections," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2015, pp. 2973C–2978.

[13] S. A. AlQahtani, "Analysis and modelling of power consumption-aware priority-based scheduling for M2M data aggregation over long-termevolution networks," *IET Commun.*, vol. 11, no. 7, pp. 177C–184, 2017.

[14] S. Bhandari, S. K. Sharma, and X. Wang, "Latency minimization in wireless IoT using prioritized channel access and data aggregation," in *Proc. IEEE Global Commun. Conf.*, 2017, pp. 1–6.

[15] Z. Qin, D. Wu, Z. Xiao, B. Fu, and Z. Qin, "Modeling and analysis of data aggregation from convergecast in mobile sensor networks for industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4457–4467, Oct. 2018.

[16] H. Wang, L. Chen, D. Xu, and M. Li, "A packet aggregation scheme for WIA-PA networks based on wireless channel state," in *Proc. 11th Int. Conf. Wireless Commun. Signal Process.*, 2019, pp. 1–6.

[17] H. Wu, L. Wang, and G. Xue, "Privacy-aware task allocation and data aggregation in fog-assisted spatial crowdsourcing," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 589–602, Jan. 2019.

[18] 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.

[19] 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 Secur.*, vol. 13, no. 12, pp. 2995–3007, Dec. 2018.

[20] Y. Chen, X. Qin, J. Wang, C. Yu, and W. Gao, "Fedhealth: A federated transfer learning framework for wearable healthcare," *IEEE Intell. Syst.*, vol. 35, no. 4, pp. 83–93, Jul./Aug. 2020.

[21] 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.

[22] F. Qiu, F. Wu, and G. Chen, "Privacy and quality preserving multimedia data aggregation for participatory sensing systems," *IEEE Trans. Mob. Comput.*, vol. 14, no. 6, pp. 1287–1300, Jun. 2015.

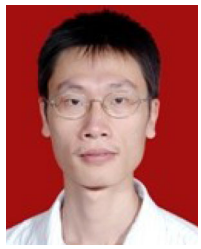
[23] J. Wang, J. Hu, G. Min, A. Zomaya, and N. Georgalas, "Fast adaptive task offloading in edge computing based on meta reinforcement learning," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 1, pp. 242–253, Jan. 2021.

[24] H. Chen, Q. Liu, Y. Yan, B. He, Y. Jiang, and L. Zhang, "An experience-guided deep deterministic actor-critic algorithm with multi-actor," *J. Comput. Res. Develop.*, vol. 56, no. 8, pp. 1708–1720, 2019.

[25] Z. Zheng, C. Yuan, Z. Lin, Y. Cheng, and H. Wu, "Self-adaptive double bootstrapped DDPG," in *Proc. 27th Int. Joint Conf. Artif. Intell.*, 2018, pp. 3198–3204.

[26] H. N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[27] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges," *Mech. Syst. Signal. Process.*, vol. 135, 2020, Art. no. 106382.



Hui Lin received the Ph.D. degree in computing system architecture from College of Computer Science, Xidian University, Xi'an, China, in 2013.

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

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

He is currently a Senior Lecturer in Computer Science with the University of Exeter, Exeter, U.K. He has authored or coauthored more than 70 research papers within these areas in prestigious international journals and reputable international conferences. His research interest include edge-cloud computing, resources optimization, applied machine learning, and network security.

Dr. Hu was the recipient of the Best Paper Awards at the IEEE International Conference on Service-Oriented System Engineering, 2016 adn IUCC'14. He serves on the editorial board of Elsevier Computers and Electrical Engineering and has guest-edited many special issues on major international journals (e.g., IEEE Internet of Things Journal, *Computer Networks*, *Ad Hoc Networks*). He was a General Chair/Co-Chair of IEEE International Conference on Computer and Information Technology, 2015, IEEE International Conference on Ubiquitous Computing and Communications (IUCC), 2015, etc., and Program Chair/Co-Chair of IEEE International Symposium on Parallel and Distributed Processing with Applications, 2020, IEEE International Conference on Scalable Computing and Communications, 2019, IEEE International Conference on Smart City, 2018, IEEE International Conference on Cybernetics, International Conference on Smart Grid Inspired Future Technologies, 2016, etc.

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

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

Mohammed F. Alhamid (Member, IEEE) received the master's and Ph.D. degrees in computer science from the School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON, Canada, in 2010 and 2015, respectively.

He is currently an Assistant Professor of Software Engineering with the College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. His research interest includes machine learning, AI, social computing, Internet-of-Things, and e-commerce/FinTech application.

Md. Jalil Piran (Member, IEEE) received the Ph.D. degree in electronics engineering from Kyung Hee University, Seoul, South Korea, in 2016.

He is currently an Assistant Professor with the Department of Computer Science and Engineering, Sejong University, Seoul, South Korea. Subsequently, he continued his work as a Postdoctoral Research Fellow with the Field of "Resource Management" and "Quality of Experience" in "5G and beyond," and "Internet of Things" in the Networking Lab, Kyung Hee University. He published substantial number of technical papers in well-known international journals and conferences in research fields of "Wireless Communications and Networking," "Internet of Things (IoT)," "Multimedia Communication," "Applied Machine Learning," "Security," and "Smart Grid."

Dr. Piran was the recipient of "IAAM Scientist Medal of the year 2017 for notable and outstanding research in the field of New Age Technology and Innovation," in Stockholm, Sweden. Moreover, he has been recognized as the "Outstanding Emerging Researcher" by the Iranian Ministry of Science, Technology, and Research in 2017. In addition, his Ph.D. dissertation has been selected as the "Dissertation of the Year 2016" by the Iranian Academic Center for Education, Culture, and Research in the field of Electrical and Communications Engineering. In the worldwide communities, he is an active delegate from South Korea in Moving Picture Experts Group (MPEG) since 2013, and an active member of the International Association of Advanced Materials (IAAM) since 2017.