Enabling Secure Authentication in Industrial IoT With Transfer Learning Empowered Blockchain

Xiaoding Wang, Sahil Garg, *Member, IEEE*, Hui Lin, Md. Jalil Piran, *Member, IEEE*, Jia Hu, and M. Shamim Hossain, *Senior Member, IEEE*

***Abstract*—Industrial Internet of Things (IIoT) is ushering in huge development opportunities in the era of Industry 4.0. However, there are significant data security and privacy challenges during automatic and real-time data collection, monitoring for industrial applications in IIoT. Data security and privacy in IIoT applications are closely related to the reliability of users, which is determined by user authentication that have been widely used as an effective approach. However, the existing user authentication mechanisms in IIoT suffer from single factor authentication and poor adaptability with the rapid growth of the number of users and the diversity of user categories. To solve the aforementioned issues, this article proposes a novel Authentication mechanism based on Transfer Learning empowered Blockchain, coined ATLB. In ATLB, blockchains are applied to achieve the privacy preservation for industrial applications. In addition, by introducing the transfer learning based authentication mechanism, trustworthy blockchains are built such that the privacy preservation for industrial applications is further enhanced. Specifically, ATLB first employs a guiding deep deterministic policy gradient algorithm to train the user authentication model of a specific region, which is then transferred locally for foreign user authentication or cross-regionally for another region's user authentication such that the model training time is significantly reduced. Experimental results show that the proposed ATLB not only provides accurate authentications for IIoT applications but also achieves high throughput and low latency.**

***Index Terms*—Authentication, blockchain, Industrial Internet of Things (IIoT), transfer learning (TL).**

Manuscript received August 25, 2020; revised November 9, 2020 and December 5, 2020; accepted December 23, 2020. Date of publication January 5, 2021; date of current version July 26, 2021. This work was supported by the Researchers Supporting Project number (RSP-2020/32), King Saud University, Riyadh, Saudi Arabia. Paper no. TII-20-4036. *(Corresponding authors: Hui Lin; Md. Jalil Piran.)*

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 École de Technologie Supérieure, Montreal, QC H3C 1K3, Canada (e-mail: sahil.garg@ieee.org).

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

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

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

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2021.3049405.

Digital Object Identifier 10.1109/TII.2021.3049405

I. Introduction

In THE last decade, the industrial standards and infrastructures have substantially evolved due to the amalgamation of the Internet of Things technology and industrial equipment in industrial applications, referred as Industrial Internet of Things (IIoT). At present, as the largest and most important application of Internet of Things, IIoT has ushered in the greatest opportunity and it is also actively playing in the ongoing innovations of Industry 4.0 [1]. IIoT deeply integrates Internet of Things, mobile communications, artificial intelligence (AI), cloud computing, and big data analysis into all aspects of the industrial production process. Through analyzing the data collected from industrial equipment and carrying out predictive maintenance to optimize production processes, IIoT effectively improves manufacturing efficiency and product quality, reduces product cost and resource consumption, and eventually upgrade the traditional industry to the intelligent one. As an open and scalable information interaction platform, IIoT enables the exchange of various data between industrial devices in local and wider areas' industrial operations [2], [3]. However, the humongous amount of data generated by the connected IIoT devices have also put forward new requirements on efficiency and accuracy of automatic, real-time data collection, monitoring, and processing. Besides, the challenges related to data security and privacy will also draw a great attention [4].

To cope with such challenges, researchers in industries all over the world develop state-of-the-art technologies, i.e., edge intelligence [5], transfer learning (TL) [6], and blockchain [7]. As a new paradigm, the edge intelligence integrates mobile edge computing, edge caching, and AI in the vicinity of end users [8]. In edge-intelligence-enabled IIoT, edge resource management controlled by AI can offer powerful computation and massive data storage at edge networks while meeting the strict delay constraints and other performance requirements of industrial applications. TL allows previously developed machine learning models to be reused and then to be retrained in different scenarios. It simplifies the model developing process by reducing the need of evaluating large datasets and investing in more computations. Furthermore, TL fosters greater explorations and experimentations, leading to innovations and greater productivity. Blockchain acts as a tamper-resistant distributed ledger sharing and storing data among a large amount of IIoT devices, and helps to achieve the data security and privacy of the IIoT by empowering

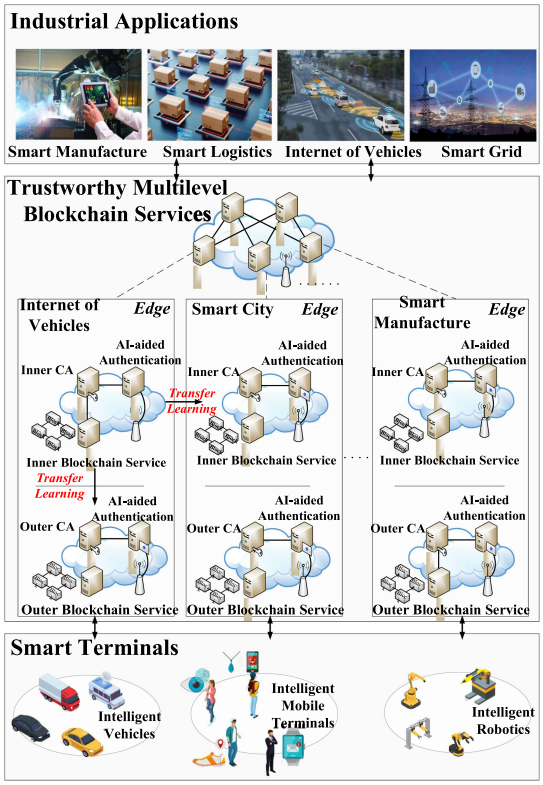


Fig. 1. Architecture of trustworthy AI-empowered blockchains for industrial applications.

anonymous and trustful transactions in decentralized and trustless environment.

In IIoT, the collaboration between TL and blockchain contributes to performance boosts on both TL and blockchain [9]. Specifically, aided by blockchains, TL can verify the credibility of data sources to prevent data forgery and tampering. Furthermore, incentives built on blockchains can be utilized to motivate the participation in TL execution. On the other hand, due to powerful data analysis and prediction capabilities, TL makes blockchain scalable and efficient by using TL to learn terminal characteristics in industrial applications and allocate computational resources efficiently. However, several critical hurdles have impeded the development of TL and blockchains in IIoT. For example, the traditional blockchains allow a user to pass the authentication process depending on single characteristic, i.e., local historical behaviors of that user in a specific region. That suggests a user whoever acts maliciously in one region might be able to pass the authentication in another region.

Based on the aforementioned analysis, we first construct an edge intelligence empowered IIoT architecture, in which the TL-aided authentication is employed, to build trustworthy intelligent blockchains. As shown in Fig. 1, there are three main parts in the proposed architecture: industrial application intelligent terminals, an edge intelligence network, and IIoT applications. The industrial application intelligent terminals are responsible for collecting efficient and reliable industrial data. The edge intelligence network, consists of the edge server, AI, and blockchain systems, is responsible for the intelligent data fusion, analysis, and process while providing data security and privacy protection to support various IIoT applications. Then, based on the proposed IIoT architecture, a novel Authentication mechanism for TL-empowered Blockchain (ATLB) is proposed. The major contributions of this article are outlined as follows.

1) To achieve privacy preservation, different blockchains, i.e., the inner blockchain and the outer blockchain, are introduced for user authentication mechanism against collusion attack and Sybil attack.
2) To improve authentication accuracy, the user authentication in each region is implemented based on user's credit. Specifically, for each user, the credit of whom, which consists of local credit and cross-region credit, is integrated with the authentication mechanism design. Then, a guiding network based deep deterministic policy gradient (G-DDPG) algorithm is proposed to train local authentication model with high accuracy.
3) To reduce the training time of authentication models, the TL is applied. Specifically, within a region, the user authentication model is transferred locally to foreign user authentication utilizing the TL in the outer blockchain. In addition, the user authentication model could also be transferred cross-regionally to another region's user authentication in the inner blockchain. By implementing user authentication with transferred deep reinforcement learning, trustworthy blockchains are built and the privacy preservation is achieved.
4) Experimental results show that: first, the proposed ATLB enables accurate authentications in IIoT for both local users and foreign users; second, it achieves high throughput and low latency in various IIoT scenarios.

II. Related Work

Recently, the authentication for machine learning empowered blockchain in IIoT has gained a lot of attention. In [10], a lightweight RFID based authentication is proposed for blockchain-empowered mobile edge computing, in which bitwise rotation, one-way hash, and XOR operations are adopted. In [11], both blockchain and machine learning are utilized to design the smart contract for the removal of the third party in data trading, in which the data owner and the data purchaser are authenticated and authorized through the challenge response and the off-chain download mechanism, respectively. In [12], the problems of single node exposure for centralized record keeping and expensive computation for decentralized case are considered. Then, a cryptographic authentication mechanism is proposed to improve the reliability of the blockchain for healthcare records keeping. In [13], a multi-WSN authentication is developed based on blockchain. Similar to the inner blockchain and the outer blockchain introduced in this article, the local chain and public chain are integrated with the hybrid blockchain design. In addition, different authentication scenarios are implemented w.r.t. local chain and public chain. In [14], the edge computing is utilized for the authentication system design based on blockchain for authentication efficiency

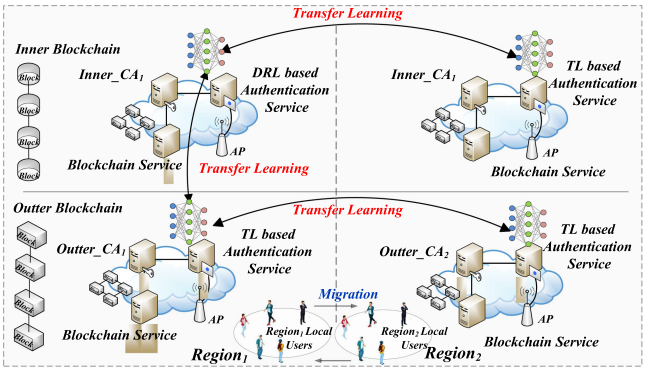


Fig. 2. System model of the proposed ATLB.

improvement. In this system, the consortium blockchain uses Byzantine fault-tolerant consensus for the trusted authentication mechanism design and the traceability of terminal activity. Feng *et al.* [15] propose a blockchain-assisted authentication system for privacy-preserving vehicle authentication in VANETs. This system provides conditional traceability of misbehaving vehicles with the Hyperledger Fabric platform employed for performance and security evaluation. In [16], an anonymous authentication mechanism is proposed for vehicular fog services, in which cross-datacenter authentication, anonymity of vehicles, lightweightness of authentication communications, and resistance of attacks against datacenter are accomplished. Wang *et al.* [17] propose a authentication mechanism based on blockchain for smart grid utilizing edge computing. This mechanism can provide conditional anonymity as well as reasonable security assurance. On the other hand, the TL is capable of reducing model training time for authentication. Lu *et al.* [18] propose a physical authentication mechanism against spoofing attack launched by edge attackers in VANETs, in which both reinforcement learning and TL are utilized to discover authentication models. In [19], an authentication framework is proposed utilizing specific device information and the TL against cyber and cyber-physical emulation attacks.

III. System Model

In this article, a novel authentication mechanism is developed based on TL-empowered blockchain in IIoT. To construct trustworthy and intelligent blockchains, a multilevel structure is introduced, i.e., for each IIoT application, there are an inner blockchain and an outer blockchain. Specifically, the inner blockchain authenticates local users within each region, whereas the outer blockchain authenticates foreign users. To improve authentication accuracy, both deep reinforcement learning (DRL) and TL are employed. All CAs, authentication servers, and blockchain servers are deployed on edge servers for computation resources required. The system model is given in Fig. 2.

1) *User:* Users can join the inner blockchain or the outer blockchain if they pass the authentication. If a user works excellently in region$_i$, then the inner_credit of whom rises such that this user might pass the region$_i$ authentication. However, if the user migrates from region$_i$ to region$_j$, then this user might fail to pass the authentication in region$_j$ due to the authentication standard differs from region to region.
2) Certificate Authority (CA): Two types of CAs are considered in this article. One is for the inner blockchain, named the inner_CA, which is responsible for local user authentication. The other is for the outer blockchain, named the outer_CA, which is responsible for foreign user authentication. Any CA employs edge servers to perform DRL-based authentication in IIoT. In addition, each CA is capable of withdrawing users' key pairs to eliminate malicious users of lower credits.

In addition, the privacy leakage problem in IIoT is considered in this article. Specifically, in traditional blockchains, a user whoever passes the authentication based on local records might act maliciously in another region. Therefore, following two types of attacks launched by malicious users are considered.

1) *Collusion attack:* Malicious users launch such attack by exchange individual task information to discover the complete sensitive task information from the blockchain.
2) *Sybil attack:* A malicious user try to join different blockchains and play the role of a legitimate user in each blockchain in order to get sensitive task information from both blockchains.

IV. Implementation of the ATLB

A. Guiding Deep Deterministic Policy Gradient Based User Authentication

In the traditional blockchain design, once a user passes the authentication based on local records, he/she can join the blockchain as a legitimate user. However, there could be a potential risk for a malicious user joining in the blockchain. That suggests both local records (i.e., credits to measure local behaviors inner_credit) and cross-region records (i.e., cross-regional credit to evaluate historical behaviors in other regions outer_credit) should be integrated with the authentication mechanism design. Then, the ith user's credit credit$_i$ can be obtained by

$$\text{credit}_i = \gamma * \text{inner\_credit}_i + (1-\gamma) * \text{outer\_credit}_i. \quad (1)$$

For authentication accuracy improvement, we develop a G-DDPG-based user authentication. Different from the traditional DDPG, the G-DDPG consists of m critic networks Q_i s and corresponding target critic networks Q_i' s, and m actor networks π_i s and corresponding target actor networks π_i' s, the parameters of which are denoted by ϑ^{Q_i}, $\vartheta^{Q_i'}$, ϑ^{π_i}, and $\vartheta^{\pi_i'}$, respectively. The high-return trajectories [20] exist in DRL learning process. Thereby, a senior experience pool $\mathcal{P}^*$ is introduced to store such experiences compared with ordinary ones stored in the experience pool $\mathcal{P}$. The structure of G-DDPG is given in Fig. 3.

In user authentication, we choose the credit as the state s. To determine whether the user should pass the authentication, a credit threshold should be discovered as the action a_t chosen in timeslot t. In addition, the next state s_{t+1} is obtained by measuring the user's behaviors. For example, if the user passes the authentication, then his/her inner_credit rises locally for good performance at work or drops otherwise. On other hand,

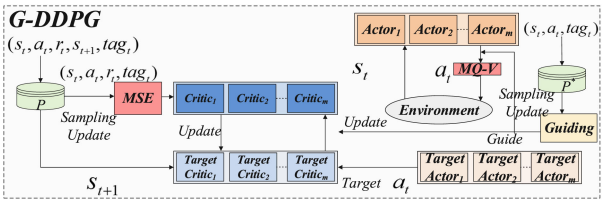


Fig. 3. Framework of G-DDPG.

if the user fails to pass the authentication, then by working well cross-regionally, he/she will be rewarded in the improvement of outer_credit. Then, the working performance of the ith user Performance_i is the gain of letting him/her passing the authentication. Note that both task completion task_completion and data reliability data_reliability are important factors to measure user's working performance. For the ith user, by integrating a scale factor α, we have

$$\text{Performance}_i = \alpha * \text{task\_completion}_i + (1-\alpha) * \text{data\_reliability}_i. \quad (2)$$

Accordingly, we give the reward r_t as

$$r_t = \sum_i \text{Performance}_i. \quad (3)$$

The action a_t is computed based on the guiding network $G_1(s|\vartheta^{G_1})$, i.e.,

$$a_t = \pi_1(s_t|\vartheta^{\pi_1}) + \zeta(G_1(s_t|\vartheta^{G_1}) - \pi_1(s_t|\vartheta^{\pi_1})) \quad (4)$$

where $0 \le \zeta \le 1$. Then, we use experience poor $\mathcal{P}_1$ to store experiences (s_t, a_t, r_t, s_{t+1}) and use trajectory Traj to record (s_t, a_t).

We train the guiding network of the G-DDPG with N randomly chosen experience from $\mathcal{P}_1^*$ as

$$\mathcal{L}(\vartheta^G) = \frac{1}{N}\sum_i^N [G_1(s_i|\vartheta^{G_1}) - a_i]^2. \quad (5)$$

We then update the critic network with N experiences randomly sampled from $\mathcal{P}$ by

$$\mathcal{L}(\vartheta^{Q_1}) = \frac{1}{N}\sum_i^N [Q_1(s_i, a_i|\vartheta^{Q_1}) - \mathcal{Y}_i]^2 \quad (6)$$

where

$$\mathcal{Y}_i = r_i + \delta[(1-\zeta)Q_1(s_{i+1}, \pi_i(s_{i+1}|\vartheta^{\pi_1'})|\vartheta^{Q_1'}) + \zeta(Q_1(s_{i+1}, G(s_{i+1}|\vartheta^G)|\vartheta^{Q_1'})]. \quad (7)$$

Then, the policy gradient is utilized to update π by

$$\nabla_{\vartheta^{\pi_1}} J = \frac{1}{N}\sum_i^N [\nabla_a Q_1(s, a|\vartheta^{Q_1})|s = s_i, a = \pi_1(s_i|\vartheta^{\pi_1}) \nabla_{\vartheta^{\pi_1}} \pi_1(s|\vartheta^{\pi_1})|s = s_i]. \quad (8)$$

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

Note that the proposed G-DDPG has a more stable learning process while compared with the double bootstrapped DDPG (DBDDPG) [21]. First, the guiding network determines the stability of the supervised algorithm G-DDPG. Excellent experiences are used to update the guiding network, which further enhance the stability. Second, as a stochastic gradient algorithm, the DBDDPG employs the "confidence" network as the stabilizer to reduce oscillations during the learning process. In DBDDPG, the unsupervised stochastic gradient is adopted to update actor/critic networks based on the immediate reward, which is considered as the unbiased estimation of the reward function. However, the immediate reward fluctuates significantly with the unpredictable environment such that it is hard to stabilize the learning process. Therefore, compared with DBDDPG, the developed G-DDPG can provide a stable learning process and an accelerated convergence.

B. TL-Based User Authentication for Inner/Outer Blockchain

Two types of transfers are considered in this article. The first one is the local transfer, i.e., the model trained for local user authentication on region_i is transferred to that on foreign users, i.e., users who migrate from other regions to region_i. The second one is the cross-region transfer, i.e., the model trained for local user authentication on region_i is transferred to that on region_j. In general, the foreign user authentication aims to determine whether users of region_j, $i \neq j$, are qualified to join the outer blockchain; the local user authentication decides whether users of region_j, for all i, are qualified to join the inner blockchain. It is worth to mention that the reason for applying the TL is the resemblance between local user authentication and foreign user authentication. Specifically, the similarity between a pair of regions can be quantified. For example, we denote the ith region region_i by a tuple, i.e., $\text{region}_i = (\text{task}_i, \text{user}_i)$, where task_i and user_i represent the task set and user set of region_i, respectively. Thus, we can obtain the similarity between region_i and region_j, denoted by $\text{similarity}_{i,j}$, based on the Mahalanobis distance, i.e., $\text{similarity}_{i,j} = \sqrt{(\text{region}_j^{\rightarrow} - \text{region}_i^{\rightarrow})^T \sum^{-1} (\text{region}_j^{\rightarrow} - \text{region}_i^{\rightarrow})}$ to eliminate the scale effect. Obviously, the similarity sequence allow us to determine which pair of regions can transfer authentication models cross-regionally. On other hand, users who can pass the authentication in a specific region should have credits higher than corresponding thresholds. According to (1), it is evident that weight α should be set higher than 0.5 for local user authentication or less than 0.5 for foreign user authentication for the appreciation of the inner_credit or the outer_credit. That suggests the possibility for transferring authentication models locally. Specifically, in the foreign user authentication of a specific region, credits, the threshold and the overall performance of foreign users serves as the state, the action, and the reward referring to that of the local user authentication. Based on these similarities, the local user authentication model can be transferred to that of the foreign user authentication.

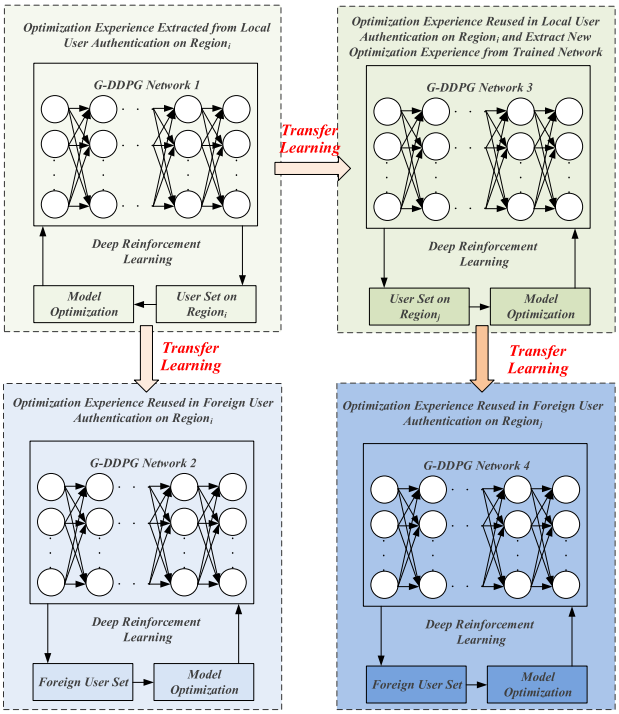


Fig. 4. TL-based user authentication: locally transferred user authentication and cross-regionally transferred user authentication.

Fig. 4 shows the implementation of model transferring. Specifically, for the first type of transfer, the G-DDPG networks are trained for local user authentication and then use the trained networks as initialization of the G-DDPG networks in foreign user authentication. That is, the parameters of the input and the hidden layers of the G-DDPG networks trained for local user authentication are shared as initializations of that for foreign user authentication to reduce the training time. However, we do not share the parameters of the output layer due to local user authentication and foreign user authentication might utilize different reward calculations. Moreover, all layers can be adjusted as parameters transferred to evaluate authentication results. The second type of transfer is implemented similarly.

Once both local and foreign user authentications are completed, each user is granted an authority, i.e., the security level. In addition, we introduce the mechanism for task decomposition and user grouping. Specifically, users are partitioned into groups based on the security level of each user. Then, each sensitive task is decomposed into a series of nonsensitive ones, each of which is associated with a certain security level. Each task is acceptable only if the security level of the user is higher than that of the task. On the other hand, we introduce the incentive mechanism. That is, the honest users will be reward with extra credits, which are closely related to the security level of the tasks, i.e., a task of a higher security level brings a higher credit reward and vice versa. In addition, CAs are capable of withdrawing key pairs to prevent malicious users from stealing sensitive information.

It is worth to mention that the proposed ATLB can prevent both Sybil attack and collusion attack. Because once a user is authenticated, this user can only join the inner blockchain or the outer blockchain. Note that if the user acts maliciously, i.e., sabotaging tasks or stealing sensitive information, then the credit of whom drops rapidly. Once the credit is lower than a threshold, the CA will withdraw this user's key pair such that with such low credit, there is no chance for this user to pass the authentication in any region. That suggest this user cannot do further damage to either blockchain such that the Sybil attack is prevented. On the other hand, the authority granted for the outer blockchain is much lower than that for the inner blockchain. That indicates even if two users from different blockchains collude with each other, the information they obtained will be insignificant due to the task information of the inner blockchain is irrelevant to that of the outer blockchain.

TABLE I
SIMULATION PARAMETERS

Parameter	*Description*	*Range*
Num_Reg	number of regions	[5,10,15]
$Send\_Rate$	send rate	[200,550] tps
Num_User	number of users	[100,1000]
Num_Tran	number of transactions	[200, 500, 800]
$Num\_BlocTran$	number of transactions in block	[100,800]
$Block\_Size$	block size	[1,4.5] mb

V. PERFORMANCE EVALUATION

A. Simulation Setup

We conduct the simulation with the computer of i7 3.2GHZ CPU, 16-G memory, and 64-b win7 system. The performance evaluation of the proposed strategy ATLB for industrial applications is implemented using Hyperledger Fabric1.3 on VMware 14 Pro of four processors, 16-G memory, and 60 GB of Ubuntu system. The parameters of this simulation are given in Table I.

1) Performance Metrics: We evaluate ATLB in terms of system throughput, transaction latency, and authentication accuracy considering different Send_Rate, Num_Tran, Num_BlocTran, Num_User, and Block_Size, respectively, which are as follows.

1) *System Throughput:* The system performance is improved, if the transactions are processed at a higher speed such that the system throughput grows.
2) *Transaction Latency:* To improve the transaction processing capacity, the transaction latency should be reduced.
3) *Authentication Accuracy:* Both false alarm rate (FAR) and miss detection rate (MDR) consist of the average error rate.
4) *Model Training Time:* To reduce the model training time for user authentication, the TL is introduced.

C. Experiment Results

1) System Throughput: Observed from Fig. 5(a), we find that as the growth of the Send_Rate, the system throughput increases. Note that for each transaction number, i.e., 200, 500, and 800, the throughput equals to 90, 95, and 100 tps, respectively. However, the system throughput increases by 33% and reaches 133 tps for Num_Tran = 800, compared with 32% of Num_Tran = 500 and 14% of Num_Tran = 200, respectively. Task processing is verified in Fig. 5(a) by the trustworthy

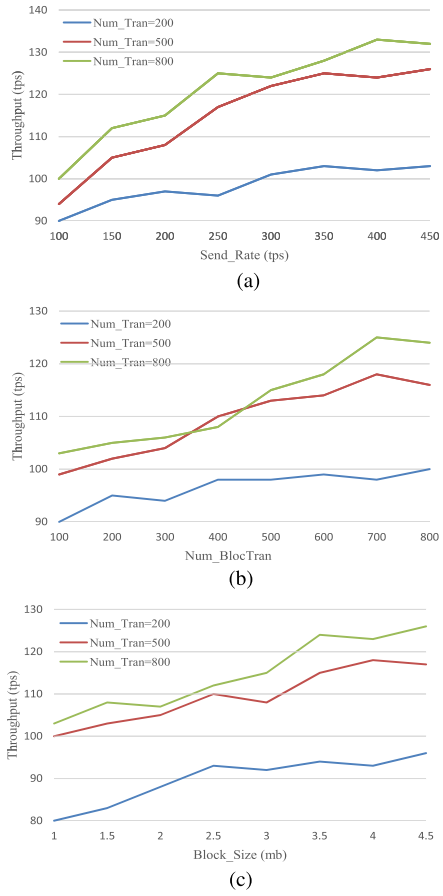


Fig. 5. Throughput of ATLB while varying (a) Send_Rate, (b) Num_BlocTran, and (c) Block_Size.

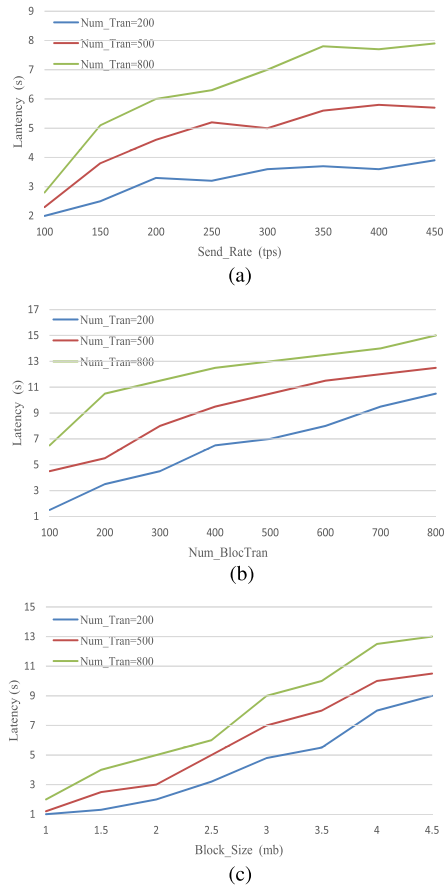


Fig. 6. Latency of ATLB while varying (a) Send_Rate, (b) Num_BlocTran, and (c) Block_Size.

blockchains constructed by the proposed ATLB. As shown in Fig. 5(b) and (c), as either Block_Size or Num_BlocTran increases, the system throughput grows for each transaction number. It is clear that the throughput begins to level off when Block_Size $\geq$ 3.5 mb and Num_BlocTran $\geq$ 700. This is because by introducing the TL to trustworthy blockchains, efficient and reliable user authentications for either local users or foreign users are accomplished. The results shown in Fig. 5 indicate that the proposed ATLB is able to improve system throughput for various industrial applications.

1) Transaction Latency: The variation of latency is shown in Fig. 6, with different values of Send_Rate, Num_BlocTran, and Block_Size. Note that a lower latency indicate a better system performance. We first set the block size to 2.5 mb. As shown in Fig. 6(a), we find that with the Send_Rate grows, the latency increases as expected. In addition, the maximum latency is no more than 8 s when Num_Tran = 800 compared with 6 s of Num_Tran = 500 and 4 s of Num_Tran = 200, respectively. The latency stabilizes as Send_Rate = 350 tps for each transaction number. Then, we set Send_Rate = 350 tps for block generation to show the latency variation with Num_BlocTran varying from 200 to 800 [see Fig. 6(b)] and Block_Size changing from 1 to 4.5 mb [see Fig. 6(c)], respectively. Although a higher latency is resulted from a greater Num_BlocTran and a bigger Block_Size, the maximum latency is less than 15 s when Num_BlocTran = 800 and Block_Size = 4.5 mb. The reason behind that is the proposed ATLB can efficiently authenticate users utilizing the TL. The results shown in Fig. 6 verify that the trustworthy intelligent blockchain of the ATLB has an excellent capability of transaction processing for a variety of industrial scenarios.

1) Authentication Accuracy: Figs. 7 and 8 show the accuracy comparison in FAR and MDR between G-DDPG and DDPG on user authentication in IIoT. We let LCR_FAR and LCR_MDR denote the FAR and MDR while TL is applied locally, i.e., the model trained for region$_i$ local user authentication is transferred locally to authenticate region$_i$ foreign users. L2_FAR and L2_MDR represent the FAR and MDR when the model trained for region$_i$ local user authentication is transferred cross-regionally to authenticate region$_j$ local user. Then, we consider the case that region$_j$ accepts the transferred model from region$_i$, based on which region$_j$ builds its own local user authentication model. Let CR2_FAR and CR2_MDR denote the FAR and MDR if the retained model is transferred locally to the region$_j$ foreign user authentication.

As shown in Fig. 7(a), as Num_User increases, both FAR and MDR grow at first and then drop for either G-DDPG or DDPG. The reason for that is with less participation, the authentication accuracy decreases that contributes to larger FAR and MDR. However, when Num_User reaches a certain threshold, i.e., Num_User = 500 for G-DDPG or Num_User = 700 for

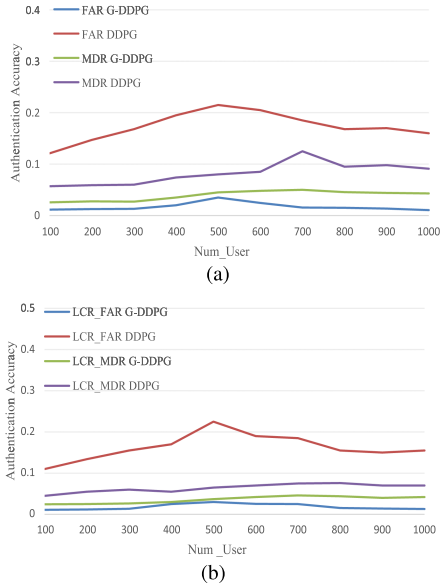


Fig. 7. Authentication accuracy in FAR, LCR_FAR, MDR, and LCR_MDR while varying Num_User. (a) FAR and MDR. (b) LCR_FAR and LCR_MDR.

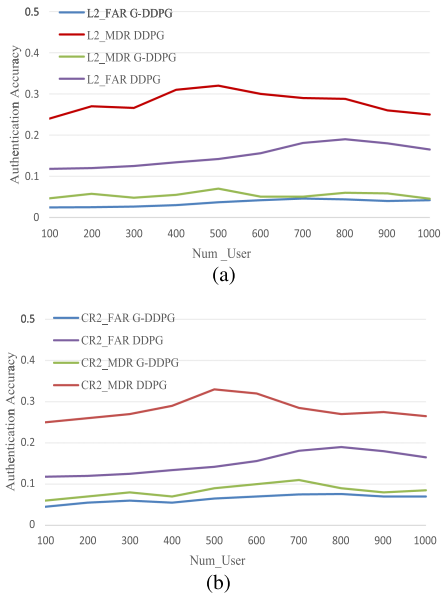


Fig. 8. Authentication accuracy in L2_FAR, CR2_FAR, L2_MDR, and CR2_MDR while varying Num_User. (a) L2_FAR and L2_MDR. (b) CR2_FAR and CR2_MDR.

DDPG, the authentication accuracy on either local users or foreign users improves such that FAR and MDR drop gradually. Note that both MDR and FAR of the G-DDPG is less than that of DDPG due to the guiding network of the G-DDPG can discover more accurate credit threshold than DDPG such that authentication accuracy is improved. As shown in Fig. 7(b), it is obviously that the G-DDPG is affected by Num_User compared with the DDPG resulting less fluctuated LCR_FAR and LCR_MDR. In addition, the G-DDPG can achieve a LCR_FAR less than 3% and a LCR_MDR less than 5%. This is because the cross-regional model transferring and the later retraining can maintain high authentication accuracy. Fig. 7 illustrates that the ATLB can accomplish accurate user for various industrial scenarios.

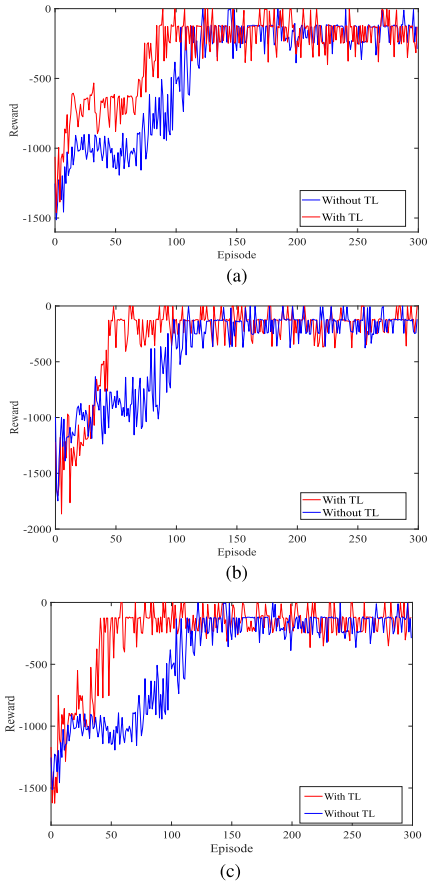


Fig. 9. Authentication model training time with/without TL while considering different region number. (a) Num_Reg = 5. (b) Num_Reg = 10. (c) Num_Reg = 15.

TABLE II
AVERAGE AUTHENTICATION ACCURACY WITH VARYING REGION NUMBERS
Num_Reg

FAR/MDR \ Num_Reg	5	10	15
LCR_FAR/LCR_MDR	3%/5%	5%/6%	5%/8%
$L2\_FAR/L2\_MDR$	5%/6%	7%/9%	8%/10%
$CR2\_FAR/CR2\_MDR$	7%/8%	8%/11%	9%/13%

As shown in Fig. 8(a), we know that both L2_FAR and L2_MDR increase as the Num_User at first, then decrease, and eventually levels off. Obviously, higher authentication accuracy requires more participants as expected. It is clear that either L2_FAR or L2_MDR of G-DDPG is the lowest compared with that of DDPG. In addition, although the TL-based user authentication can reduce the model training time by model transferring locally or cross-regionally, the authentication accuracy relies on regional user dataset. As shown in Fig. 8(b), G-DDPG outperforms DDPG in lower CR2_FAR and CR2_MDR, i.e., the maximum CR2_FAR and CR2_MDR of G-DDPG are 8% and 11% compared with that of 19% and 32% of DDPG. Fig. 8 verifies the efficiency of the proposed ATLB for user authentication in IIoT.

Observed from Table II, we find that with the region number varying from 5 to 10 with the increment of 5, all authentication

accuracy metrics increase. In addition, when Num_Reg = 15, the CR2_FAR and CR2_MDR reach their peak, which are 9% and 13% compared with the LCR_FAR of 5% and the LCR_MDR of 8%, and the L2_FAR of 8% and the L2_MDR of 10%, respectively. The reason for that is more regions bring more participating users, which results in difficulties in authenticating users. However, the results shown in Table II indicate that the proposed ATLB can provide reliable user authentication in a reasonable scale for IIoT applications.

1) Model Training Time: Different from the comparisons in system throughput (see Fig. 5), transaction latency (see Fig. 6), and authentication accuracy (see Figs. 7 and 8), the model training time comparison is conducted and the results are shown in Fig. 9.

We compare the model training time with/without the TL with the number of regions Num_Reg set to 5, 10, and 15. Observed from Fig. 9, we find that the authentication model training time is significantly reduced by applying the TL as we expected. More importantly, a larger Num_Reg leads to a more significant model training time reduction. Therefore, aided by the TL, the proposed ATLB is efficient in user authentication for different IIoT applications.

VI. Conclusion

The data security and privacy are a prerequisite of a variety of IIoT applications, and are also important foundation and guarantee for industrial safety and national security. Industrial applications in IIoT require real-time and reliable information interaction, which makes it extremely vulnerable to attacks, such as illegal intrusion, information leakage, and denial of service. As a less complex security mechanism, user authentication was proved to be one of the most effective means to solve aforementioned security problems. To overcome the shortcomings of previous user authentication mechanisms for IIoT, a new authentication mechanism based on TL-empowered blockchain, named ATLB, was proposed. In ATLB, hierarchical blockchains were applied to achieve privacy preservation for various industrial applications. In addition, by introducing the TL for the improvement of the authentication mechanism, a trustworthy blockchain was built such that the privacy preservation for industrial applications was further enhanced. Specifically, ATLB first employed a guiding deep deterministic policy gradient algorithm to train the user authentication model of a specific region, which was then transferred locally for foreign user authentication or cross-regionally for another region's user authentication to reduce the model training time. Experimental results showed that the proposed ATLB not only provided accurate authentications for IIoT applications but also achieved low latency and high throughput.

References

[1] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial Internet of Things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, 2018.

[2] 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.

[3] X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu,, and M. S. Hossain, "A secure data aggregation strategy in edge computing and blockchain empowered internet of things," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2020.3023588.

[4] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, 2020, Art. no. 102481.

[5] M. Aazam, S. Zeadally, and K. A. Harras, "Deploying fog computing in industrial Internet of Things and Industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4674–4682, Oct. 2018.

[6] E. K. Wang, X. Liu, C.-M. Chen, S. Kumari, M. Shojafar, and M. S. Hossain, "Voice-transfer attacking on industrial voice control systems in 5G-aided IIoT domain," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2020.3023677.

[7] M. Liu, F. R. Yu, Y. Teng, V. C. Leung, and M. Song, "Performance optimization for blockchain-enabled industrial Internet of Things (IIoT) systems: A deep reinforcement learning approach," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3559–3570, Jun. 2019.

[8] Y. Zhang, X. Ma, J. Zhang, M. S. Hossain, G. Muhammad, and S. U. Amin, "Edge intelligence in the cognitive Internet of Things: Improving sensitivity and interactivity," *IEEE Netw.*, vol. 33, no. 3, pp. 58–64, May/Jun. 2019.

[9] X. Jiang, F. R. Yu, T. Song, Z. Ma, Y. Song, and D. Zhu, "Blockchain-enabled cross-domain object detection for autonomous driving: A model sharing approach," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3681–3692, May 2020.

[10] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment," *IEEE Trans. Ind. Informat.*, vol. 16, no. 11, pp. 7081–7093, Nov. 2020.

[11] W. Xiong and L. Xiong, "Smart contract based data trading mode using blockchain and machine learning," *IEEE Access*, vol. 7, pp. 102331–102344, 2019.

[12] P. Pandey and R. Litoriya, "Securing and authenticating healthcare records through blockchain technology," *Cryptologia*, vol. 44, pp. 341–356, 2020.

[13] Z. Cui *et al.*, "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Trans. Serv. Comput.*, vol. 13, no. 2, pp. 241–251, Mar./Apr. 2020.

[14] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1972–1983, Mar. 2020.

[15] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4146–4155, Jun. 2020.

[16] Y. Yao, X. Chang, J. Mišić, V. B. Mišić, and L. Li, "BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3775–3784, Apr. 2019.

[17] J. Wang, L. Wu, K. R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1984–1992, Mar. 2020.

[18] X. Lu, L. Xiao, T. Xu, Y. Zhao, Y. Tang, and W. Zhuang, "Reinforcement learning based PHY authentication for VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3068–3079, Mar. 2020.

[19] Y. S. Dabbagh and W. Saad, "Authentication of wireless devices in the Internet of Things: Learning and environmental effects," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6692–6705, Aug. 2019.

[20] 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.

[21] 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.

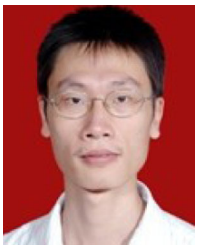
Xiaoding Wang received the Ph.D. degree in computer science from the College of Mathematics and Informatics, Fujian Normal University, Fuzhou, China, in 2016.

He is currently an Associate Professor with the School of Fujian Normal University, Fuzhou. 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 the École de Technologie Supérieure, Université du Québec, Montréal, QC, Canada. He has authored or coauthored more than 80 publications in high ranked journals and conferences, including more than 40 IEEE transactions/journal papers. His research interests include machine learning, big data analytics, security and privacy, Internet of Things, software-defined networking, and cloud computing.

Dr. Garg was the recipient of the prestigious Visvesvaraya Ph.D. Fellowship from the Ministry of Electronics and Information Technology under the Government of India (2016–2018), the IEEE ICC Best Paper Award in 2018 at Kansas City, USA and the IEEE TCSC Award for Excellence in Scalable Computing (Early Career Researcher) in 2020. He is the Managing Editor for the *Human-Centric Computing and Information Sciences* (Springer) and an Associate Editor for the *IEEE Network Magazine*, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, Elsevier's *Applied Soft Computing*, and Wiley's *International Journal of Communication Systems*. He is also the Workshops and Symposia Officer for the IEEE ComSoc Emerging Technology Initiative on Aerial Communications. He is/was the Workshop Chair/Publicity Co-Chair for several IEEE/ACM conferences including IEEE INFOCOM, IEEE GLOBECOM, IEEE ICC, ACM MobiCom, and so on. He also guest-edited 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, and *Future Generation Computer Systems*. He is a Member of ACM.



Hui Lin received the Ph.D. degree in computing system architecture from the 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, Fuzhou, China. He is also an M.E. Supervisor with the 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.

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

Then, he continued his research carrier as a Postdoctoral Fellow in information and communication engineering with the Networking Laboratory, Kyung Hee University. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Sejong University, Seoul, South Korea. He has authored or coauthored a substantial number of technical papers in well-known international journals and conferences in the area of information and communication technology, specifically in the fields of: wireless communications and networking, e.g., 5G/6G; Internet of Things; multimedia communication, streaming, adaptation, and QoE; applied machine learning; and security.

Dr. Jalil Piran has been an Active Delegate from South Korea in the Moving Picture Experts Group since 2013 and an Active Member of the International Association of Advanced Materials since 2017. He was the recipient of the IAAM Scientist Medal of the year 2017 for notable and outstanding research in new age Technology and Innovation, Stockholm, Sweden. He has been recognized as the Outstanding Emerging Researcher by the Iranian Ministry of Science, Technology, and Research in 2017. Also, 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 Engineering Group.

Jia Hu received 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 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 serves on the Editorial Board of Elsevier *Computers & Electrical Engineering* 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 a General Co-Chair of the IEEE International Conference on Computer and Information Technology in 2015, International Conference on Ubiquitous Computing and Communications (IUCC) in 2015, and a Program Co-Chair of the IEEE International Symposium on Parallel and Distributed Processing With Applications in 2020, IEEE International Conference on Scalable Computing and Communications in 2019, IEEE International Conference on Smart City in 2018, IEEE International Conference on Cybernetics in 2017, EAI International Conference on Smart Grid Inspired Future Technologies in 2016, etc. He was the recipient of the Best Paper Awards at the IEEE International Conference on Service-Oriented System Engineering in 2016 and IEEE IUCC in 2014.

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 currently 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 or coauthored more than 300 publications, including refereed journals, conference papers, books, and book chapters. Recently, he co-edited a book *Connected Health in Smart Cities* (Springer, 2019). 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.

Dr. Hossain is the Chair of the IEEE Special Interest Group on Artificial Intelligence for Health with IEEE ComSoc eHealth Technical Committee. He is on the Editorial Board of 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 is also a Lead Guest Editor for the IEEE NETWORK, *ACM Transactions on Internet Technology*, *ACM Transactions on Multimedia Computing, Communications, and Applications*, and *Multimedia Systems Journal*. He served as a Guest Editor for the *IEEE Communications Magazine*, IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE (currently JBHI), and IEEE TRANSACTIONS ON CLOUD COMPUTING. He is a Senior Member of the ACM. He is an IEEE ComSoc Distinguished Lecturer.