An Intelligent Privacy Preservation Scheme for EV Charging Infrastructure

Shafkat Islam, Shahriar Badsha, Shamik Sengupta, Ibrahim Khalil, and Mohammed Atiquzzaman

***Abstract*—The electric vehicle (EV) charging ecosystem, being a distinguishable paradigm of IIoT infrastructure, consists of distributed and complex hybrid systems that demand adaptive data-driven cyber-defense mechanisms to tackle the ever-growing attack vectors of cyber-physical systems. We propose an adaptive differential privacy-based federated learning framework for building a collaborative network intrusion detection system model for EV charging stations (EVCS). We use utility optimized local differential privacy to provide data privacy to the local network traffic data of each EVCS. Moreover, we propose a reinforcement learning-based intelligent privacy allocation mechanism at the EVCS level. The main significance of the proposed mechanism is that it can make privacy provisioning adaptive to the extent of privacy breaching rate, and dynamically optimize the privacy budget and the utility to avoid human intervention such as domain knowledge experts. The experimental results confirm the efficacy of our proposed mechanism and achieves appropriate privacy provisioning accuracy to approximately 95%.**

***Index Terms*—Critical energy infrastructure, differential privacy, electric vehicle (EV) charging infrastructure, federated learning, intrusion detection system (IDS), privacy automation, reinforcement learning (RL).**

I. Introduction

IN THE advent of widespread industrial Internet of Things (IIoT) applications, the growth in adopting electric vehicles (EVs) is accelerated due to its divergent benefits, i.e., fuel efficiency, dynamic pricing, genial environmental effects, to name a few. It is expected that about 125 million EVs will be in operation on the road by 2030 [1]. The EV industry needs to facilitate adequate charging infrastructure to EV users to achieve this ambitious figure. The Edison electric utility predicts that approximately 9.6 million public charging ports are required to operate only on U.S. roads by 2030.[1] These charging ports, alternatively known as smart EV charging stations (EVCS), serve as the EVs' access point to the energy infrastructure (i.e., smart grid). Conventionally, the energy infrastructure and the smart EVs exchange information and energy in a bidirectional manner through these EVCS [2]. Hence, appropriate management of EVCS (in terms of privacy protection) is inevitable as it may cause havoc on power grid infrastructure if any of these EVCS is compromised (by the adversary) or even remain unmanaged. Moreover, manual management of privacy provisioning in the EVCS infrastructure is cumbersome since EVCS contains heterogeneous systems as well as diverse kinds of data. The main objective of this work is to develop an automated privacy management mechanism for the EVCS infrastructure.

The EV charging infrastructure usually comprises heterogeneous cyber-physical systems, i.e., mobile devices, autonomous entities, IIoT sensors, among others, which create an EV charging network [3]. To operate its functionality in this network, each EVCS communicates with other entities (i.e., charging service provider or centralized management system) through a protocol commonly known as open charge point protocol (OCPP). Though OCPP provides a standardized protocol for EV charging, it suffers from severe cyber-security threats, such as man-in-the-middle attack, denial of service (DoS), exploitation, reconnaissance, etc. [3]. This vulnerability creates the necessity for establishing an intrusion detection system (IDS) at the EV charging network to differentiate the anomalous traffic from the normal ones, thus, eliminating the adversary from successfully conducting cyberattacks on EVCSs.

Fig. 1 illustrates the traditional collaborative IDS mechanism for the EV charging infrastructure. In the conventional method, each EVCS sends their local network log to the charging service provider (CSP) or third-party vendors to generate the IDS rule or model. This implies severe privacy complication since an adversary can access the network log of a targeted EVCS if the CSP or the transmission channel is compromised. Since network logs usually contain information regarding attacks, i.e., DoS, backdoors, exploits, reconnaissance, worms, etc., EVCSs' are typically disinterested in disclosing such information to other entities. As such, disclosure can have a negative effect on the EVCS's reputation and can even cause economic loss.

Manuscript received 30 October 2021; revised 30 March 2022 and 16 July 2022; accepted 27 August 2022. Date of publication 2 September 2022; date of current version 13 December 2022. Paper no. TII-21-4810. *(Corresponding author: Shafkat Islam.)*

Shafkat Islam is with the Purdue University, West Lafayette, IN 47907 USA (e-mail: shafkat@nevada.unr.edu).

Shahriar Badsha is with the Bosch Engineering, North America, Farmington Hills, MI 48331 USA (e-mail: sbadsha@unr.edu).

Shamik Sengupta is with the University of Nevada Reno, Reno, NV 89557 USA (e-mail: ssengupta@unr.edu).

Ibrahim Khalil is with the School of Science, RMIT University, Melbourne, VIC 3000, Australia (e-mail: khalilrmit@gmail.com).

Mohammed Atiquzzaman is with the University of Oklahoma, Norman, OK 73019 USA (e-mail: atiq@ou.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2022.3203707.

Digital Object Identifier 10.1109/TII.2022.3203707

[1][Online]. Available: https://www.greentechmedia.com/squared/dispatches-from-the-grid-edge/electric-vehicles-and-the-power-grid-roadmaps-from-california-and-new-york

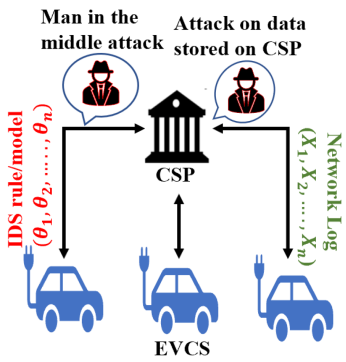

Fig. 1. Traditional collaborative IDS mechanism.

In recent years, machine learning (ML)-based IDS model has become popular in IIoT applications due to its various offerings, such as automated rule generation without human intervention, rigorous rule update scope, etc. [4]. To develop a robust detection model, multiple EVCSs must collaborate since each EVCS possesses a portion of the EVCS network traffic data. However, EVCSs may not be interested in disclosing any traffic information to others since this can reveal the attack information as well, which can discourage EV users from using that compromised EVCS (if it is compromised within its operation cycle). Hence, federated learning [5]-based IDS model is required at the EV charging infrastructure for restricting the adversary at an earlier attack stage.

Although the federated learning-based IDS model can prevent sensitive data disclosure, it fails to eliminate membership inference attack [6] if any of the federated entity becomes compromised. To avoid such membership inference attacks, multiple techniques have been proposed in the literature, such as data anonymization [7], homomorphic encryption [8], etc.; however, these two techniques suffer from deanonymization attack [9], and key distribution and calculation overhead, respectively. On the contrary, differential privacy (DP) [10] can provide a substantial privacy guarantee to the data without any communication and minimal computation overhead. However, naively applying DP (without considering the optimization of utility versus privacy) to the EV charging infrastructure is not appropriate since the DP adversely effects the data utility and EVCS comprises of multiple nontrusted heterogeneous entities. Though the authors in [11] presented the state-of-the-art techniques of privacy provisioning for virtual assistants, such techniques are infeasible for EVCS due to computational or communication costs. Moreover, the existing literature [12], [13], [14] on EVCS does not consider its privacy issues as well. The authors in [15] and [16] stated the blockchain-enabled security solution for IIoT infrastructure and trajectory data mining application, respectively, however, such blockchain techniques may pose additional communication burden on the EVCS infrastructure. Therefore, it motivates us to investigate the performance of adaptive utility optimized local differential privacy (uLDP) in EVCS infrastructure. We outline the main contributions of this work as follows.

1) We propose a collaborative as well as robust IDS framework based on federated learning for the EV charging infrastructure. In this framework, each EVCS engage in IDS model training through sharing the model parameters instead of network traffic data. In this architecture, the EVCSs serve as federated worker and the CSP serve as federated master.
2) We use uLDP for defending membership inference attacks on model parameters. This work is the first attempt to implement uLDP in federated learning setting to the best of our knowledge.
3) We propose an intelligent privacy obfuscation mechanism based on reinforcement learning (RL) to automate the privacy budget allocation process, and thus, avoid human intervention in the privacy provisioning process. This technique can assist IIoT security in advancing the security management process through automating privacy provisioning.
4) We conduct rigorous experiments to confirm the efficacy of our proposed method. Results show that our proposed method can defend against inference attack and allocate an appropriate privacy budget autonomously.

II. Related Works

In this section, we describe the related works, regarding security vulnerabilities of EV energy infrastructure. We also discuss works related to the security issues of federated learning. Finally, we discuss about the research gaps as well.

A. Security Vulnerability in EV Infrastructure

The authors in [2] presented a detailed security analysis of EV charging infrastructure. The authors emphasized the necessity for enhancing data confidentiality and privacy in EV charging systems. In [17], the authors proposed a blockchain-based security solution for EV charging infrastructure. Though it can provide security while charging, it ignores the requirements for data privacy. In [18], the authors also presented a blockchain and fog computing-based distributed EV charging scheme. The authors also claimed that the method was both secure and privacy-preserving. The authors in [19] presented a blockchain-based EV charging and discharging scheme.

Moreover, in [12], [13], and [14], the authors have also discussed EV charging solution. However, the above literature did not consider the security or data privacy issues regarding the EV charging infrastructure. They only consider privacy and security from the users perspective. Since EV charging infrastructure is connected with the electric grid, it is essential to protect the security and privacy of the EV infrastructure.

B. Privacy Issues in Federated Learning

The authors in [20] presented a comparative analysis between local differential privacy and federated learning for ensuring data privacy. However, the authors did not consider the membership inference attack scenario in the federated learning framework. In [21], the authors proposed a differential privacy-based federated learning framework for defending inference attacks. The authors added perturbation during model sharing. The authors

in [22] presented a blockchain-based federated learning scenario for secure data sharing. The scheme can protect data privacy by sharing models instead of raw data, though the authors do not consider the inference attack scenario in such sharing system.

Moreover, in [23] and [24] the authors proposed a federated learning-based data sharing scheme for protecting data privacy. Among these articles, the authors in [23] considered the inference attack scenario and proposed a differentially private federated learning framework. Though there exist works regarding defending the inference attack in a federated learning environment; however, the existing literature fails to address the issue of privacy provisioning since understanding the tradeoff between privacy budget and model efficacy is a difficult task [5].

Therefore, we envision developing an adaptive privacy-preserving federated learning framework for EV charging infrastructure to facilitate the EV infrastructure in developing a robust anomaly detection model (to protect EV charging stations from being compromised) through collaboration while considering the inference attack scenario and also the issues related to privacy provisioning.

III. Problem Formulation

This section briefly describes the challenges of building a privacy-preserving collaborative intrusion detection model for EV energy infrastructure and underlying assumptions.

A. Distributed EV Charging Infrastructure

We consider that the EV charging infrastructure consists of $\mathbf{n}$ charging stations and one global CSP. The charging infrastructure can be described by the following set in (1)

$$S_{\text{CSP}} = \{\text{EVCS}_1, \text{EVCS}_2, \text{EVCS}_3, \ldots\ldots, \text{EVCS}_n\} \quad (1)$$

where each EVCS (alternatively, CS) is located into different geographic locations and each EVCS (or ith EVCS) can communicate with other peer EVCSs and the CSP for conducting functional operations. We also consider that the CSP is a vendor organization responsible for providing energy resource to EVs. The EVCSs serve as an edge buffer point between the EVs and the energy grid. To keep things simple, we build a single CSP model; however, there can be multiple CSPs in real-world scenarios. This work is extendable for those scenarios as well.

B. Network Traffic Dataset

We consider that each charging station (CS) contains a network traffic logger to log its traffic information. As each CS requires to communicate with different entity during its operational life cycle, the network traffic log-set (or dataset) for ith EVCS, $D_i = \{x, y\}$, is distinguishable (in terms of log-contents and log-size) from the log-set of any other jth$(i \neq j)$ EVCS. Usually the log-set contains information regarding network flow features (i.e., IP addresses, etc.), basic network features (i.e., packet count, retransmission or drop information), content features (i.e., sequence number, window size), and time features (i.e., start time, jitter) [25]. In the dataset, x represents each traffic data's feature set, and y represents the corresponding label (normal traffic or anomalous traffic). We also consider that there exists an identical standard mechanism for labelling each traffic data at each EVCS. Hence, the log-set eventually will have two distinct classes (i.e. normal and anomaly). Among these two classes, the EVCS is conservative regarding the anomaly class members since this class contains the attack information regarding that EVCS. In this article, the anomaly class data is regarded as sensitive whereas normal class data is regarded as nonsensitive.

C. Attack Vectors

In this work, we consider that network traffic data for each EVCS is confidential as such dataset contains attack information of the corresponding EVCS. An adversary or even a competing peer EVCS can become interested in such attack information to breach the vulnerable EVCS or reveal such data to the EVs to demean the reputation of the vulnerable EVCS. Adversaries can probe the vulnerable EVCS and conduct an attack on energy grids through that EVCS, whereas achieving additional economic benefits can drive the latter motivation. In this work, we consider one attack vector, i.e, membership inference (MI).

1) Membership Inference Attack: We consider a trustless collaborative learning environment for the EV energy infrastructure. Each of the entities in S_{CSP}, including the CSP itself, is interested in breaching the peer entity's network log-set (or dataset). To avoid traffic log exchange in raw format (which can cause excessive communication overhead and makes it easier for the adversary to breach into the log-set), we adopt a federated learning-based approach. In federated learning, peers exchange their model parameters which seem to preserve data privacy to some extent. However, in [6], the authors have shown that adversaries can conduct attacks only knowing the ML model parameters to infer about the training dataset of the model. This type of data inference attacks is termed as MI attack in literature. In the context of this work, MI is the most prevalent and dominant attack vector.

D. Issues in Federated Learning

Though federated learning can facilitate EV energy infrastructure to develop robust learning models, it suffers from multiple challenges, i.e., expensive communication, system heterogeneity, statistical heterogeneity, and privacy concerns [5]. We only focus on the privacy concerns of the federated learning environment in this work. We consider that each EVCS can add differentially private noise to its local network log-set (or dataset) to preserve the model privacy (and defend inference attacks) during federated training. However, it is challenging to understand the tradeoff between noise level and model accuracy, which requires an expert's intervention to determine such noise levels. This article envisions automating such noise level addition process to minimize human intervention, and optimize the model accuracy.

This article aims to develop a resilient (in terms of defending MI and man-in-the-middle (MITM) attacks) and adaptive federating learning environment for the EV energy infrastructure and automate the privacy provisioning mechanism.

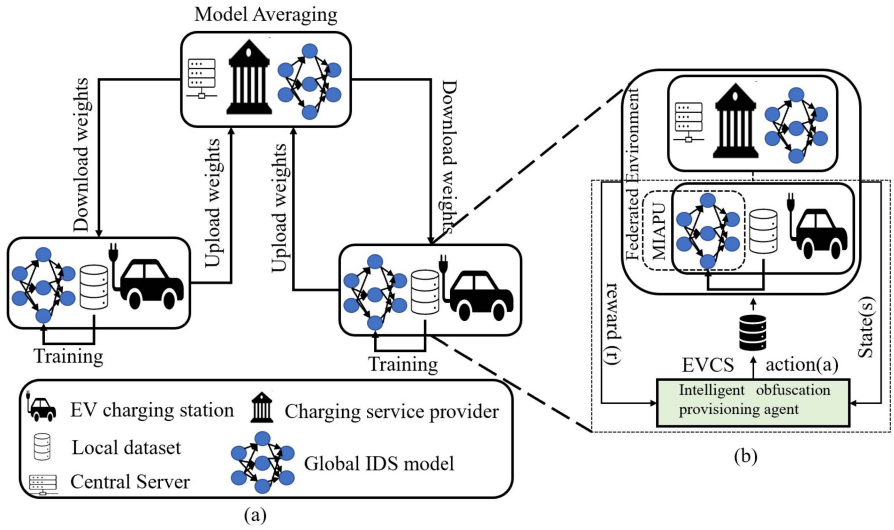

Fig. 2. System architecture: (a) Federated learning based collaborative IDS for EV charging infrastructure, (b) RL-based intelligent obfuscation mechanism for EVCS.

IV. Proposed ADPFL Mechanism

To enhance the EV energy infrastructure's operational efficacy, it is essential to develop a resilient learning environment that can ensure data privacy and improve operational performance. This section presents an adaptive privacy-preserving federated learning environment for EV charging infrastructure to detect anomalous traffic and automate the privacy provisioning mechanism.

A. Federated Anomaly Detection Mechanism

Federated learning [5], being a novel distributed learning paradigm, has become popular in divergent applications, i.e., Internet of Things (IoT) network, smart industry, edge computation, mmWave communication, etc. The goal of federated learning is to learn a single statistical global model from data stored in multiple distributed remote devices without sharing any training data [5]. This distinct attribute delineates federated learning from other traditional ML algorithms and makes this architecture suitable for sensitive datasets.

Usually, network traffic data of EVCS is considered private if it contains attack (or threat) information, which can cause significant reputation degradation (or vulnerability if adversaries exploit such logs for conducting attacks) if such attack information is disclosed to others. Hence, EVCS's typically remains conservative regarding such network logs, let alone sharing with any other organization or entity (i.e., CSP or other EVCS). To tackle with such issues, we envision to develop a robust global anomaly detection model for EV charging infrastructure from the distributed local network logs of different EVCS using the federated learning technique.

Fig. 2(a) illustrates the federated anomaly detection architecture for the EV charging stations. This federation aims to minimize the following optimization function as we describe in (3):

$$\min_{w} \left[\sum_{i=1}^{n} p_i f_i(w) \right]. \tag{2}$$

n denotes the quantity of EVCS that take part in the collaborative process, p_i is a hyperparameter that is used for tuning the relative impact of each EVCS (usually, $p_i = 1/n$ or D_i^n/n), and $f_i(w)$ denotes the local objective function for each (or ith) EVCS, whereas

$$f_i(w) = (1/D_i^n) \left(\sum_{ji=1}^{D_i^n} f_{ji}(w; x_{ji}, y_{ji}) \right) \tag{3}$$

in which D_i^n denotes the log-size of the ith EVCS, and this local objective function represents the empirical loss over the local dataset (D_i).

We assume that the EVCS and the CSP agree on a global deep neural network architecture at the beginning of the learning phase $(t = 0)$. We also assume that each EVCS also uses an identical learning rate (μ), and each entity in the learning environment is honest but curious. It implies that the EVCS and the CSP perform their duties during the learning phase perfectly while remaining curious about the dataset of peers. Algorithm (1) presents the federated learning process for EVCS in brief. We ignore the channel loss probability during model weight transmission; hence, each weight transmission is considered successful.

B. uLDP-Based Privacy Protection

DP [26] provides a mathematical foundation to formalize the notion of privacy. It can provide a substantial privacy (ϵ-DP) guarantee to a dataset. A mechanism M is defined as ϵ differentially private if (4) is satisfied

$$P[M(D) \in S] \leq e^{\epsilon} P[M(D') \in S] \tag{4}$$

Algorithm 1: Federated Learning for EVCS.

Input: Initial global model parameters, w_0
Output: Trained model parameter, w_N
Requirement: Local log-set or dataset (D_i)
for $t = 1, 2, 3, \ldots, N$ do
  Local Update (EVCS)
  for EVCS i in parallel do
    $w_{t+1}^i \leftarrow w_t - \mu \nabla loss(w; x_i, y_i)$
    Send w_{t+1}^i to CSP
  end
  Global Update (CSP)
  $w_{t+1} \leftarrow \left[\sum_{i=1}^{n} (1/n) w_{t+1}^i \right]$
  Send w_{t+1} to EVCS
end

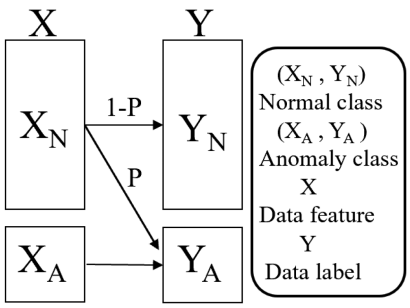

Fig. 3. Illustration of uLDP mechanism in the proposed ADPFL scenario. The scheme provides $\epsilon-$LDP only for the Y_A class. There is no transition from X_A to Y_N; hence, every sample in Y_N reveals the corresponding feature set in X_N.

where D and D' datasets which at-least by single entry and S denotes a subset of the query outcome.

Local differential privacy (LDP) can provide equal privacy protection, without the need for any third-party organization, for all samples in a given dataset (D^i) irrespective of a sample being sensitive or not. This extensive obfuscation mechanism causes to decrease utility to a great extent. On the other hand, utility optimized LDP (uLDP) [26] can guarantee privacy protection (equivalent to LDP) only to the sensitive data with substantial improvement in data utility. This attribute motivates us to adopt uLDP for providing privacy protection to our EV charging infrastructure setting.

In the proposed EVCS anomaly detection model, each EVCS contains a network log that includes data of two distinct classes, i.e., 1) normal traffic; and 2) anomalous traffic. In contrast, only the anomalous traffic class is considered sensitive, and usually, EVCSs' are unwilling to disclose any of their attack information. Fig. 3 illustrates the training set obfuscation mechanism for the EVCS. According to this mechanism, the normal class's data points label is inverted with probability p. By definition of uLDP, this obfuscation technique provides $(X_A, Y_A, ln(1/p))$ LDP and preserves privacy only for the sensitive anomalous class dataset (X_A, Y_A). We can define the privacy budget (ϵ) by the following equation in (5):

$$\epsilon = ln(1/p). \tag{5}$$

However, it does not provide any privacy to the normal class dataset. This implies that an attacker can make an inference guess on normal class data with hundred percent confidence while failing to do that for the anomaly class data. Since it is not required to protect the nonsensitive normal class data, this type of disclosure does not hold any significance. Therefore, using this obfuscation technique, the EVCSs' can obfuscate their local training dataset and make the anomaly data indistinguishable.

In this architecture, we assume that the network logger is responsible for obfuscation as well. It continuously obfuscates after a certain interval (or whenever a substantial number of new traffic data is stored in the log). We also assume that the traffic logger is a secure entity and no other entity can access the data before it is obfuscated. The study of attack vectors in the traffic logger is beyond the scope of this article.

C. RL-Based Intelligent Privacy Provisioning

RL [27] is an adaptive ML algorithm that can facilitate conventional mechanism with intelligence without the need for any supervision. Distinguishable attributes of RL is a feedback loop (or trial and error) based on search for optimal action set and delayed rewards. These attributes motivates researchers in deploying RL in divergent sectors, i.e. mmWave communications, smart grid, EVs, etc.

The RL mechanism consists of a learning agent along with a set of states (S), actions (A), interactive environment (E), and a set (or function) of rewards (R). In every state (S) the agent takes an action (A) and ends up with a new state (S') which we can describe as, $S \times A \xrightarrow{S'} R$. The RL agent learns an optimal decision-making policy (π) that can maximize the following value function$(V^{(\pi)})$ as described in [28]:

$$V^{(\pi)}(s) = \mathbf{E}\left[\sum_{t=0}^{\infty} \gamma^t r_t | s \right] \tag{6}$$

where γ is defined as the discount factor for rewards of future actions, r_t is termed as immediate reward, and s represents the state at time t. $V^{\pi^*}(s)$ represents the state-value function for the policy π[27].

The action-value function (alternatively, $(Q^{\pi}(s, a))$) is used for determining optimum action in each state. In (7) we describe the action-value function [27]. The action-value function provides quantitative evaluation regarding an action in a particular state, whereas, value function evaluates the policy

$$Q^{\pi}(s, a) = \mathbf{E}\left[\sum_{t=0}^{\infty} \gamma^t r_t | s, a \right]. \tag{7}$$

Therefore, the optimal action-value function and optimal policy can be defined as of (8) and (9)

$$Q^*(s, a) = \overset{\max}{\pi}\, Q^{\pi}(s, a) \tag{8}$$

$$\pi^*(s) = \overset{\arg\max}{\pi}\, Q^*(s, a). \tag{9}$$

1) Context-Aware Intelligent Obfuscation Mechanism: The addition of differential privacy in training data will cause degrade in the federated model performance. It is not easy to understand and balance the tradeoff between privacy and model performance, both theoretically and empirically [5]. In this work, we assume that each EVCS adds obfuscation at its local level and EVCS does not disclose it to others since disclosing the obfuscation level will make the job easier for the adversary to conduct an inference attack. Moreover, the EVCS's network log-set will differ over time during its operational life cycle. Furthermore, it is not desired to have excessive privacy while the inference attack probability is significantly low. Thus, each EVCS requires an adaptive obfuscation mechanism that can determine the privacy budget (ϵ) depending on the dynamics of the learning environment.

Fig. 2(b) illustrates the workflow of the intelligent obfuscation provisioning agent. In the figure, membership inference attack performing unit (MIAPU) represents the membership inference attack possibility gauging unit. The MIAPU unit utilizes standard membership inference gauging technique, i.e., mia [29], determine the attack possibility of each distinct EVCS at a particular privacy budget. This unit and the agent are both located in the EVCS. To keep the figure simple, we only show the obfuscation workflow for a single EVCS. We assume that such identical architecture is prevalent in all the other EVCSs. In the following we describe the detailed obfuscation provisioning process.

State space: In this architecture, the obfuscation provisioning agent considers the existing contextual information (i.e., federated model accuracy (f_A), MI attack accuracy (m_A), and obfuscation level (p)) for determining the appropriate privacy budget. The state space for an agent can be defined as a tuple of these three parameters, i.e., $S = (f_A, m_A, p)$. The agent receives the f_A value from the CSP, and m_A value from MIAPU.

Action space: We assume that the obfuscation agent makes an obfuscation decision whenever a new traffic log-set arrives in the EVCS. Thus, it becomes an event-driven decision-making process. By observing the federated environment's current state, the agent makes one of the decisions as described in (10). Therefore, we can define the action-space as $A = \{\text{increase},\ \text{decrease},\ \text{static}\}$.

$$d_m^i = \begin{cases} 0, & \text{increase},\ \epsilon \\ 1, & \text{decrease},\ \epsilon \\ 2, & \text{static},\ \epsilon. \end{cases} \tag{10}$$

We assume that the agent increases privacy budget (ϵ) when the MI attack accuracy (m_A) is over a threshold (x), decreases when it is far less than the threshold (x). However, increasing privacy will eventually reduce the federated performance. Hence, the agent must make a tradeoff decision between privacy and efficacy dominated by the threshold value (x). For example, in binary classification tasks, if the inference accuracy becomes less than half, the inference attack becomes equivalent to random guessing [6].

Reward function: Reward motivates an agent to make decision towards the objective function. In this article, the objective for the agent is to maintain the inference attack accuracy around random guessing. We define the reward function for the agent as in (11)

$$\beta_1 = \eta_1 f_A + \eta_2 \left| 1 - e^{(\alpha x + m_A)/c} \right| \tag{11}$$

where η_1 and η_2 are the weight factors, α and c are normalizing constants. Alternatively, the first term in the reward function can be viewed as the gain for the defender (or the gain for federated accuracy) and the second term is the attacker's gain. We assume that the attacker's gain is of two folds, one is for the higher inference accuracy and the other is for lower federated accuracy due to privacy measures. This reward function motivates the agent to set the privacy budget around the threshold value (x) which is described in the previous section.

State transition: The agent makes a privacy decision based on the present state (s) status, alternatively, the $Q(s, a)$ value. The agent chooses the greedy policy to make a decision at any state, which we describe by the following equation in (12). Here, q is the probability of taking random action

$$\pi(s) = \begin{cases} \text{random action from } A;\ (q) \\ \arg\max\limits_{\pi} Q(s, a);\ (1 - q). \end{cases} \tag{12}$$

V. Performance Evaluation and Discussion

In this section, we evaluate the efficacy of the proposed adaptive differentially private federated learning (ADPFL) framework. We divide our evaluation process into two different parts. In the first part, we evaluate the efficacy of uLDP in defending the membership inference attack in a federated learning setting. In the second part, we gauge the performance of the intelligent obfuscation agent in successfully provisioning privacy budget to the local dataset. We also evaluate its resiliency in terms of handling false federated accuracy (f'^A) injection attack by the CSP. We describe the detailed results and simulation setups in the following.

A. Simulation Setup

We assume that the EV charging infrastructure consists of n (we use $n = 2$) EVCS. Each EV charging station contains a nonidentical IDS dataset. We collect the IDS dataset from the benchmark UNSW-NB-15 [25]. We assign 350 000 training data samples to each of the EVCS and 175 000 samples to the CSP as federated test-set. We also assure that the training samples in each EVCS are not identical to the other, and also, the testing samples are not identical to any of the training sample. To validate the proposed method, we also conduct experiments using the classic binary breast cancer classification dataset [30]. This multivariate dataset consists of 32 real-valued attributes and 569 samples. We keep the similar federated learning simulation set up to make the validation realistic. Here, each federated worker is assigned to 225 random data samples as the training set and the federated server contains the rest 119 data samples for testing. We also utilize the uLDP as the privacy technique. The detailed results of validation is described in Section V-D. We conduct the experiments using Python on a windows machine with 16-GB RAM, and the processor is built by Intel. We also utilize the keras library to simulate the federated learning process

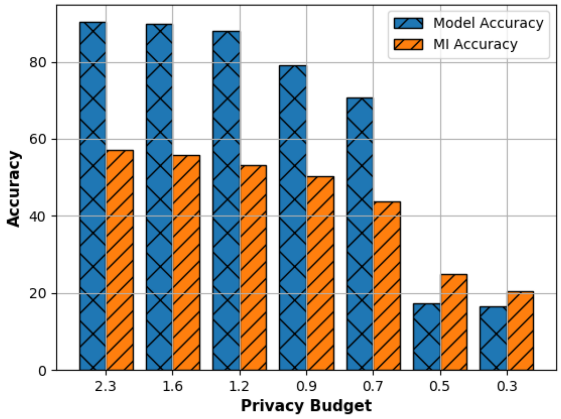

Fig. 4. Performance of MI attack model and federated model with respect to different privacy budget (ϵ) for anomaly dataset.

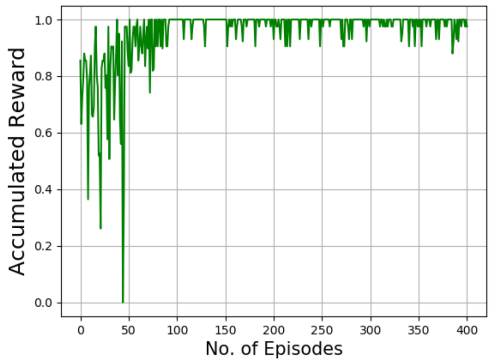

Fig. 5. Accumulated reward for the intelligent privacy provisioning agent.

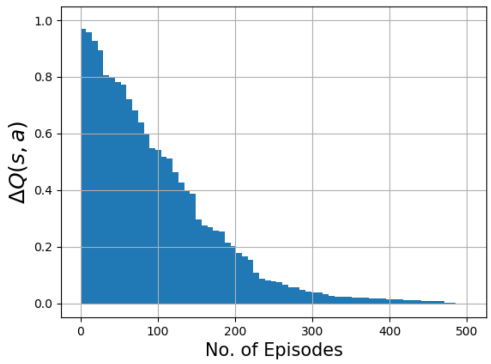

Fig. 6. Convergence analysis of the intelligent privacy provisioning agent.

and mia [29] library to determine the membership inference attack accuracy of each local model.

To evaluate the performance, we consider different evaluation matrix. In assessing the performance of the federated learning, we consider accuracy as an evaluation matrix. In this regard, accuracy represents the federated framework's test accuracy, which is defined as the percentage of correctly classified samples from the testing set. For gauging the inference attack, we also calculate the attack accuracy. In this regard, this implies the percentage of correctly inferred data from the local training dataset, only looking into the local model. To determine the efficacy of the intelligent obfuscation agent we consider reward utility and successful provisioning rate (in percentage) as gauging matrix. The reward utility (alternatively, cumulative reward utility) determines whether the agent is learning from its experience or not, whereas, the successful provisioning rate determines how correctly the agent can set the privacy budget based. In this regard, we consider correct provisioning if the agent can set the privacy budget such that the MI attack accuracy is close to a predefined threshold value (x).

B. Performance Analysis Under Different Privacy Budget

We conduct a membership inference attack on each of the two local models described in [6]. We evaluate the attack model's performance and present the average attack accuracy of the two local models in Fig. 4. From the figure, we can see that the attacker's highest inference accuracy is approximately 57% at privacy budget $\epsilon = 2.3$. For the sake of simplicity, we also assume that both the local models utilize identical privacy budget. As we continue to decrease the privacy budget (ϵ) we observe that the attack accuracy continually decreases, and finally, it becomes as low as 20.4% at $\epsilon = 0.3$. This justifies the fundamental notion of differential privacy. To achieve better privacy in any model, the privacy budget should be lower. However, this has a negative impact on the federated accuracy, which we discuss in the following paragraph.

Fig. 4 also illustrates the relationship between federated accuracy and privacy budget (ϵ). The highest federated accuracy we can achieve is approximately 90% at $\epsilon = 2.3$. As we decrease the privacy budget, the federated accuracy also decreases since with the increase in privacy budget the amount of inverting training labels is also increasing. The model achieves lowest federated accuracy of 16.5% at $\epsilon = 0.3$. Thus, the model achieves better privacy at the cost of loss in model utility. Therefore, it is desired to find an optimum privacy point (where inference attack equivalents to random guessing) at which the privacy protection is acceptable and the federated accuracy is also higher.

C. Determining the Efficacy and Convergence Analysis of Intelligent Obfuscation Mechanism

This section evaluates the intelligent obfuscation agent's performance in terms of accumulated reward, action-value function convergence, and successful privacy provisioning rate. Fig. 5 illustrates the accumulative reward over episodes for the defender in distinct learning rate of 0.01. In this regard, we use the term defender to represent the obfuscation agent's purpose; hence, both are an identical entity (we use defender and obfuscation agent interchangeably in this section). We observe that accumulative reward for the defender increases over the episodes. This trend illustrates that the defender learns the optimum policy over episodes, and it converges after sufficient episodes are executed. We depict the convergence of the agent in Fig. 6. In this figure, the change in action-value function $(\Delta Q(s, a))$ is illustrated over the episodes. As we can observe that the difference of action-value function approaches to zero over time,

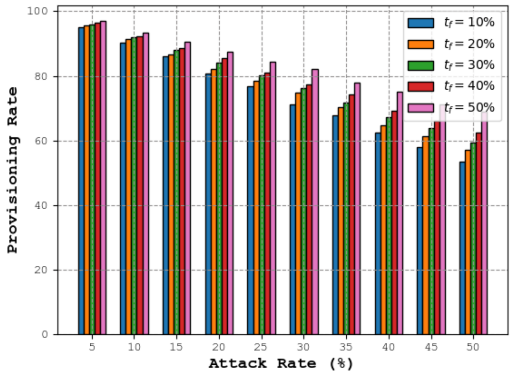

Fig. 7. Analysing the resiliency of the intelligent obfuscation agent for anomaly detection dataset.

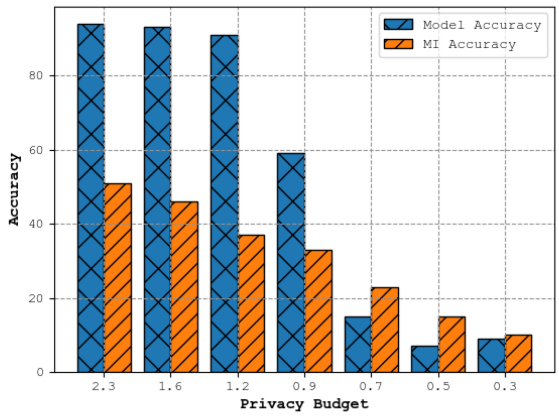

Fig. 8. Performance of MI attack model and federated model with respect to different privacy budget (ϵ) for breast cancer dataset.

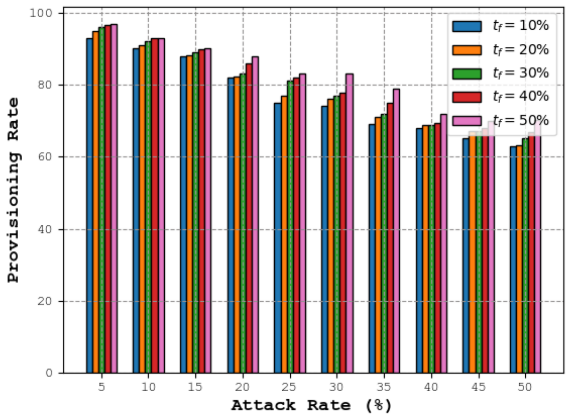

Fig. 9. Analyzing the resiliency of the intelligent obfuscation agent for breast cancer dataset.

we can say that the Q-table begins to converge and the intelligent privacy provisioning agent learns the optimal privacy budget selection policy. This convergence also illustrates that the agent can determine appropriate action over the episodes based on its interaction with the environment. Since we define the reward function such that it takes care of both the federated accuracy (f_A) and attacker accuracy (m_A), this convergence finds the optimal point at which the inference accuracy equivalents to the random guessing (or threshold x). We leave this threshold value (x) as a hyperparameter, and it can vary depending on the application and data sensitivity.

Fig. 7 illustrates the resiliency of the obfuscation agent. Since the obfuscation agent determines its current state based on values (f_A) from the CSP (and we consider CSP as an untrusted entity), the CSP can intentionally send false federated accuracy values (f_A) to make the agent in taking incorrect decision regarding privacy budget (ϵ). Thus, the agent can hold a misconception regarding its current state if such adversarial activity occurs. We assume that if the agent has any such distorted information regarding its state, it will eventually have misconception of its current state and, thus, it will determine the incorrect privacy budget (ϵ). The aftermath of this effect is that the agent will require longer steps to reach the optimum privacy budget (ϵ) point.

We conduct simulations for different attack rates (in percentage) and observe the successful provisioning rate (p_r). In this regard, we define a tolerance factor (t_f) that determines the tolerable increment in step size. This hyperparameter is application dependent. With this parameter's increase, the attacker gets a higher possibility to conduct the inference attack since the privacy provisioning is delayed (by the increment in step size). From the figure, we can observe that as the attack rate increases, the provisioning rate decreases, but the decline rate depends on the tolerance factor (t_f). If t_f is large, the decrease rate is lower.

Hence, we can conclude from the above discussion that the proposed ADPFL mechanism can mitigate membership inference attack during federated learning while intelligently determining the appropriate privacy budget ϵ.

D. Validation

To validate the proposed method, we analyze the results of our method for the breast cancer classification task [30]. This is a classical binary classification dataset and we utilize this dataset to test the ADPFL method. Since the ADPFL is proposed for the binary anomaly detection for EVCS infrastructure, this method should be plugable to other binary classification tasks with appropriate modifications. Hence, we validate the proposed method using binary breast cancer classification task. We keep the number of federated worker $n = 2$ for this dataset also and split the training set equally in two parts and keep the test-set to the central federated server. Fig. 8 illustrates the relationship between federated accuracy and privacy budget for the breast cancer dataset and Fig. 9 illustrates the privacy provisioning accuracy which is approximately 96% for lower attack rates. Thus, the proposed ADPFL is also effective for the breast cancer dataset.

VI. Conclusion

Enhancing security at EV energy infrastructure (or IIoT infrastructure) is challenging due to its dynamic and complex architecture. Data-driven security management can play a pivotal role in this regard. However, deploying data-driven security solutions at EV energy infrastructure requires overcoming challenges, i.e., data scarcity and data privacy. In this regard,

federated learning can become a game-changing solution; however, it also has to overcome challenges in defending against inference attack and privacy provisioning. This article presented an adaptive privacy-preserving federated learning framework that could protect data privacy and automate the privacy provisioning (determine the privacy budget) process. Simulation results showed that the proposed mechanism can defend against inference attack and allocate an appropriate privacy budget to optimize the model's accuracy and privacy. The limitation of this work is that the proposed method was tested for the binary classification tasks, however, we leave it as our future task to consider multiclass classification tasks and provisioning privacy at the granular level to optimize the utility of each class. Moreover, we will consider the security vulnerabilities (i.e., if any federated worker or server intentionally transmits wrong parameters) and adopt lightweight blockchain-based solutions for enhancing the security of the learning environment.

REFERENCES

[1] T. Bunsen et al., "Global EV outlook 2018: Towards cross-modal electrification," 2018. Accessed: Jan. 10, 2021. [Online]. Available: https://libraryguides.vu.edu.au/ieeereferencing/webbaseddocument

[2] J. Antoun, M. E. Kabir, B. Moussa, R. Atallah, and C. Assi, "A detailed security assessment of the EV charging ecosystem," *IEEE Netw.*, vol. 34, no. 3, pp. 200–207, May/Jun. 2020.

[3] C. Alcaraz, J. Lopez, and S. Wolthusen, "OCPP protocol: Security threats and challenges," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2452–2459, Sep. 2017.

[4] Z. Zhang, Y. Cao, Z. Cui, W. Zhang, and J. Chen, "A many-objective optimization based intelligent intrusion detection algorithm for enhancing security of vehicular networks in 6G," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5234–5243, Jun. 2021.

[5] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, May 2020.

[6] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *Proc. IEEE Symp. Secur. Privacy*, 2017, pp. 3–18.

[7] A. Majeed and S. Lee, "Anonymization techniques for privacy preserving data publishing: A comprehensive survey," *IEEE Access*, vol. 9, pp. 8512–8545, 2021.

[8] H. Karim and D. B. Rawat, "TollsOnly please—Homomorphic encryption for toll transponder privacy in internet of vehicles," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2627–2636, Feb. 2022.

[9] W. Peng, F. Li, X. Zou, and J. Wu, "A two-stage deanonymization attack against anonymized social networks," *IEEE Trans. Comput.*, vol. 63, no. 2, pp. 290–303, Feb. 2014.

[10] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial Internet of Things," *IEEE Trans. Ind. Inform.*, vol. 14, no. 8, pp. 3628–3636, Aug. 2018.

[11] T. Bolton, T. Dargahi, S. Belguith, M. S. Al-Rakhami, and A. H. Sodhro, "On the security and privacy challenges of virtual assistants," *Sensors*, vol. 21, no. 7, 2021, Art. no. 2312.

[12] Y. Cui, Z. Hu, and H. Luo, "Optimal day-ahead charging and frequency reserve scheduling of electric vehicles considering the regulation signal uncertainty," *IEEE Trans. Ind. Appl.*, vol. 56, no. 5, pp. 5824–5835, Sep./Oct. 2020.

[13] L. Zhang, V. Kekatos, and G. B. Giannakis, "Scalable electric vehicle charging protocols," *IEEE Trans. Power Syst.*, vol. 32, no. 2, pp. 1451–1462, Mar. 2017.

[14] Y. Li and B. Hu, "A consortium blockchain-enabled secure and privacy-preserving optimized charging and discharging trading scheme for electric vehicles," *IEEE Trans. Ind. Inform.*, vol. 17, no. 3, pp. 1968–1977, Mar. 2021.

[15] A. H. Sodhro, S. Pirbhulal, M. Muzammal, and L. Zongwei, "Towards blockchain-enabled security technique for industrial Internet of Things based decentralized applications," *J. Grid Comput.*, vol. 18, no. 4, pp. 615–628, 2020.

[16] R. Talat, M. S. Obaidat, M. Muzammal, A. H. Sodhro, Z. Luo, and S. Pirbhulal, "A decentralised approach to privacy preserving trajectory mining," *Future Gener. Comput. Syst.*, vol. 102, pp. 382–392, 2020.

[17] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, 2018.

[18] H. Li, D. Han, and M. Tang, "A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3189–3200, Sep. 2021.

[19] Y. Li and B. Hu, "An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2627–2637, May 2020.

[20] H. Zheng, H. Hu, and Z. Han, "Preserving user privacy for machine learning: Local differential privacy or federated machine learning?," *IEEE Intell. Syst.*, vol. 35, no. 4, pp. 5–14, Jul./Aug. 2020.

[21] K. Wei et al., "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 3454–3469, 2020.

[22] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Trans. Ind. Inform.*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020.

[23] B. Zhao, K. Fan, K. Yang, Z. Wang, H. Li, and Y. Yang, "Anonymous and privacy-preserving federated learning with industrial big data," *IEEE Trans. Ind. Inform.*, vol. 17, no. 9, pp. 6314–6323, Sep. 2021.

[24] A. Fu, X. Zhang, N. Xiong, Y. Gao, H. Wang, and J. Zhang, "VFL: A verifiable federated learning with privacy-preserving for big data in industrial IoT," *IEEE Trans. Ind. Inform.*, vol. 18, no. 5, pp. 3316–3326, May 2022.

[25] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf.*, 2015, pp. 1–6.

[26] T. Murakami and Y. Kawamoto, "Utility-optimized local differential privacy mechanisms for distribution estimation," in *Proc. 28th USENIX Secur. Symp.*, 2019, pp. 1877–1894.

[27] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*. Cambridge, MA, USA: MIT Press, 2018.

[28] X. Xu, D. Hu, and X. Lu, "Kernel-based least squares policy iteration for reinforcement learning," *IEEE Trans. Neural Netw.*, vol. 18, no. 4, pp. 973–992, Jul. 2007.

[29] B. Kulynych and M. Yaghini, "MIA: A library for running membership inference attacks against ML models," Sep. 2018. [Online]. Available: https://doi.org/10.5281/zenodo.1433744

[30] D. Dua and C. Graff, "UCI machine learning repository," 2017. [Online]. Available: http://archive.ics.uci.edu/ml

Shafkat Islam received the M.S. degree in computer science and engineering from the University of Nevada, Reno, NV, USA, in 2021. He is currently working toward the Ph.D. degree in computer science with Purdue University, West Lafayette, IN, USA.

His research outcomes have been published in top venues and high-impact journals and magazines including IEEE NETWORK, IEEE IoT JOURNAL, IEEE International Symposium on World of Wireless Mobile and Multimedia Networks (WoWMoM), IEEE Local Computer Networks Conference (LCN), and so on. His current research interests include responsible AI, cybersecurity, and connected autonomous vehicles.

Shahriar Badsha received the Ph.D. degree in computer science and software engineering from RMIT University, Melbourne, Australia, in 2019.

He is currently working as a Senior Security Engineer with Bosch Engineering, MI, USA. Before joining Bosch, he served as an Assistant Professor in cybersecurity in Computer Science and Engineering at the University of Nevada, Reno. He was also with Data61, Commonwealth Scientific and Industrial Research Organisation (CSIRO), Melbourne.

Shamik Sengupta received the Ph.D. degree in electrical engineering and computer sciences from the University of Central Florida, Orlando, FL, USA, in 2007.

He is the Executive Director of the Cybersecurity Center, University of Nevada, Reno, (UNR), NV, USA, and a Professor with the Department of Computer Science and Engineering. He has authored or coauthored more than 150 international conferences and journal publications including IEEE GLOBECOM 2008 best paper award, International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS) 2017 best paper award, and IEEE CCWC 2020 best paper award. His research interests include various cybersecurity issues such as vulnerability assessment and malware analysis, security and privacy in cybersecurity information exchange, anomaly detection in cyber-physical systems, machine learning, network security, honeypot as well as cognitive radio and DSA networks, game theory, network economics and self-configuring wireless mesh networks.

Prof. Sengupta was the recipient of NSF CAREER award in 2012, UNR CSE Best Researcher award in 2015–2016 and 2017–2018, UNR College of Engineering Excellence Award 2018, University of Central Florida CECS Distinguished Alumni Honor award (Department of Electrical and Computer Engineering) 2018, and the UNR Ralph E. & Rose A. Hoeper Professorship Award 2019.

Ibrahim Khalil received the Ph.D. degree from the University of Bern, Bern, Switzerland, in 2003.

He is a Professor in computer science and software engineering with RMIT University, Melbourne, Australia. He has several years of experience in Silicon Valley-based companies working on Large Network Provisioning and Management software. His research interests include privacy, blockchain, network and data security, and secure data analysis including Big Data security.

Mohammed Atiquzzaman is the Edith Kinney Gaylord Presidential Professor with the School of Computer Science at University of Oklahoma, Norman, OK, USA.

He is the Editor-in-Chief of *Journal of Networks and Computer Applications*, the founding Editor-in-Chief of *Vehicular Communications*, and has served on the editorial boards of many journals, including *IEEE Communications Magazine, IEEE Journal on Selected Areas in Communications*, etc.