# Privacy-Preserving Deep Reinforcement Learning in Vehicle AdHoc Networks

Usman Ahmed
Western Norway University of Applied Sciences, Norway
Jerry Chun-Wei Lin
Western Norway University of Applied Sciences, Norway
Gautam Srivastava
Brandon University, Canada
China Medical University, Taiwan

***Abstract*—The increasing number of road vehicles results in more fatalities and accidents. Thus, the manufacturing industry is working on driver safety to secure and safe transportation in Vehicle Adhoc networks. In addition, the mobile vehicles run in the geographical zone and communicate roadside units over the wireless medium with a certain radius. The Internet of Vehicles has become a new network type where vehicles communicate with the application over public networks. This results in an increase in data exploration and threats related to network security. We propose the deep reinforcement learning method to sensitize the private information for a given vehicle connect over Vehicle Adhoc networks, maintaining a balance between security and privacy through any sanitization process. Furthermore, we provide a set of recommendations and potential applications for the Vehicle Adhoc networks as use cases.**

## I. Introduction

A Mobile AdHoc Networks (MANET) are a dynamic network technology that enables self-configuration, infrastructure-less, and autonomous [1]. Vehicle Adhoc Networks (VANET) is a sub-type of MANET, in which vehicle nodes communicate over the wireless network [1]. The vehicle node frequently joins and leaves the network due to topology changes dynamically, as mentioned in Fig. 1. The major components include vehicles, Road Side Units (RSU), vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-infrastructure (I2I). Another significant difference between MANETs and VANETs is that the rate and type of vehicular nodes cannot be predicted in advance that results in a progressive density of random, asymmetrical vehicles and mostly unknown [1]. With the implementation of IoT technology, VANETs evolve to become more dynamic, reliable, and highly flexible in solving those challenges. This results in advances in both applications and services known as IoV, short for the Internet of Vehicles. IoV infrastructure [2] is illustrated in Fig. 1. However, the advances always come with exposure to security concerns that impact the trust between the vehicle node and network. VANETs are generally restricted to a smaller scale than IoV. IoV has integrated vehicles connected over a global network where vehicular infrastructure and the Internet are connected, providing a collection of both applications and services for vehicles [2].

Moreover, the VANETs nodes frequently come and go from the network due to many constraints like tall buildings and the general inconsistencies within road networks. Simultaneously, the Internet of Vehicles (IoV) seems not to be plagued by the constraints mentioned above [2]. The IoV provides connectivity with multiple services, functionality, and application; however, security and privacy are still issues, particularly regarding the vehicles used in public transports. We have seen that VANETs are an essential component for any Intelligent transportation system (ITS) as VANET's primary purpose is to provide safe and secure transportation for drivers and travellers.

VANETs have three primary purposes road safety, comfort, infotainment, and traffic management by using the transportation network [3]. The

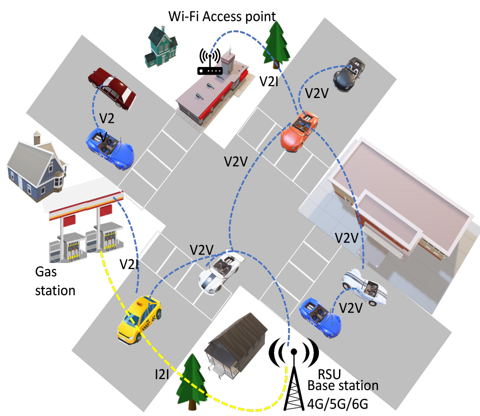


Fig. 1: The communication method and overview of the VANET and IoV.

main goal of the safety application is to decrease accidents and save lives. On-time warning messages can be achieved by using the vehicular nodes in the network. Some of the early warning messages include a collision warning, a recommendation about hazardous conditions, and lane change assistance. Other traffic management applications of VANETs include congestion avoidance or speed limitation notifications. We can see that infotainment applications can provide services that enhance any driver's experience. Any of these infotainment-based applications require Internet connections [3]. The primary goal of the VANETs is to make driving safe and secure. Therefore, secure network communication is vital. The critical nature of VANETs becomes more vulnerable in the context and reference to both law enforcement and first responders. Therefore, this research aims to address security and privacy concerns for vehicular networks in Intelligent Transport Systems (ITS).

The data traffic generated over the VANETs connected over 5G networks is extensive. These lead to the development of progressive technologies in data mining used for implicit information discovery. Managers or decision-makers then use the extracted and mined data to decide and update policy. However, excess data open was concerning in the privacy protection domain. Since data mining is designed to look for patterns and valuable information from data that may reveal sensitive personal information, in turn, this may cause high-risk security issues for trust in vehicular communication.

Mostly, researchers use heuristic and metaheuristic approaches to sanitize sensitive information. Here, we present the idea of using the PPDM issue with deep reinforcement learning (Q-learning model [4]). The proposed model takes the input states and predicts the actions. An advantage of this approach is adjusting to fewer parameters and hiding sensitive information by keeping the utility. The Q-learning model helps in the prediction process and can achieve good generalizations. Our model discovers instances dynamically and perturbs them to hide information successfully without predefined rules. Also, it dynamically maintained the utility of the data.

## II. Related work

Security and privacy issues have been considered a vital research area [5] with exponential data generation. The model-like $l$-diversity and $k$-anonymity in data streams are utilized to make the process anonymized [6]. The standard $K$-means algorithm is used in the data privacy and sanitization process [7]. The encryption and data utility is improved with the proposed model [7]. These are a standard method that is used in the fields of machine learning (ML) as well as data mining. In a wireless medium, network threats and attacks used radio communication broadcast technology in VANETs. This data over wireless communication mediums must be secure, or it can lead to unnecessary attention for adversaries.

Private information of the user's vehicle must be protected from the exchange of information in vehicular nodes. Moreover, the control authorities should preserve the driver's privacy while keeping private identity [3]. Privacy concerning vehicular networks should be a key component in VANETs. Both forged and adversarial information broadcasted in unknown vehicles may result in severe repercussions for drivers and pedestrian well-being. On the flip side, if a trustworthy safety message may also be sent using adversarial information using a component in a VANET, it causes delayed and modified information. As a result, human lives have server consequences. This means the security-related legitimate and accurate information also required the same security level over VANETs [3].

## III. VANETS AND DATA SANITIZATION

To enable the communication for service and application, VANETs include the application unit (A.U.), onboard unit (OBU), and the roadside unit (RSU). These RSU units are connected over the Internet for services providing tasks. The application units following, as shown in Fig. 1 are the fundamental components of VANETs with a brief description of each: The application units use an application and handle the networking issues. The A.U. coupled with OBU and communicate over the wireless medium. The application can control OBU [3]. The OBU helps connect the network components among OBUs and RSUs in VANET architecture using the IEEE 802.11p radio technology. Mainly OBU consists of different sensors (i.e., wireless communication element), a central control module (CCM), and an interface component. The CCM provides the user interface to do a resource command process (RCP) and contains the memory to read and write operations using the transceiver. Sensors data are usually processed using the OBU; the proposed model is also deployed here to hide the sensitive information. OBU also provides the vehicles' geographical location, Ad Hoc routing, data security, network congestion control mechanism, message dissemination, and I.P. mobility. The RSU is the fixed infrastructure located on the road and provide wireless access in vehicular environments (WAVE) or dedicated short-range communications (DSRC) device. It is based on the IEEE 802.11p wireless technology to enable communications with vehicles on the road [3]. The RSU also provides the access point (A.P.) in wireless Ad Hoc networks [3]. The RSU functionality includes infotainment, traffic status sharing, safety message from central authorities [8]. It also provides message sharing among OBUs to extend communication, function as the gateway for OBUs, and act as the data source to provide infrastructure-to-vehicle communications. All RSUs (within a specific geographical zone) can communicate and are interconnected. The trusted authority is responsible for controlling TSUs. It can process high computations and provide high storage capacity. T.A.s aims to authenticate all the vehicles and validated security relevant to vehicles transmitting false messages. It also verifies digital signatures and certificates.

Attackers used the false traffic emergency to forge the signals [1]. This miscommunication way has successfully become more effective when hacker identification has become untraceable [1]. Therefore, there is a need to improve the security of the communication. Data sanitization method was introduced [7], where evolutionary-based algorithm is utilized by optimization model. The method first selects the key utility transaction and then clusters them for hiding the sensitive information. The rules-based approach is also used for data privacy preservation [9]. The model used the $k$-anonymous imprecise rules to compose the data tables. The composed data is then used to protect privacy ability. Vehicular sensors data are also used for the motor torque based on the model prediction [10]. The model is used to close the loop between system engineering. The model output is used in E-powertrain mounted vehicles. The privacy preserved call data record analysis (CDRA) is also performed for the COVID-19 patients to control the pandemic [11].

### A. Problem statement

PPDM for VANETs can be seen in Figs. 2 and 3 that represent the Road Side Units (RSU) vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-infrastructure (I2I), and trusted authority (T.A.), respectively. The Intelligent Internet of Vehicular Things (IIOVT) network RSU and T.A. mentioned in Fig. 2. Both used different OBU sensors to create data sent to the PPDM algorithm shared via RSU and T.A. mentioned in Fig. 2. Once the sanitization process is complete and the data is stored, group anonymization is done to hide any group information. This article uses a Markov Decision Process for the sanitation process as given in Fig. 3.

We can see the method as proposed in Fig. 3 and described in Algorithm 1. In step 1, the model takes all its arguments as input. Next, the algorithm extracts all of the F.I.s, or frequent itemsets $F_{itemsets} = \{f_1, f_2, \ldots, f_k\}$. The F.I.s need to have a support count value that can not be less than the min support count value as given in (Algorithm 1, Line 1). Based on F.I.s, we select 20% of the F.I.s for utility and data sanitization. We project each item set to get instances $Ins_{I.D.}$ from the raw original dataset, as shown in (Algorithm 1, Line 1). Next, we can represent the states as a set of instances $Ins_{I.D.}$ as shown in (Algorithm 1, line 3). We initialize the $Q$ table and simultaneously set the exploration rate. Randomness is used in the model based on the epsilon greedy policy given in [12], from this each episode is updated as given in (Algorithm 1, Lines 4-6). Action reward *R* represents change based on the action, State and next State (Algorithm 1, Lines 10) and is then calculated using a fitness function (Algorithm 1, Lines 7 to 13).

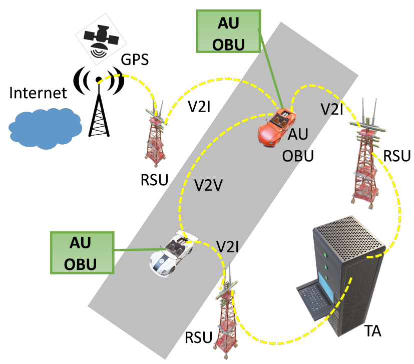


Fig. 2: VANETs communication with trusted units and others components.

$$\text{fitness}\ (s) = w_1 \times a + w_2 \times \beta + w_3 \times \delta \quad (1)$$

Using Equation (1), state fitness values can be found. We only calculate fitness values for deletion operations. To update the $Q$ table, the Bellman equation is implemented as shown in (Algorithm 1, Lines 12 to 13). Every cycle sees the instance set selected using random deletion points. Our model gets trained using it and the length of the input feature of $Ins_I D$, as well as the action (Delete/Not-Delete), next State (if action = Delete), is only used for Reinforcement Learning $(R.L.)$ as shown in (Algorithm 1, Line 13). At episode end, our model minimizes fitness value which in turn indicates that the instance set (sensor data) needs deletion for hiding sensitive itemsets as shown in (Algorithm 1, Line 16). As mentioned in Fig. 3, the training phase is done based on Algorithm 1. In a recurrent neural network-based LSTM network - one State represents the instances (vehicular sensors data) with two actions (delete or not delete) that results in another state is the union of the previous and current State. It is noted that both decisions lead to different fitness values depending upon the set instances when deleted. Then, during privacy preservation, Algorithm 1 trained network is used for decision-making, leading to the fitness value. The fitness value is used to calculate the side effects of privacy preservation as mentioned in Fig. 3 privacy preservation phase. Upon deletion of certain item sets, the data has a specific impact for each instance. The impact on each sample can be calculated using the fitness function and represents the quality of privacy preservation mentioned in Equation 1 and Fig. 3 privacy preservation phase.

**State:** Let $s = [p, h, b]$ : be defined as the set of instances $p \in \mathbb{R}_+^D$, where we see that cost to delete instances $h \in \mathbb{Z}_+^D$, as well as the remaining instance after the sanitization process, is given as $b \in \mathbb{R}_+$, where $D$ is the number of instances in the projected datasets and $\mathbb{Z}_+$ denotes non-negative integer numbers.

**Action:** Let there be a set of actions on $s$ i.e. delete/not-delete. If the action is a deletion, then and only then can it lead to the union of instance in $s_{t+1}$ and $s_t$. If action is not deleted, then the union operation is not made. The action will result in increasing/decreasing the fitness values as given in Equation 1, where $\alpha$ can be seen as hiding of sensitive itemset ratio before/after sanitization, and $\beta$ can be defined as the # of F.I.s before/after sanitization. Furthermore, we can say that $\delta$ is defined as the # of F.I.s that are present in sanitized database $D'$ and were also previously infrequent in original database $D$, where we see that $w_1, w_2, \ldots, w_3$, are known to be the relative importance of each side effect, which is set at runtime by a user in the range of $[0, 1]$.

**Policy:** We define that $\pi(s)$ : is the method to delete/not delete state $s$. We give the probability distribution of $a$ at state $s$ as a policy.

**Reward:** Let us define $r(s, a, s')$ as the the change in fitness value that can occur only when action $a$ occurs at state $s$ while arriving at new state $s'$. In policy, if action is deleted, then and only then is the fitness value calculated. If the fitness value decreases, then the reward will be 10. Otherwise, we set the reward to $-10$. The Bellman

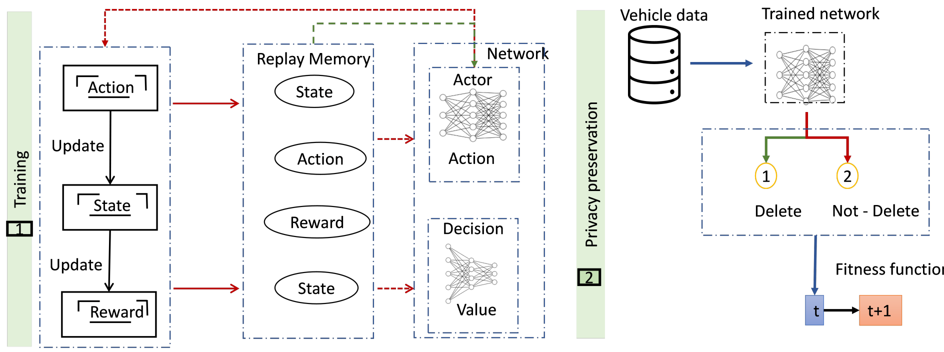


Fig. 3: DSRL framework.

Equation is followed originally given in [12], where action reward $a_t$ is in expectation $r\left(s_t, a_t, s_{t+1}\right)$. We see that the discounted factor $\gamma$ is returned only based on assumption. Our method's goal is to minimize fitness value at a given target time $t_f$. Our model's Markov property, which optimizes policy minimizing the function $Q_\pi\left(s_t, a_t\right)$. Using the optimization of fitness value while also considering the interaction with the environment, our policy is learned. A sample table for the State, action, and reward is mentioned in Table I.

TABLE I: A sample table for state, action, reward and fitness value. *a, b, c, d, e* represent vehicle sensors data.

| States | T_ID | a | b | c | d | e | Action / Policy | Reward | Fitness Value |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | Delete | 10 | 1 |
| 2 | 34 | 0 | 1 | 1 | 0 | 1 | Delete | 10 | 0.5 |
| 3 | 9 | 1 | 1 | 1 | 0 | 1 | Delete | 10 | 0.3 |
| 4 | 14 | 1 | 0 | 1 | 1 | 0 | no Delete | -10 | 0.3 |
| 5 | 16 | 0 | 1 | 1 | 0 | 1 | no Delete | -10 | 0.3 |

### B. Deep reinforcement learning (DRL)

We proposed the LSTM based network, as mentioned in Fig. 3. The architecture input is sensors input values, whereas the output is $delete$ or $not-delete$, making a binary classification problem. We also proposed a windows-based time stepping. The fitness value of the previous State and its prediction is added as input features. As the vehicular communication frequency is very high, we set the windows time step to two. Therefore, $(t+1)$ is used with two previous ($t-1$ and $t-2$) decision and fitness values. In this way, a model can relearn the complex patterns and try to achieve generalization [13]. Model input is encoded item value, a previous decision, and fitness value as the input vector. In the decoder network, the $Dense$ layer is added to produce the output. The rectified linear unit $ReLU$ is used as the activation function in encoder and decoder network as defined as $f(x) = \max(0, x)$. To avoid overfitting, the $Dropout$ mechanism should be adopted. The $Adam$ optimization algorithm is used as an optimizer, which very effective in the training of LSTM.

**Algorithm 1** Deep Sanitization Reinforcement Learning (DSRL)

**INPUT:** $D$, OBU dataset, support threshold $\varepsilon$, percentage of sensitive itemsets $P$, state size $S$, episode size $M$
**OUTPUT:** Minimize fitness value actions.

```
1:  Select sensitive itemsets using P from calculated frequent itemsets
    based on ε
2:  Get the T_ID of the Select sensitive itemsets from D
3:  Select set S combination based on randomized set of T_ID
4:  for episode = 1, M do
5:      Take random decision 𝒩 for action exploration
6:      Receive output based 𝒩 on state s_1
7:      for t = 1, S do
8:          Take action based on the 𝒩
9:          Execute (action a_t, observe reward r_t, state s_{t+1})
10:         R ← transition (s_t, a_t, r_t, s_{t+1})
11:         Train_DRL ← Input (action a_t, rewards r_t )
12:         Update Bellman Equation using 𝒩
13:         Update Train_DRL (action a_t)
14:     end for
15: end for
16: Return States, action and fitness_value
```

## IV. Security and Privacy required of VANETs

The vehicular network collects different data that includes sensors equipped with healthcare, smart city, and surveillance. Data fragmentation in dynamic VANETs is a challenge for practitioners. In the case studies [14], [15], the number of autonomous vehicles indicates the network breaches through the communication system. Hackers target the ECU program and try to compromise the vehicle networks. As a result, the vehicle behaves abnormally. This leads to solid communication network security measures including intrusion detection systems at the vehicle. Privacy preserved method is considered for sensors communication, frequent log reviews of mobile application and servers [14]. If any vulnerability is detected, then the vehicle owner and manufacture should be informed before the attack. We proposed a data sanitization process for VANETS component OBUs. The function only shares limited data with other components attached wirelessly. The deep learning method is adopted to improve and learn patterns of the sensors. We attempt to demonstrate that the DQRL model can be sufficient to hide private information while communicating. Sensitive information can be removed on certain public data points by using the sanitization process. The framework can help users who want to hide information especially for private events. The VANETs are equipped with multiple sensors to read the data from the temperature, humidity, camera, accelerometer sensors, ultrasonic, proximity, and gas. These sensor values are instrumental for a smart city to evaluate and improve the transportation system. However, while collecting the sensors points, private information is also being processed to be vulnerable to the users.

**Data Safety:** Safety of the data among communication in public wireless connection is essentials. Correct and on-time message delivery can be safe and causes fatalities if the malicious nodes injecting adversarial models result in misinformation. The data security and privacy requirements highlight this research that can be reduced using the proposed model. Failure of the requirement can cause vulnerabilities in VANETs. A proposed model can satisfy security and privacy issues in VANET. **Integrity and Data Trust:** The data communicated between two parties should not be altered [3]. The content should be non-modified and dropped [3]. Integrity is violated when data is modified [3]. Detection of such a mechanism should be adopted. **Authentication and Identification:** All connected nodes must be authenticated to ensure protected data transfer. The unauthorized access must be blocked to secure node communication and messages. Also, the identity of the user should be preserved using the proposed model. Therefore, a malicious node prevented to be duplicating the identity of a genuine node. Upon compromise, the malicious node might delete the warning message; thus, the driver might not respond according to instructions. Like Sybil attack, the attack can be prevented by using the unique I.D. mechanism [8]. Legal forensic evidence to law enforcement agencies requires a strong authentication process to avoid any adversarial attacks [8]. The only vehicular node that authenticated and authorized vehicles should access RSUs and benefit from services the VANET [8]. **Availability:** The vehicular nodes should send and receive messages even in an attack such as a D/DoS or jamming attack [3] or under any malicious activity [8]. For example, in a specific area, the server cannot communicate in a very congested area due to attacks. Availability required high bandwidth and connectivity. The importance of availability arises when some messages are delayed and not transmitted in real-time. As a result, messages lose their values (e.g., message about road conditions) and might even be harmful (e.g., hazardous reporting message) to the users in the network [8]. **Privacy and Confidentiality:** Vehicular and driver privacy must be preserved even when the liable connection is available. The proposed helpful model removed the identity of the person to avoid identity theft issues. The actual identity of the driver, vehicle, and location should always be preserved. Only official authorities can see the drivers and vehicle identity.

**Suggestions for Sanitization method:** During sanitization progress, vehicular node data scalability analysis should be done and information required to be shared. Vehicle sensors data relationships within the vehicle. The dimension size analysis (Number of sensors) should be performed concerning the number of instances (sensors rate of data). The modality analysis should also be performed to analyze the model distribution. Outliers often decrease model performance [16]. The noise and contamination (anomalies) analysis is required to be considered [16]. The unbalanced data distribution for DSRL results in underperformance. In particular, the following suggestions should be considered. **Problem identification:** For the VANETs application, the machine learning engineer should identify the problem to be solved with the sanitization process. **Client instrumentation:** Some applications cache the vehicular sensors data for the model's prediction. Data instrumentation should be done for the interaction of the network. **Simulation prototyping:** The model architecture and hyper tunning should be tested using the valid tested data [16]. The purpose is to carefully monitor data distribution drift and its performance in the simulated online production system. **Deep learning model training:** Different architectures should be trained and tested to check adversarial attack compatibility. The model should be optimized, and hyper-tuned [16]. **Model evaluation:** The model should be trained and tested under different tests case. **Deployment:** For the deployment, the best model configuration should be selected.

## V. Conclusion

We proposed a data sanitization model to hide sensitive information. Our model can analyze the OBU sensors and hide them using the RL method. The method can adopt concerning the fitness function and gets the feedback reply integration method to correct the wrong decision making. The time series's additional features can also be employed, including uncertainty, utility, frequency, and co-occurrence.

## References


[1] J. Zhang and Q. Zhang, "On the security of a lightweight conditional privacy-preserving authentication in vanets," *IEEE Transactions on Information Forensics and Security*, 2021 (early access).

[2] M. Abu Talib, S. Abbas, Q. Nasir, and M. F. Mowakeh, "Systematic literature review on internet-of-vehicles communication security," *International Journal of Distributed Sensor Networks*, vol. 14, no. 12, 2018.

[3] M. Obaidat, M. Khodjaeva, J. Holst, and M. B. Zid, "Security and privacy challenges in vehicular ad hoc networks," in *Connected Vehicles in the Internet of Things*, 2020, pp. 223–251.

[4] C. J. C. H. Watkins and P. Dayan, "Q-learning," in *Machine learning*, vol. 8, 1992, pp. 279–292.

[5] D. Das, W. Banerjee, Souravand Mansoor, U. Biswas, P. Chatterjee, and U. Ghosh, "Design of a secure blockchain-based smart iov architecture," in *International Conference on Signal Processing and Information Security*, 2020, pp. 1–4.

[6] M. A. Mohamed, S. M. Ghanem, and M. H. Nagi, "Privacy-preserving for distributed data streams: towards l-diversity," *The International Arab Journal of Information Technology*, vol. 17, no. 1, pp. 52–64, 2020.

[7] P. Lekshmy and M. A. Rahiman, "A sanitization approach for privacy preserving data mining on social distributed environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 7, pp. 2761–2777, 2020.

[8] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Intelligent transportation system security: impact-oriented risk assessment of in-vehicle networks," *IEEE Intelligent Transportation Systems Magazine*, 2019 (early access).

[9] M. Inuiguchi and K. Washimi, "Utilization of imprecise rules for privacy protection," in *International Symposium on Integrated Uncertainty in Knowledge Modelling and Decision Making*, 2019, pp. 260–270.

[10] B. Forrier, A. Loth, and Y. Mollet, "In-vehicle identification of an induction machine model for operational torque prediction," in *International Conference on Electrical Machines*, vol. 1, 2020, pp. 1157–1163.

[11] S. Nisar, M. A. Zuhaib, A. Ulasyar, and M. Tariq, "A privacy preserved and cost efficient control scheme for coronavirus outbreak using call data record and contact tracing," *IEEE Consumer Electronics Magazine*, vol. 10, no. 2, pp. 104–110, 2021.

[12] X. Y. Liu, Z. Ding, S. Borst, and A. Walid, "Deep reinforcement learning for intelligent transportation systems," *arXiv preprint arXiv:1812.00979*, 2018.

[13] Q. Wang, C. Feng, Y. Xu, H. Zhong, and V. S. Sheng, "A novel privacy-preserving speech recognition framework using bidirectional LSTM," *Journal of Cloud Computing*, vol. 9, no. 36, pp. 1–23, 2020.

[14] M. K. Khan and A. Quadri, "Augmenting cybersecurity in autonomous vehicles: Innovative recommendations for aspiring entrepreneurs," *IEEE Consumer Electronics Magazine*, vol. 10, no. 3, pp. 111–116, 2021.

[15] K. Greene, D. Rodgers, H. Dykhuizen, Q. Niyaz, K. Al Shamaileh, and V. Devabhaktuni, "A defense mechanism against replay attack in remote keyless entry systems using timestamping and xor logic," *IEEE Consumer Electronics Magazine*, vol. 10, no. 1, pp. 101–108, 2020.

[16] K. Stapor, P. Ksieniewicz, S. García, and M. Woźniak, "How to design the fair experimental classifier evaluation," *Applied Soft Computing*, vol. 104, pp. 107–219, 2021.



**Usman Ahmed** is a PhD candidate at the Western Norway University of Applied Sciences. Contact him at usman.ahmed@hvl.no.

**Jerry Chun-Wei Lin** is a full professor at the Western Norway University of Applied Sciences, Bergen, Norway. Contact him at jerrylin@ieee.org (*Corresponding author).

**Gautam Srivastava** is an associate professor at the Department of Computer Science, Brandon University as well as China Medical University, Taiwan. Contact him at srivastavag@brandonu.ca.