AI-enhanced Digital Twin Framework for Cyber-Resilient 6G Internet-of-Vehicles Networks

Yagmur Yigit, *Student Member, IEEE*, Leandros Maglaras, *Senior Member, IEEE*, William J. Buchanan, *Senior Member, IEEE*, Berk Canberk, *Senior Member, IEEE*, Hyundong Shin, *Fellow, IEEE*, and Trung Q. Duong, *Fellow, IEEE*

***Abstract*—Digital twin technology is crucial to the development of the sixth-generation (6G) Internet of Vehicles (IoV) as it allows the monitoring and assessment of the dynamic and complicated vehicular environment. However, 6G IoV networks have critical challenges in network security and computational efficiency, which need to be addressed. Existing digital twin technologies in 6G IoV networks often suffer from limitations such as reliance on static models and high computational demands, leading to unstable attack detection and inefficiencies. Their results for attack detection performance metrics, precision, detection rate, and F1-Score are insufficient for 6G IoV. Moreover, these systems concentrate all computational processes within the digital twin's service layer, leading to inefficiencies. To address these challenges, we introduce a novel artificial intelligence (AI) enhanced digital twin framework designed to significantly improve 6G IoV network security and computational efficiency under dynamic conditions. Our framework employs an advanced feature engineering module that uses feature selection methods and stacked sparse autoencoders (ssAE) to reduce feature dimensions within the cyber twin layer, effectively distributing the overall computational load. It also utilises an online learning module which enables a network-aware attack detection mechanism for precise attack detection. The proposed solution exhibits a stable performance of around 98% success rate regarding attack detection metrics against two datasets. Specifically, our solution reduces system latency by 12%, energy consumption by 15%, RAM usage by 20%, and improves packet delivery rates by 6.1%. These findings underscore the potential of our framework to enhance the robustness and responsiveness of 6G IoV systems, offering a significant contribution to vehicular network security and management.**

***Index Terms*—AI, Security, Digital Twin, IoV, ITS, VANET.**

Yagmur Yigit, Leandros Maglaras, and Berk Canberk are with the School of Computing, Engineering and The Build Environment, Edinburgh Napier University, United Kingdom. Berk Canberk is also an affiliated professor at the Department of Artificial Intelligence and Data Engineering, Istanbul Technical University, Turkey (e-mail: (yagmur.yigit, l.maglaras, b.canberk)@napier.ac.uk, canberk@itu.edu.tr).

William J. Buchanan is with the Blockpass ID Lab, Edinburgh Napier University, United Kingdom (e-mail: b.buchanan@napier.ac.uk).

Hyundong Shin is with the Department of Electronics and Information Convergence Engineering, Kyung Hee University, South Korea (e-mail: hshin@khu.ac.kr).

T. Q. Duong is with the Faculty of Engineering and Applied Science, Memorial University, St. John's, NL A1C 5S7, Canada, and with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, BT7 1NN Belfast, U.K., and also with the Department of Electronic Engineering, Kyung Hee University, Yongin-si, Gyeonggi-do 17104, South Korea (e-mail: tduong@mun.ca).

This work was supported in part by the Scientific and Technological Research Council of Turkey (TUBITAK) 1515 Frontier R&D Laboratories Support Program for BTS Advanced AI Hub: BTS Autonomous Networks and Data Innovation Lab Project 5239903. The work of H. Shin was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (NRF-2022R1A4A3033401). The work of T. Q. Duong was supported in part by the Canada Excellence Research Chair (CERC) Program CERC-2022-00109.

This paper has been accepted in part for presentation at the IEEE International Conference on Communication (ICC), Denver, CO, USA, June 2024.

Corresponding authors are Trung Q. Duong and Hyundong Shin.

I. Introduction

THE evolution of vehicular ad-hoc networks (VANETs) marks an important advancement in road safety and transportation efficiency, as the World Health Organization underscored in its Global Status Report on Road Safety in 2023 [1]. VANETs are becoming increasingly important in the sixth-generation (6G) Internet of Vehicles (IoV) era, since Internet-connected systems in vehicles, which consist of sensors, actuators, and smart devices, allow different objects to collect, transfer, and process data. 6G networks are expected to transform VANETs further, improving on the developments of fifth-generation (5G) networks by delivering higher data rates, lowering latency to almost real-time, and expanding coverage. To enable 6G IoV networks, digital twin technology is essential for monitoring and analysing the dynamic and complex nature of the vehicular environment [2], [3].

In the 6G IoV, vehicular networks are essential as they allow vehicles to communicate with each other (vehicle-to-vehicle (V2V) communication), and with the infrastructure (vehicle-to-infrastructure (V2I) communication). By giving drivers precise and timely traffic information, vehicular communication improves comfort, safety on the road, and the feasibility of implementing autonomous vehicles [4]. However, these advancements also introduce new challenges in managing the complexity and security of vehicular networks, underscoring the necessity for innovative solutions.

A. Motivation

There is currently an increase in adverse attacks, especially in V2I communications, due to the heterogeneity and dynamic topology of vehicular networks [5]–[7]. The attackers cause significant harm by employing sophisticated attacks and interfering with vehicle services. By making the 6G IoV network unavailable or unresponsive to intended customers, a cyber attack, such as distributed denial of service (DDoS), attempts to interfere with vehicular services and systems. This kind of attack leaves these vehicles inoperable, causing a negative impact on service providers and customers. Moreover, the attack could result in vehicle problems, traffic congestion, interference with vehicular communication, and even accidents

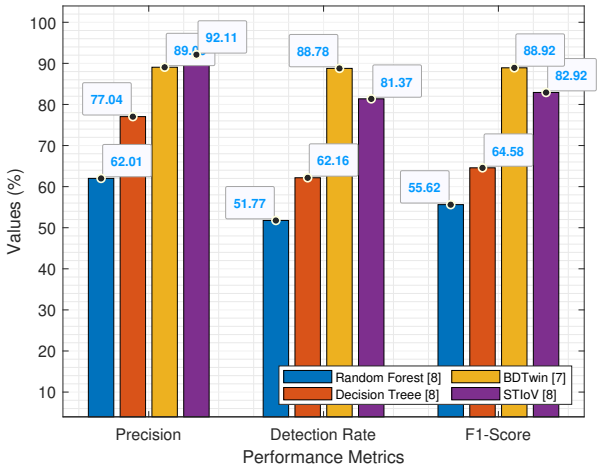

Fig. 1. The performance analysis of current solutions.

[8], [9]. Consequently, it is crucial to create advanced defensive systems to protect VANETs from attacks and maintain their dependability in this 6G IoV age.

The recent works on vehicular network attack identification using digital twin technology [10], [11] are not sufficient to meet the 6G IoV network performance metrics such as detection rate, precision, and F1-score as can be seen in Fig. 1. These solutions use the static model, which is unsuitable for the 6G IoV networks since they require dynamic solutions to handle different attacks and heterogeneity in their network. Moreover, they are unstable between various data. For example, when we compare the performance results of the solutions in [10], [11] on two datasets, there is a difference of around 15% between performance results. Similarly, the performance result of the random forest and decision tree algorithms in [11] showed approximately 25% differences between the two datasets. Therefore, the current solutions are not stable and capable of handling diverse attacks in dynamic 6G IoV environments. There is a need for an advanced solution that can dynamically identify attacks and has stable performance in the 6G IoV environments.

The other problem is the computational load in the current vehicular network identification solutions, which directly affects the system's end-to-end latency, an important factor for attack detection time. The growth of vehicular communication systems highlights the increased computational load in 6G IoV environments. The current research on vehicular networks using digital twin technology has a significant overall computational system burden since all computational operations are performed at the digital twin's service layer [12], [13]. Therefore, their total end-to-end latency, energy consumption, RAM usage, and packet delivery rate results are not adequate to handle the 6G IoV environments. This computational load must be distributed for the system to function more effectively and quickly identify attacks.

To address these two main challenges, an online learning approach can be utilised for dynamic attack identification, while the digital twin layer, not its service layer, can be used for feature engineering and feature dimension reduction to split the system computational load. Moreover, network data can be effectively processed and analysed by utilising the capabilities of a stacked sparse autoencoder (ssAE) [14], [15]. The ssAE extracts relevant characteristics for cyber security applications such as anomaly detection, pattern identification, and attack detection [16]. It reduces the dimensionality of the data while maintaining its key features and minimising the difference between the original and recreated data.

B. Coverage of Paper and Contributions

In this paper, the ssAE is utilised thanks to its enhanced feature extraction and efficient dimensionality reduction capabilities. To mitigate the challenges mentioned above, this work primarily focuses on V2I communication, specifically on fortifying roadside unit (RSU) security. Furthermore, we introduce an innovative approach based on artificial intelligence (AI) to enhance the security aspects of 6G IoV networks by applying digital twin technology and AI algorithms, focusing on cyber security and computational efficiency. Our work stands out by proposing a comprehensive layered system architecture that integrates data, cyber twin, and security layers, uniquely addressing the challenges of high mobility and heterogeneity in 6G IoV environments, as can be seen in Fig. 2. We employ a feature engineering module, which includes a ssAE algorithm for efficient feature dimension reduction, and an online learning module that provides stable attack identification performance in the cyber twin layer. Our novel approach addresses the inherent challenges of 6G IoV networks, such as high mobility and heterogeneity. It pioneers the use of digital twin technology for real-time monitoring and management of vehicular networks, offering significant advancements over existing methodologies regarding computational system load and stable system performance.

Our main contributions to this paper are outlined below:

- We propose a digital twin-assisted smart attack detection framework to handle different attacks in the 6G IoV environments, especially those targeting RSUs.
- We provide an online learning module to ensure the stable performance of our detection mechanism in a network-aware manner. This module mainly consists of AutoFS and AutoCM components to find the best feature selection and classification techniques for the network.
- We introduce a feature engineering module which utilises a ssAE algorithm to decrease data dimension. We employ the feature engineering and online learning modules in the cyber twin layer of the proposed framework to divide the overall computational load of the system.
- We present an automated neighbour RSU relation to share the malicious IP address of the vehicle between neighbour RSUs.

This paper extends the framework presented in our conference paper [2] by incorporating several significant advancements tailored for 6G networks. In this paper, we employed a feature engineering module, AutoCM element ([2] includes only multi-layer perceptron (MLP) for classification), division of the system's overall computational load between cyber

twin and security layers, and an automated neighbour RSU relation unlike [2]. The conference paper's AutoFS module includes recursive feature elimination (RFE), backward feature elimination, chi-square, fisher score, and analysis of variance (ANOVA) F-value selection algorithm. After conducting the comprehensive experiment, we replaced the backward feature elimination and fisher score with the principal component analysis (PCA) and random forests for feature importance algorithms in this paper since their results were better.

The remainder of the document is structured as follows: Section II gives an overview of the related work. In Section III, we first propose and provide a detailed explanation of our system model. Then, we analyse how our solution performs in Section IV, and provide a discussion in Section V. The paper is then concluded in Section VI.

II. Related Work

In recent years, digital twin technology has gained significant attention in the development of intelligent transportation systems. For example, [17] explore the role of digital twins in connected and automated vehicles, emphasizing their potential to revolutionize the transportation domain by enabling real-time communication and predictive analytics. A digital twin framework was proposed for smart city traffic management, utilizing real-time data to optimize traffic flow and enhance safety. However, this approach focuses primarily on traffic efficiency and lacks specific mechanisms for attack detection within vehicular networks. Similarly, the convergence of the Internet of Things (IoT) and AI technologies has paved the way for innovative digital twin architectures. [18] explores task offloading and task caching strategies in nearby edge servers to lower the latency and so provides a powerful computing infrastructure through mobile edge computing-based ultra-reliable and low-latency communications digital twin architecture. Nevertheless, there are also no specific procedures for attack detection in this work.

There are only a few studies in the literature focusing on attack identification using digital twin technology for vehicular networks. In [19], a support vector machine algorithm using digital twins was used for malicious node identification. Digital twins were employed to find and eliminate malicious nodes on a VANET architecture in this work. However, the solution used the static model and could not adapt to the dynamic nature of the vehicular network. Moreover, this work does not provide any metric related to computational load, which is important for efficient attack detection. The work in [13] proposed a blockchain-enabled decentralised trust management system to identify malicious vehicles using digital twins technology. The proposed method is not aware of the network and does not update itself according to the network condition to provide stable performance for attack detection. It is, therefore, not suitable for use in a vehicular network. The performance was only evaluated in terms of transmission overhead, which is insufficient to determine the system computational load. The work [10] provided a blockchain and attention-based bidirectional long short-term memory (LSTM) framework, which uses a digital twin for attack detection in the vehicle-to-everything environment. The authors tested the effectiveness of this framework using two well-known Internet-of-Things datasets. However, the results indicated approximately a 14% difference between datasets, which is a huge difference and does not provide stable performance in the dynamic nature of IoV networks. Furthermore, no computational load metric is provided by this work, which is essential for effective attack detection in the vehicle-to-everything environment.

In another study [11], the authors proposed a deep learning-based framework to catch intrusions in an IoV network. It utilised a stacked variational autoencoder and attention-based bidirectional LSTM. In this work, digital twin technology was employed to map RSU servers to enable the building of the vehicular association model. The proposed solution was evaluated using two widely recognised datasets. Nonetheless, the findings reveal a significant distinction of about 15% between the datasets, highlighting unstable performance within the ever-changing IoV networks. This study overlooks the system computational burden metrics, a critical element for successful attack detection within the IoV ecosystem. The authors in [20] presented an LSTM-based actor-critic deep reinforcement learning system for attack detection in vehicle-to-grid-enabled cyber-physical systems by utilising a digital twin approach. The performance results of this work are insufficient to evaluate the attack detection performance of the proposed system. The presented system used a static model, which does not have any updating method. Therefore, it is not appropriate to provide a stable performance in the dynamic vehicular network environment. Moreover, the work in [21] presented a digital twin-assisted honeypot system to enhance security by providing insights into attacks, demonstrating its effectiveness in detecting and mitigating simultaneous. The proposed system utilises a dynamic model updating approach to handle different types of attacks. However, this work also has drawbacks since all computational systems and algorithms work on the digital twin's service layer. Therefore, it is not proper for the 6G IoV network. The authors in [22] offered a deep learning and identity-based encryption approach to scrutinise the anomalies in 6G IoV communication systems. Even though the attack detection performance result of the proposed solution exhibited around 97%, the evaluation is made by only one dataset. Therefore, the performance results against different datasets are unknown. Similarly, the system's computational load metrics results are also unknown. [23] introduces a novel approach to improve the energy efficiency and operational effectiveness of UAVs in serving terrestrial intelligent IoT by leveraging digital twin technology. To provide a clearer explanation of the implementation steps of digital twins in the dynamic characteristics of IoV environments, we drew upon the insights from this study.

The above-mentioned investigations highlight the significant yet under-exploited capabilities of securing IoV networks. Nonetheless, there is a noticeable shortfall in efficiently integrating digital twins and AI models to boost security, providing stable performance in 6G IoV networks. A dynamic attack detection system in IoV environments is needed to handle variations in network data while providing stable attack detection performance. Moreover, the current digital twin-enabled studies in vehicular networks indicate that the system load is

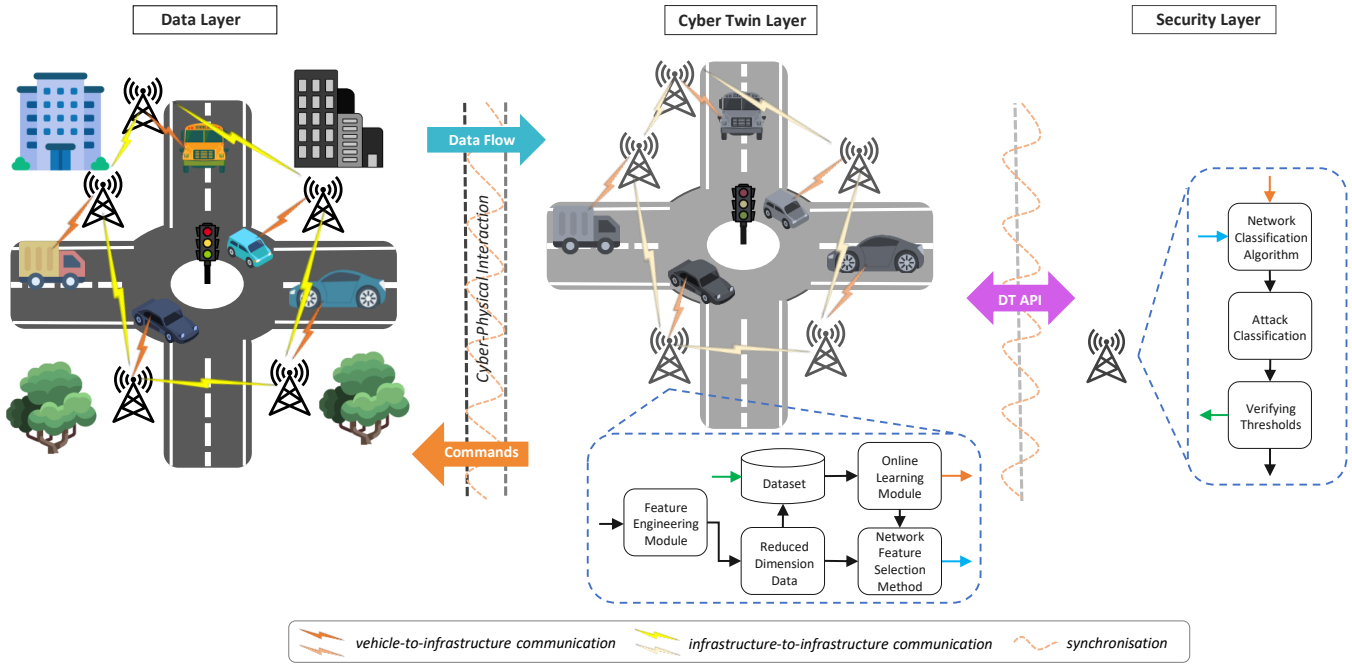

Fig. 2. The proposed system architecture for cyber-resilient 6G IoV networks.

significantly high, necessitating load distribution to enhance system performance and enable faster detection of attacks. At this point, digital twin technology can be effectively utilised to divide computational load throughout the vehicular system. In this paper, we aim to address these two shortfalls, offering an innovative strategy for securing V2I communication and diminishing the workload of the 6G IoV environments.

III. PROPOSED FRAMEWORK

In this framework, the RSUs collect all communication requests from the vehicles within their transmission range.

A. Mathematical Model of the RSU Traffic

We assume that vehicles share the appropriate channels of an RSU within its transmission area and that every vehicle has an equal priority, which means there is no priority between them. To model vehicle communication requests, we use the M/M/m queuing model, a fundamental concept in queuing theory. Queuing theory is a mathematical study of waiting lines or queues that helps predict queue lengths and waiting times. The M/M/m model specifically represents a system with multiple servers (m), where arrivals follow a Poisson process and service times are exponentially distributed. In our case, the model treats vehicle communication requests on a first-in-first-out (FIFO) basis, ensuring that requests are processed in the order they are received.

The nomenclature table can be seen in Table I, which provides definitions for the symbols used throughout the paper to enhance clarity and understanding of the mathematical formulations.

The number of communication requests in each time slot is used to characterise the system's condition. The servers are modelled as channels. Every time slot's total number of communication requests is compared with the number of channels that are accessible during that same time slot. The requests are held until the following time slot to check the availability of channels if none are available to serve. Fig. 3 illustrates the state diagram representing the communication demands from vehicles within the transmission range of a RSU using an M/M/m queuing model. This model helps in understanding the flow and processing of communication requests, where each vehicle request is treated based on the availability of channels. c_{num} represents the channel numbers

TABLE I
NOMENCLATURE TABLE

Symbol	Description
v_{num}	Number of vehicles demanding communication
c_{num}	Number of channels available at the RSU
λ	Arrival rate of communication demands
μ	Service rate of each channel per request
ρ	Traffic intensity
P_0	Probability of zero communication requests
P_{vnum}	Probability of having v_{num} vehicles
$\wp$	Probability that all requests are accepted
ξ	Probability that requests are queued
P_{Queue}	Probability of a communication request waiting
T_{AVGQ}	Average waiting time in the queue
Θ	Sparsity constraint weighting factor
σ	Nonlinear activation function used in neural networks
W_{ij}	ssAE weight matrix between input and hidden layers
W_{jk}	ssAE weight matrix between hidden and output layers
φ_1, φ_2	Bias vectors for hidden and output layers in ssAE
ρ	Predefined sparsity parameter in the ssAE algorithm
$J(W, b)$	Loss function for reconstruction error in ssAE
$J_{\text{sparse}}(W, b)$	Total loss function with sparsity penalty in ssAE
λ	Weight attenuation coefficient in ssAE loss function
γ_i	Threshold factor for the i-th classification algorithm
$\mathcal{V}(\mathcal{I})$	Verifying threshold function for system reliability
$\mathcal{R}$	System reliability metric

of the RSU, and v_{num} means the number of vehicles which demand the communication. λ indicates the arrival rate of the communication demands, and μ represents the channel's service rate for each request, which is dependent on time.

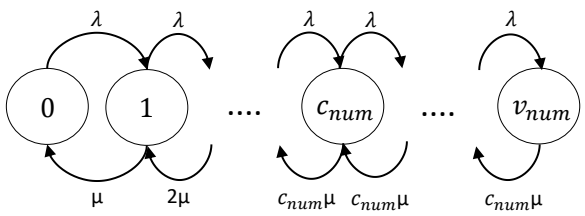

Fig. 3. The state diagram of the communication demands from vehicles within the transmission range of the RSU.

In this diagram, each state corresponds to a specific condition of the RSU as it processes communication requests. The transitions between states indicate changes based on the availability of communication channels and the arrival of new requests. For instance, when the number of vehicle requests is less than or equal to the number of available channels ($v_{num} \leq c_{num}$), the RSU can directly handle these requests, all requests are accepted. Conversely, if the requests exceed available channels ($v_{num} > c_{num}$), the remaining requests have waited in the queue, following a first-in-first-out order. This ensures that all requests are eventually serviced as channels become available. The diagram helps visualize key metrics such as the probability of the system being idle (P_0) and the likelihood of having a specific number of requests being processed ($P_{v_{num}}$). By understanding these probabilities and the average waiting time in the queue (T_{AVG_Q}), the diagram demonstrates how the RSU efficiently handles varying levels of communication demand. The equation (1) describes the probability of having a specific number of vehicles (v_{num}) in the system, accounting for the availability of channels (c_{num}), the service rate (μ), and the arrival rate (λ) of the communication requests:

$$P_{v_{num}-1} = min(v_{num}, c_{num}) \frac{\mu P_{v_{num}}}{\lambda}, \ \forall\, v_{num} \in [1, .., v_{tot}] \tag{1}$$

in which v_{tot} is total number of vehicles. The probability of all channels' busy situation is calculated by (2).

$$P_{v_{num}} = P_0 \frac{(c_{num}\rho)^{v_{num}}}{v_{num}\ !}, \ \forall\, v_{num} \in [0, 1, .., c_{num}] \tag{2}$$

where P_0 shows the probability of zero communication requests of the vehicles in the system, which is given in (4) and ρ is the intensity of traffic, which is given in (3).

$$\rho = \frac{\lambda}{c_{num}\mu} \tag{3}$$

$$P_0 = \left[\sum_{v_{num}=0}^{c_{num}-1} \frac{(c_{num}\rho)^{v_{num}}}{v_{num}\ !} + \frac{(c_{num}\rho)^{c_{num}}}{c_{num}\ !(1-\rho)} \right]^{-1} \tag{4}$$

The probability of v_{num} vehicles in the system is calculated by using $P_{v_{num}}$. $\wp$ is the probability of all communication requests being accepted, given in (5), and ξ is the probability of the communication request being waited in the queue, given in (6).

$$P_{v_{num}} = \begin{cases} \wp, & v_{num} \leq c_{num} \\ \xi, & v_{num} > c_{num} \end{cases}$$

$$\wp = P_0 \frac{(c_{num}\rho)^{v_{num}}}{v_{num}\ !} \tag{5}$$

$$\xi = P_0 \frac{(c_{num})^{c_{num}}(\rho)^{v_{num}}}{c_{num}\ !} \tag{6}$$

The probability of waiting in the queue for a communication request is calculated using the Erlang C Formula as

$$P_{Queue} = \frac{P_0\ (c_{num}\rho)^{c_{num}}}{c_{num}\ !\,(1-\rho)} \tag{7}$$

The average waiting time in the queue for the communication request is calculated by

$$T_{AVG_Q} = \frac{\rho\, P_{Queue}}{\lambda\,(1-\rho)} \tag{8}$$

B. Automated Neighbour RSU Relations

After modelling the communication requests of vehicles for an RSU, we work on the neighbour relations of RSUs. In our system, each RSU has its own Internet Protocol (IP) blocklist, which includes previously defined malicious vehicles' IP addresses. We describe an automated neighbour RSU relation, which is similar to our previous work [24]. However, the main aim of this automated neighbour RSU relation is to share the malicious vehicles's IP addresses between neighbour RSUs. The sequence diagram of the proposed automated neighbour RSU relation can be seen in Fig. 4.

When a vehicle sends a connection request to the RSU, it first checks its IP blocklist and then checks the neighbour RSU IP blocklists. If the IP address is not in the blocklist, the proposed smart attack detection mechanism starts to work to identify whether there is any attack on the system or not. If there is no attack on the communication request, it is taken to the available channel in the RSU, which is situation $\wp$ in (5). The communication request is brought to the queue if there is no available channel in the RSU, which is situation ξ in (6).

C. Proposed Attack Detection

The proposed smart attack detection system architecture follows a layered design methodology, combining interactions between physical and digital layers to create a comprehensive framework within 6G IoV networks. It is organised into three distinct layers: data, cyber twin, and security. As shown in Fig. 2, each layer is essential to the 6G IoV's overall functionality and security. The proposed system re-trains its models using the latest traffic data thanks to the online learning module, ensuring that it remains current with evolving attack tactics. The proposed system architecture is in line with the Internet Engineering Task Force (IETF) digital twin network architecture. Moreover, the proposed system also aligns with

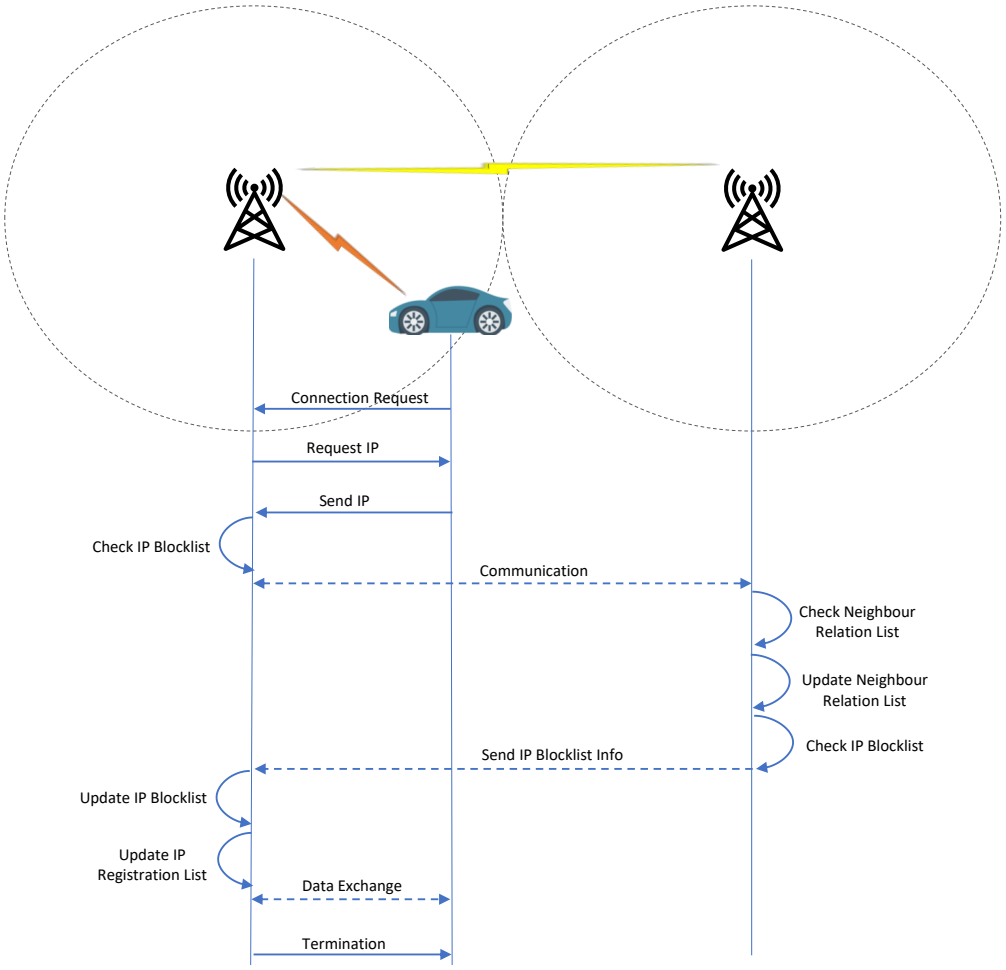

Fig. 4. The sequence diagram of automated neighbour RSU relation for malicious vehicles' IP list in 6G IoV networks.

the Gemini Principle by clearly defining its purpose, ensuring trust, and delivering critical functions for 6G IoV networks. The framework's purpose is to enhance vehicular network security and efficiency, addressing the pressing need for adaptable solutions in dynamic environments. Trust is established through the integration of AI-driven analytics and real-time data processing, ensuring accurate and reliable threat detection. Functionally, the framework operates across multiple layers, each contributing to its overall goal of providing robust, efficient, and scalable security for next-generation vehicular networks. By focusing on these core components, the framework represents a significant advancement in the application of digital twin technology to intelligent transportation systems, offering improved performance and resilience against cyber threats.

1) Data Layer: The foundational layer of our framework, the data layer, is essential for collecting and disseminating information in the 6G vehicular networks' layers. It effectively merges vehicles and RSUs to gather data that supports a high-fidelity representation of physical objects in the cyber twin layer and security evaluations of the proposed solution. The accuracy of the data layer in real-time data representation and communication is essential to preserving the digital twin-enabled vehicular network system's efficiency and integrity.

2) Cyber Twin Layer: The cyber twin layer plays a crucial role in generating dynamic digital models that mirror the physical elements of the 6G IoV networks, enhancing the system's adaptability and accuracy in reflecting real-world conditions. It processes feature engineering to reduce load in the security layer. This layer includes a feature engineering module and an online learning module.

Feature Engineering Module: This module includes a ssAE algorithm to reduce the data's feature dimensions. The ssAE algorithm is an advanced neural network architecture primarily used for dimensionality reduction and feature extraction of the data. To generate the ssAE, multiple sparse autoencoder layers are stacked, with each layer's output serving as the layer's input. Thanks to its hierarchical structure, the network can gradually learn sophisticated, high-level features from data.

The core operation of the ssAE involves two key phases: encoding and decoding. During the encoding phase, the network compresses the input data X into a lower-dimensional representation H using the transformation:

$$H = \sigma(W_{ij}X + \phi_1) \tag{9}$$

where W_{ij} defines the weight matrix between the input and hidden layers of the ssAE, σ stands a nonlinear activation

function, and ϕ_1 is the bias vector for the hidden layer.

The decoding phase aims to reconstruct the input data from this compressed form, generating a reconstruction Y through the transformation:

$$Y = \sigma(W_{jk}H + \phi_2) \tag{10}$$

where the bias vector for the output layer is ϕ_2 and the weight matrix from the hidden layer to the output layer is W_{jk}. The objective is to minimise the reconstruction error, encouraging the network to preserve essential information while filtering out noise.

Moreover, the ssAE introduces a sparsity constraint on the hidden layer activation to enforce sparsity, ensuring that only a small fraction of neurons are active at any given time. This is achieved by penalising the deviation of the average activation of hidden neurons from a predefined sparsity parameter ρ, using the Kullback-Leibler (KL) divergence [25].

The overall loss function of the ssAE combines the reconstruction error with the sparsity penalty, facilitating the extraction of significant and compact representations from high-dimensional data.

$$J_{\text{sparse}}(W,b) = J(W,b) + \Theta \sum_{j=1}^{m} \text{KL}\left(\rho \middle\| \hat{\rho}_j\right) \tag{11}$$

where m represents the count of hidden units while Θ is a weighting factor that determines the intensity of the item. Furthermore, to avoid overfitting, the error function incorporates weight attenuation terms [25].

$$\begin{aligned} J_{\text{sparse}}(W,b) = J_E(W,b) + \Theta \sum_{j=1}^{m} \text{KL}\left(\rho \middle\| \hat{\rho}_j\right) \\ + \frac{\lambda}{2} \sum_{r=1}^{3} \sum_{i=1}^{m} \sum_{j=1}^{m+1} (w_{ij}^{r})^2 \end{aligned} \tag{12}$$

where λ denotes the weight attenuation coefficient.

Algorithm 1 shows the pseudocode of the ssAE algorithm, indicating that our ssAE module runs the ssAE algorithm to reduce the data dimension. Firstly, the inputs and outputs are specified in lines 1-2. After that, the encoder and decoder layers are initiated in lines 4-5. Lines 6-9 show the encoded data for each layer from *1* to *k*. Then, the final encoded representation X_k is set as Y, which is the data with reduced dimensions. The encoded data are decoded to reconstruct the input. In line 13, for each decoder from *k* down to *1*, the *i*-th decoder is applied to the output of the next layer up or the encoded representation if it is the first decoder in the sequence. Finally, the algorithm returns the reduced dimension data *Y*.

After reducing the dimension of the data in the ssAE module, the low-dimensional data is sent to the online learning module to decide on the network feature selection and classification methods.

Online Learning Module: This module includes a labelling algorithm from our previous study [26], an AutoFS component, an AutoCM element, and a final selection algorithm. We adjust the AutoFS and AutoCM elements from our prior work [27], [28] and update them according to the specific

Algorithm 1 Feature Dimension Reduction using ssAE.

1: **Input:** for every data point $X \in \mathbb{R}^{n \times m}$, n stands the number of samples, and m is the number of features
2: **Output:** Reduced dimension data Y
3: **procedure** SSAE(X)
4: Initialise encoder layers $E_1, E_2, ..., E_k$
5: Initialise decoder layers $D_1, D_2, ..., D_k$
6: **for** $i = 1$ to k **do**
7: $X_i \leftarrow$ Apply encoder E_i to X or X_{i-1} if $i > 1$
8: $X_i \leftarrow$ Apply sparsity constraint to X_i
9: **end for**
10: *# Encoded representation with reduced dimension*
11: $Y \leftarrow X_k$
12: **for** $i = k$ down to 1 **do**
13: $Y \leftarrow$ Apply decoder D_i to Y
14: **end for**
15: **return** Y
16: **end procedure**

requirements of the 6G IoV environment. Thanks to this module, our system works in a network-aware manner.

The AutoFS element contains five feature selection (FS) algorithms: chi-square, RFE, PCA, random forests for feature importance, and ANOVA F-value selection. Each algorithm is tailored to specific data types and requirements, allowing the system to dynamically choose the most appropriate method based on current data characteristics and network conditions.

The AutoCM component encompasses four classification methods (CM): MLP XGBoost, LSTM, and support vector machines (SVMs) detection algorithms to provide flexibility and adaptability in handling various attack scenarios within 6G IoV environments. Each algorithm serves a specific role: MLP is employed for complex pattern recognition, XGBoost is employed for its efficiency in structured data analysis, LSTM is used for sequential pattern detection, and SVM is used for high-dimensional classification.

Since we use supervised learning algorithms, we also define a labelling algorithm to label unlabelled data when updating the network FS and CM methods. This algorithm uses one thousand samples of the current network data, which is represented by u_{data} in *Y* and one thousand samples of the baseline data, which is signified by b_{data}. The pseudocode of our labelling algorithm can be seen in Algorithm 2. Firstly, the inputs and outputs are defined in lines 1-2. K-Means clustering is used to initially separate the u_{data} into two groups, setting $K = 2$ to categorize data likely based on the presence or absence of attacks in lines 4-5. The initial clusters are then used to configure the Expectation-Maximization (EM) algorithm. The EM algorithm is applied to assign probabilistic labels to the data in line 9. After that, b_{data} is used to enhance the labelling accuracy. The second EM process is then applied for refined labelling. Lastly, the new labels l' are merged with the baseline data b_{data}, and the fully labelled data l_{data} is returned in lines 16-18. This algorithm plays a crucial role in the dynamic updating of our framework's methods. We rigorously evaluate the accuracy of this algorithm using cross-validation techniques. In a series of evaluations, it achieved

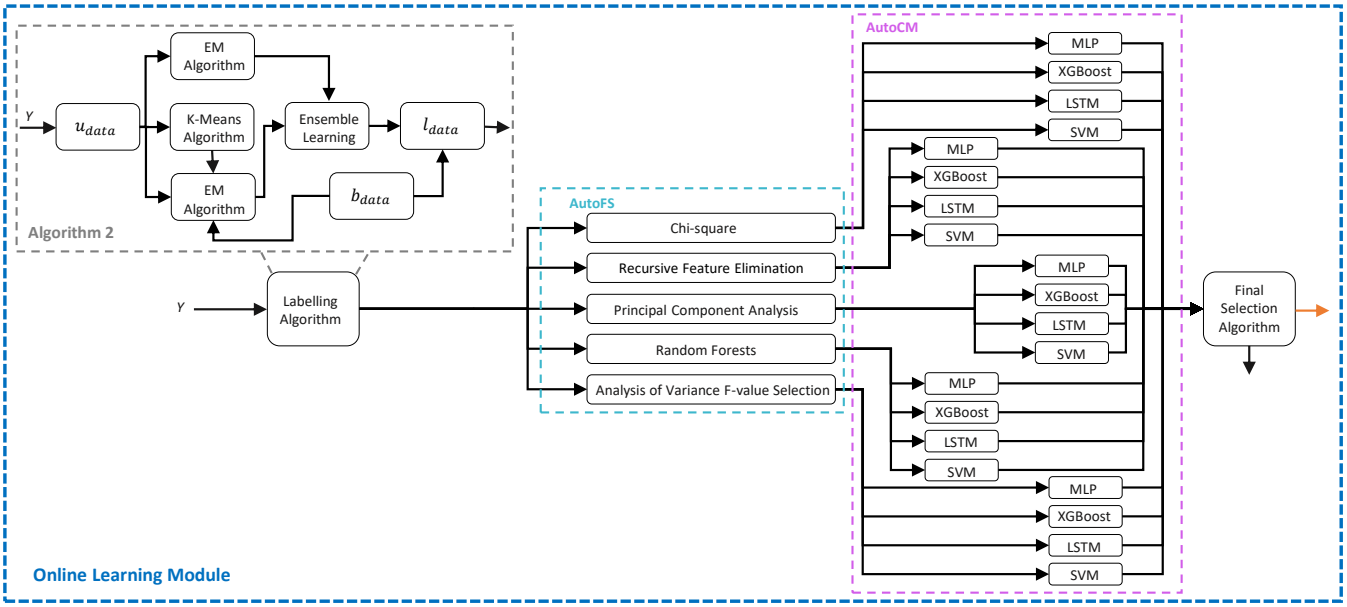

Fig. 5. The working logic of the proposed online learning module.

an accuracy of around 97.21%. This metric is critical as it ensures that the system can accurately process and label new and evolving data streams effectively. High labelling accuracy enhances the precision of our FS processes and the efficacy of classification algorithms, leading to improved detection rates of potential threats within the 6G IoV environment. To sustain this level of performance, the baseline dataset will be regularly updated at predefined intervals. These updates ensure that the algorithm remains aligned with the latest network behaviours and emerging threats, thereby maintaining high accuracy and adaptability in rapidly changing 6G IoV environments.

Algorithm 2 Labelling Algorithm.

Input: unlabelled data (u_{data}), baseline dataset (b_{data})
Output: labelled data (l_{data})
procedure LABEL(u_{data}, b_{data})
    Define $K = 2$ for K-Means algorithm
    Cluster u_{data} into two groups using K-Means
    # to determine the range of initial values
    Use the clusters for EM
    # to assign weighted probabilistic labels to u_{data}
    $x' \leftarrow$ Apply EM algorithm
    # b_{data} *includes 65% attack samples*
    Use b_{data} with its one thousand samples
    # to find the local maximum likelihood estimation
    $y' \leftarrow$ Combine b_{data} and u_{data}
    $y'' \leftarrow$ Apply the other EM algorithm using y'
    # to decide the final labels, take both EM outputs
    $l' \leftarrow$ Use ensemble learning x' and y''
    $l_{data} \leftarrow$ Merge l' with the b_{data}
    Return l_{data} with two thousand samples
end procedure

If any performance metrics fall below its specified threshold weights, the online learning module updates the network FS and network CM method, taking one thousand samples of the current network data using the labelling and final selection algorithms. This update information comes from the security layer, which checks the reliability of the system.

After taking the update information from the security layer, one thousand samples of the current network data are handled by the online learning module. The data is labelled using the labelling algorithm. After labelling the data, the AutoFS component uses this labelled data. Then, the output of the AutoFS is sent to the AutoCM element. The AutoCM trains and tests the data for each algorithm separately. After that, it sends each algorithm's precision, recall, and detection time metrics to the final selection algorithm. The working logic of the online learning module can be seen in Fig. 5.

Algorithm 3 delivers the pseudocode of our final selection algorithm. This algorithm decides on the network FS and CM techniques according to the precision, recall, and detection time metrics of the algorithms. The final selection algorithm sends the best FS approach information to the network FS method in the cyber twin layer, and then the network FS method starts to operate with this new algorithm. The final selection algorithm sends the best CM technique information to the network classification algorithm in the security layer, which then begins to operate with this new method. This adaptive selection ensures that the system can efficiently respond to emerging threats or changes in data and network environments, maintaining high performance in attack detection and system efficiency.

Thus, the online learning mechanism maintains the system's stable performance in a network-aware manner. It works nearly in real-time. To efficiently manage the computational intensity posed by multiple algorithms, we employ a microservice-based architecture where different components of the online learning module run as independent, smaller services. This enhances scalability and allows for the efficient management of different

Algorithm 3 Final Selection Algorithm

Input: precision (P), recall (R), and detection time (d_t) for each CM method and its pair FS techniques
Output: $bestFS$ and $bestCM$ for the system
procedure FINAL-METHODS(P, R, d_t)
    # to store precision, recall, and detection time for each FS and CM combination
    Initialize matrix M
    for $i = 1$ to 5 **do**
        for $j = 1$ to 4 **do**
            # metric vector for i^{th} FS and j^{th} CM
            $V_{ij} \leftarrow$ vector of P, R, d_t
            $M[i, j] \leftarrow V_{ij}$
        end for
    end for
    # α_{ij}, β_{ij} are the weights for i^{th} FS and j^{th} CM
    # ψ_{ij} is the weighted sum of P and R
    $bestFS$, $bestCM \leftarrow 0, 0$
    $maxScore \leftarrow$ -∞
    for $i = 1$ to 5 **do**
        for $j = 1$ to 4 **do**
            $\psi_{ij} \leftarrow$ (%55) $\times$ R + (%45) $\times$ P
            $score_{ij} \leftarrow \alpha_{ij} \times \psi_{ij} + \beta_{ij} \times d_t$
            if ($score_{ij} > maxScore$)
            $maxScore \leftarrow score_{ij}$
            $bestFS$, $bestCM \leftarrow$ i, j
            end if
        end for
    end for
    Return $bestFS$, $bestCM$
end procedure

algorithms running concurrently. Additionally, conditional activation of these methods ensures that computational resources are judiciously used, maintaining system performance without unnecessary resource expenditure. These strategies ensure that our framework remains both effective and efficient, capable of meeting the rigorous demands of 6G IoV networks.

3) Security Layer: This layer detects attacks in the IoV network. Our approach integrates a sophisticated classification architecture to classify the network traffic into "attack" or "not attack" categories. It includes the network classification algorithm, attack classification, and the verifying threshold components.

Recognising the dynamic nature of the 6G IoV environment, where network data flow and characteristics are subject to frequent changes, our system adopts an online learning module in the cyber twin layer. This continuous learning process is supported by monitoring the system reliability metric against the predefined threshold. If the metric value dips below the threshold, it triggers the update mechanism to the online learning module, which includes network-aware FS and CM selection processes in the cyber twin layer, to find the best suitable methods for the network in near real-time. This ensures that the model's performance remains stable and reliable, adapting to the evolving network environment and maintaining high accuracy in attack detection. We define the following objective to this end.

$$V(\Im) = \begin{cases} 1, & \text{if } \Re < \Im \\ 0, & \text{otherwise} \end{cases}$$

where $V(\Im)$ shows the verifying threshold function and $\Im$ is the threshold value; if it delivers "1," the update mechanism to the online learning module is triggered. The following objective is used to calculate the system reliability metric:

$$\Re = \frac{TP}{FN + TP} \tag{13}$$

where $\Re$ denotes the network classification algorithm reliability, emphasising the false negative (FN) and true positive (TP) metrics because of their importance in data classification. When an attack is not found, the verifying threshold component thoroughly examines the system's classification technique's reliability. The threshold ($\Im$) is calculated as:

$$\Im = \tau + \gamma_i \, \varrho \, , \quad \forall \, i \in [1, 4] \tag{14}$$

where τ is mean and ϱ is standard deviation. γ_i is the threshold factor of the ith classification algorithm.

This proactive and adaptive attack detection framework signifies a significant step forward in securing 6G IoV networks against an ever-growing spectrum of cyber threats, thereby safeguarding the integrity and reliability of vehicular communication systems.

IV. PERFORMANCE EVALUATION

We aim to demonstrate the effectiveness of our proposed framework in a simulated 6G IoV environment, in this section. The primary purpose of this experiment is to validate the framework's ability to handle dynamic and high-mobility scenarios typical in vehicular networks, while ensuring robust security and efficient resource management.

A. Simulation Environment and Strategy

To comprehensively assess the adaptability and robustness of our proposed novel framework, we utilized a combination of state-of-the-art simulation tools: OMNeT++ (version 5.1), SUMO (version 0.30.0), INET (version 3.6), and Veins (version 4.7), aligning with methodologies cited in previous studies [29]. These tools enable us to emulate a dynamic and realistic vehicular network environment where conditions such as vehicle speed, traffic density, and communication interference can change rapidly and unpredictably. We enhanced our simulation setup to include dynamic changes in network conditions that mimic real-world scenarios. By utilizing SUMO, we modelled different traffic patterns, including peak hours with high vehicle density and off-peak hours with lower traffic. This helps in assessing how well the framework manages data transmission and processing under varying loads. Using INET, we simulated varying communication channel qualities and interferences. The mobility patterns of the vehicles were varied to include different speeds and abrupt changes in direction to evaluate the system's ability to handle high-mobility scenarios typical of 6G IoV environments.

We created cyber twins of physical nodes (vehicles) in VANET using Eclipse Ditto, an open-source framework that is scalable and versatile [30]. Thanks to this tool, we can dynamically adjust the simulation parameters in real-time based on the emerging data from the vehicular network. This setup ensures that the system's response adapts to the simulated environment's evolving conditions, thereby demonstrating the practical application of our framework in a dynamic setting.

Our assessment concentrated on measuring the system's capability to lower end-to-end delay and enhance the detection of cyber threats, aiming to indicate the effectiveness and efficiency of our solution in improving network performance and security. We evaluated our proposed solution using two different datasets:

- The first, known as the RF Jamming Dataset, includes a variety of RF jamming attack scenarios in VANET environments, featuring two subsets for different maximum estimated relative speeds [31]. We merged these subsets to evaluate our proposed solution thoroughly. Features scenarios with RF jamming attacks, offering insights into how the system handles aggressive interference.
- The second dataset, ToN-IoT, is designed to test the robustness and efficacy of AI-based cybersecurity tools in next-generation IoT and industrial settings [32]. It provides a diverse range of IoT attack vectors, adding complexity and helping validate the framework's effectiveness against sophisticated cyber threats.

TABLE II
COMPOSITE DATASET DISTRIBUTION: COMBINED RF JAMMING AND TON-IOT DATASETS

Dataset Name	Number of Samples
RF Jamming Dataset-1 (No Attack Samples)	1000
RF Jamming Dataset-2 (No Attack Samples)	1000
ToN-IoT Network Dataset (Attack Samples)	600

Although the ToN-IoT is not initially VANET-focused, by integrating non-attack instances from the RF Jamming Dataset with attack cases from the ToN-IoT dataset, we built a new dataset tailored for our VANET security analysis. This composite dataset, detailed in Table II, was carefully curated to balance attack and non-attack samples, providing a comprehensive basis for our performance evaluation. The new dataset, which is combined with two datasets, is more IoT and VANET-oriented. Thus, we aim to get more comprehensive results for ITS using IoT and VANET data. We added randomly generated attack data samples to the vehicular data during the simulations, enhancing the dataset's ability to test the framework under varied and unexpected conditions.

B. Results

Firstly, we examined the attack detection performance of our proposed solution using both the RF jamming dataset and the composite dataset. Fig. 6 shows the performance results of our solution regarding attack detection rate, precision, and

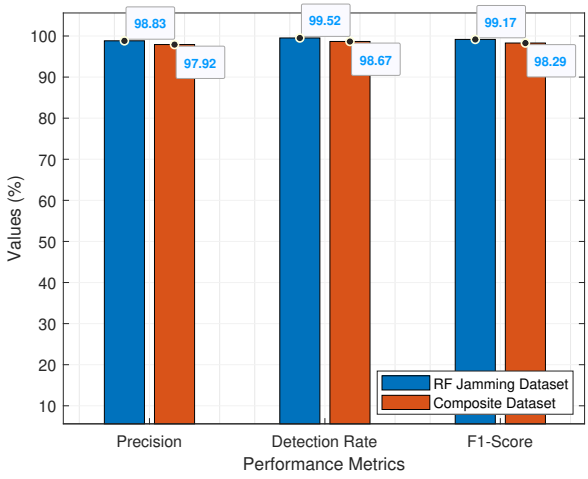

Fig. 6. The performance analysis of proposed solution across datasets.

F1-score. The RF jamming dataset results in around 99%, and the composite dataset results in stand around 98% success regarding performance metrics of the proposed solution. These results emphasise the stability of our proposed solution; further, the solution promises an essential feature identifying potential threats to ensure the security of VANETs.

After that, we scrutinised the effectiveness of our solution under dynamic conditions. To this end, we periodically injected attack samples from the composite dataset into the simulation to test the system's end-to-end latency, energy consumption, RAM usage, and packet delivery rate capabilities in real-time. This approach enables us to understand the system's responsiveness and adaptability to sudden changes in the attack landscape. The end-to-end latency measures the time taken for data to transmit from the source to the destination, which is crucial for real-time applications. The second metric, energy consumption, assesses the energy efficiency of the system under varying network loads and mobility patterns. The RAM usage metric helps us to evaluate the memory efficiency of the system, which impacts the speed and responsiveness of the data processing. The packet delivery rate checks the reliability of the network in delivering data packets correctly and completely despite the dynamic changes.

To compare the performance of our proposed solution (PS), we created another VANET digital twin network, which includes all processing components in its security layer without feature engineering. It utilises the LSTM algorithm for attack detection since it has been a more used method in VANET attack identification works [5], [33]. This network is called "VANET-2". This comparison highlights how well our system adapts to dynamic network changes compared to more traditional approaches.

To comprehensively evaluate the performance of our proposed framework under varying network loads, we meticulously analyzed the latency dynamics. In Fig. 7, the latency trends of the VANET-2 and our solution illustrate distinct performance characteristics as data volume increases. For VANET-2, there is a decrease followed by an increase in the

total end-to-end latency when the volume of data increases. This pattern is typical of traditional systems that initially handle increased loads efficiently but begin to struggle as the loads surpass the system's capacity to manage data efficiently. Conversely, our solution demonstrates significantly better performance. We achieve this by strategically dividing the computational load between the cyber twin layer and the security layer, which enables more efficient data processing and reduces the likelihood of congestion even as data volumes increase. This enhancement in our solution results in an approximately 12% reduction in system latency compared with VANET-2. Specifically, our solution incorporates advanced feature engineering in the cyber twin layer, which not only optimizes data processing but also ensures that the system adapts to increasing loads without the latency spikes seen in traditional systems. Similarly, Fig. 8 reveals that the proposed solution reduced the total energy consumption by approximately a 15% decrease compared to VANET-2. This metric is important since it quantifies the efficiency improvement in terms of energy usage.

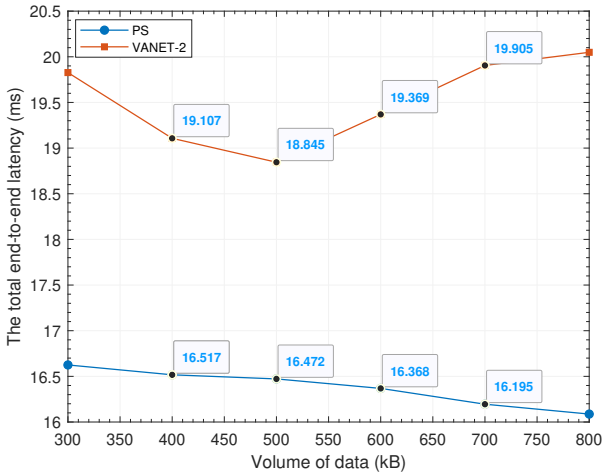

Fig. 7. The total end-to-end latency comparison regarding the volume of data.

After that, we investigated the total RAM usage and packet delivery rate of our solution. Fig. 9 depicts the total RAM usage comparison of our solution and VANET-2. While our solution shows a stable performance, minimising the total RAM usage, VANET-2 drastically consumes more RAM. Our solution improves the total RAM usage by around 20% when compared with VANET-2. The packet delivery rate comparison of our solution and VANET-2 can be seen in Fig. 10 over various simulation times. While VANET-2 exceedingly drops packets, our solution presents a stable performance to this end. Our solution slightly declines about 1.8% from its starting value to its final value. On the other hand, the VANET-2 system shows a more significant decrease, with about 7.9%. This indicates that our solution has improved performance over VANET-2 by approximately 6.1% throughout the simulation period in terms of packet delivery rate. Therefore, our solution is significantly more reliable in maintaining high packet delivery rates than VANET-2.

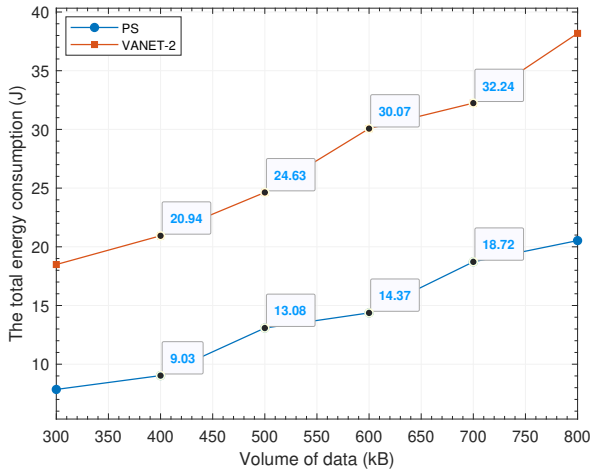

Fig. 8. The total energy consumption comparison regarding the data volume.

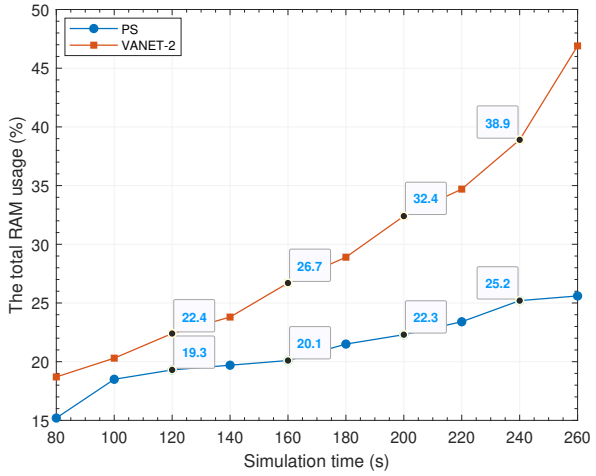

Fig. 9. The total RAM usage comparison regarding the simulation time.

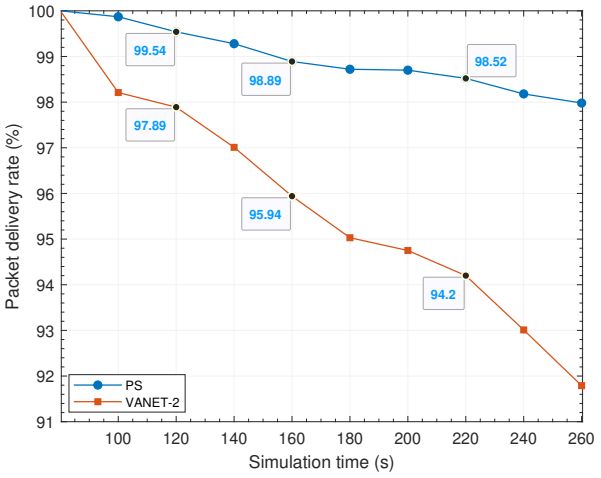

Fig. 10. The packet delivery rate comparison regarding the simulation time.

These performance results show the optimisation of our solution, which translates into more sustainable and cost-effective network operations, which is crucial for deploying secure and efficient advanced vehicular networks. Through rigorous simulation and analysis, we have demonstrated our digital twin enhanced framework's considerable RAM consumption reduction, robust attack detection capabilities, and increased packet delivery rates. These developments represent a major step towards more robust and environmentally friendly intelligent transportation networks. It also highlights the scalability and effectiveness of our system in supporting VANET defences against dynamic cyber threats. This advances the sustainability of vehicle networks and establishes a new benchmark for implementing advanced vehicular communications, representing a critical milestone in advancing intelligent transportation.

V. DISCUSSION

The practical implementation of the proposed system for 6G IoV networks requires careful consideration of several deployment, integration, and operational factors. Firstly, the infrastructure needs to support real-time communication and processing, with RSUs capable of handling advanced AI algorithms for analyzing data. It is also crucial to integrate software and hardware to ensure compatibility with existing vehicular communication standards and enable smooth operation across different network layers. For successful deployment, the framework should be able to work with current systems by using middleware solutions to manage data translations. Scalability and flexibility are key to handling increasing data volumes and changing technology landscapes, making cloud and edge computing essential parts of the system. Efficient real-time data processing is vital to keep latency low and responsiveness high. By addressing these practical aspects, the proposed framework can significantly improve the security and efficiency of 6G IoV networks, contributing to the development of intelligent and resilient transportation systems.

The proposed framework for 6G IoV networks offers significant advancements but also faces several challenges and limitations that need attention. One major challenge is managing the large amount of data generated by vehicles and RSUs while keeping latency low and processing timely. Another challenge is integrating the system with existing older infrastructure, which may not easily support advanced technologies. It is also complex to balance computational tasks while ensuring low latency and energy efficiency, especially in real-time scenarios. Scalability is another key concern, as expanding the framework to handle large-scale deployments in real-world settings requires more research and development. Additionally, the framework needs to adapt in real-time to quickly changing network conditions, which should be tested in various environments to ensure it is robust and reliable. Overcoming these challenges is crucial for optimizing the framework's performance and making sure it works well in real-world 6G IoV networks.

VI. CONCLUSION

In conclusion, we have introduced a novel AI-enhanced digital twin framework tailored to enhance the security and computational efficiency of the 6G IoV network. The proposed system employs an advanced feature engineering module using the ssAE algorithm for effective feature dimension reduction and a dynamic online learning module to maintain robust attack detection performance in real-time. Our approach distributes computational loads efficiently across the cyber twin and security layers, significantly improving system latency, energy consumption, and RAM usage. It improves RSU security and promotes sustainable communication by enhancing computational efficiency. Through comprehensive simulations, we demonstrated that our framework enhances computational efficiency and secures communication within VANETs. Against two datasets, our framework achieves around 98% success rate in attack detection metrics, demonstrating its potential to secure vehicular networks while promoting sustainable communication practices. In particular, it enhances the system latency by about 12%, the RAM usage by about 20%, decreases the total energy consumption by around 15%, and improves the packet delivery rates by approximately 6.1% throughout the simulation period against traditional architecture regarding the system computational efficiency. Our framework promises a safer and more effective future for vehicle communication and represents a critical step towards realising reliable, secure, and intelligent vehicular communication systems. Future research will focus on further enhancing the adaptability and scalability of the proposed framework.

REFERENCES

[1] SAM&SDH. Global Status Report on Road Safety 2023. [Online]. Available: https://www.who.int/publications/i/item/9789240086517, Accessed Date: Jan 15, 2024.

[2] Y. Yigit, I. Panitsas, L. Maglaras, L. Tassiulas, and B. Canberk, "CyberTwin: Digital Twin-Boosted Autonomous Attack Detection for Vehicular Ad-Hoc Networks," in *ICC 2024 - IEEE International Conference on Communications*, Denver, CO, USA, June 2024, pp. 2167–2172.

[3] T. Bilen, H. Ahmadi, B. Canberk, and T. Q. Duong, "Aeronautical Networks for In-Flight Connectivity: A Tutorial of the State-of-the-Art and Survey of Research Challenges," *IEEE Access*, vol. 10, pp. 20 053–20 079, 2022.

[4] H. Baharlouei, A. Makanju, and N. Zincir-Heywood, "Exploring Realistic VANET Simulations for Anomaly Detection of DDoS Attacks," in *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, Helsinki, Finland, June 2022, pp. 1–7.

[5] B. Lampe and W. Meng, "Intrusion Detection in the Automotive Domain: A Comprehensive Review," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, pp. 2356–2426, 2023.

[6] Y. Yigit, K. Huseynov, H. Ahmadi, and B. Canberk, "YA-DA: YAng-Based DAta Model for Fine-Grained IIoT Air Quality Monitoring," in *2022 IEEE Globecom Workshops (GC Wkshps)*, Rio de Janeiro, Brazil, December 2022, pp. 438–443.

[7] S. Dong, H. Su, Y. Xia, F. Zhu, X. Hu, and B. Wang, "A Comprehensive Survey on Authentication and Attack Detection Schemes That Threaten It in Vehicular Ad-Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 12, pp. 13 573–13 602, 2023.

[8] E. Bozkaya, K.-T. Foerster, S. Schmid, and B. Canberk, "AirNet: Energy-Aware Deployment and Scheduling of Aerial Networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12 252–12 263, 2020.

[9] M. Ariman, G. Seçinti, M. Erel, and B. Canberk, "Software defined wireless network testbed using Raspberry Pi of switches with routing add-on," in *2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN)*, San Francisco, CA, USA, November 2015, pp. 20–21.

[10] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, "BDTwin: An Integrated Framework for Enhancing Security and Privacy in Cybertwin-Driven Automotive Industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 18, pp. 17 110–17 119, 2022.
[11] R. Kumar, P. Kumar, A. Aljuhani, A. Jolfaei, A. N. Islam, and N. Mohammad, "Secure Data Dissemination Scheme for Digital Twin Empowered Vehicular Networks in Open RAN," *IEEE Transactions on Vehicular Technology*, pp. 1–13, 2023.
[12] H. Feng, D. Chen, and Z. Lv, "Blockchain in Digital Twins-Based Vehicle Management in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19 613–19 623, 2022.
[13] B. Li, X. Song, T. Dai, W. Wu, D. Zhu, X. Zhai, H. Wen, Q. Lin, H. Chen, and K. Cai, "Trust Management Strategy for Digital Twins in Vehicular Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 10, pp. 3279–3292, 2023.
[14] E. Ak and B. Canberk, "FSC: Two-Scale AI-Driven Fair Sensitivity Control for 802.11ax Networks," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, Taipei, Taiwan, December 2020, pp. 1–6.
[15] D. M. Gutierrez-Estevez, B. Canberk, and I. F. Akyildiz, "Spatio-temporal estimation for interference management in femtocell networks," in *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*, Sydney, NSW, Australia, September 2012, pp. 1137–1142.
[16] Y. Yigit, H. Ahmadi, G. Yurdakul, B. Canberk, T. Hoang, and T. Q. Duong, "Digi-Infrastructure: Digital Twin-enabled Traffic Shaping with Low-Latency for 6G Smart Cities," *IEEE Communications Standards Magazine*, vol. 8, no. 3, pp. 2–8, 2024.
[17] C. Schwarz and Z. Wang, "The Role of Digital Twins in Connected and Automated Vehicles," *IEEE Intelligent Transportation Systems Magazine*, vol. 14, no. 6, pp. 41–51, 2022.
[18] D. Van Huynh, S. R. Khosravirad, A. Masaracchia, O. A. Dobre, and T. Q. Duong, "Edge Intelligence-Based Ultra-Reliable and Low-Latency Communications for Digital Twin-Enabled Metaverse," *IEEE Wireless Communications Letters*, vol. 11, no. 8, pp. 1733–1737, 2022.
[19] V. Arya, A. Gaurav, B. B. Gupta, C.-H. Hsu, and H. Baghban, "Detection of Malicious Node in VANETs Using Digital Twin," in *Big Data Intelligence and Computing*, C.-H. Hsu, M. Xu, H. Cao, H. Baghban, and A. B. M. Shawkat Ali, Eds. Singapore: Springer Nature Singapore, 2023, pp. 204–212.
[20] M. Ali, G. Kaddoum, W.-T. Li, C. Yuen, M. Tariq, and H. V. Poor, "A Smart Digital Twin Enabled Security Framework for Vehicle-to-Grid Cyber-Physical Systems," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 5258–5271, 2023.
[21] Y. Yigit, O. K. Kinaci, T. Q. Duong, and B. Canberk, "TwinPot: Digital Twin-assisted Honeypot for Cyber-Secure Smart Seaports," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, Rome, Italy, May-June 2023, pp. 740–745.
[22] Z. Zhou, A. Gaurav, B. B. Gupta, M. D. Lytras, and I. Razzak, "A fine-grained access control and security approach for intelligent vehicular transport in 6g communication system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 9726–9735, 2022.
[23] L. Zhao, S. Li, Y. Guan, S. Wan, A. Hawbani, Y. Bi, and M. Guizani, "Adaptive Multi-UAV Trajectory Planning Leveraging Digital Twin Technology for Urban IIoT Applications," *IEEE Transactions on Network Science and Engineering*, pp. 1–16, 2023.
[24] Y. Yigit, L. D. Nguyen, M. Ozdem, O. K. Kinaci, T. Hoang, B. Canberk, and T. Q. Duong, "TwinPort: 5G Drone-assisted Data Collection with Digital Twin for Smart Seaports," *Scientific Reports*, vol. 13, p. 12310, 2023.
[25] B. Yan and G. Han, "Effective Feature Extraction via Stacked Sparse Autoencoder to Improve Intrusion Detection System," *IEEE Access*, vol. 6, pp. 41 238–41 248, 2018.
[26] Y. Yigit, B. Bal, A. Karameseoglu, T. Q. Duong, and B. Canberk, "Digital Twin-Enabled Intelligent DDoS Detection Mechanism for Autonomous Core Networks," *IEEE Communications Standards Magazine*, vol. 6, no. 3, pp. 38–44, 2022.
[27] Y. Yigit, C. Chrysoulas, G. Yurdakul, L. Maglaras, and B. Canberk, "Digital Twin-Empowered Smart Attack Detection System for 6G Edge of Things Networks," in *2023 IEEE Globecom Workshops (GC Wkshps)*, Kuala Lumpur, Malaysia, December 2023, pp. 178–183.
[28] E. Horsanali, Y. Yigit, G. Secinti, A. Karameseoglu, and B. Canberk, "Network-Aware AutoML Framework for Software-Defined Sensor Networks," in *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2021, pp. 451–457.
[29] F. A. Alhaidari and A. M. Alrehan, "A Simulation Work for Generating a Novel Dataset to Detect Distributed Denial of Service Attacks on Vehicular Ad hoc NETwork systems," *International Journal of Distributed Sensor Networks*, vol. 17, no. 3, p. 15501477211000287, 2021.
[30] Eclipse. Eclipse Ditto Documentation. [Online]. Available: https://www.eclipse.org/hono/docs/, Accessed Date: June 18, 2023.
[31] D. Kosmanos, D. Karagiannis, A. Argyriou, S. Lalis, Y. Yigit, and L. Maglaras. RF Jamming Dataset for Vehicular Wireless Networks. [Online]. Available: https://dx.doi.org/10.21227/4zwk-yw78, Accessed Date: May 20, 2023.
[32] N. Moustafa. ToN IoT datasets. [Online]. Available: https://ieee-dataport.org/documents/toniot-datasets, Accessed Date: May 20, 2023.
[33] Y. Yu, X. Zeng, X. Xue, and J. Ma, "LSTM-Based Intrusion Detection System for VANETs: A Time Series Classification Approach to False Message Detection," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 23 906–23 918, 2022.

Yagmur Yigit (Graduate Student Member, IEEE) is a PhD student in the School of Computing Engineering and The Built Environment. She received her MSc in the Department of Computer Engineering at the Istanbul Technical University and her BSc in Mechatronics Engineering from Istanbul Aydin University in 2023 and 2017, respectively. She worked as an R&D engineer at General Mobile, a Turkish smartphone company, for two years and as a 5G R&D engineer at Netas, a Turkish company operating in information technologies, for one year. She was also one of the DeepMind scholars in 2020-2022 and a Turkcell Research Assistant in 2023. Her research focuses on AI-assisted and digital-twin-enabled next-generation cyber-secure networks.

Leandros A. Maglaras (Senior Member, IEEE) is a professor of cybersecurity in the School of Computing at Edinburgh Napier University. From September 2017 to November 2019, he was the Director of the National Cyber Security Authority of Greece. He obtained a B.Sc. (M.Sc. equivalent) in Electrical and Computer Engineering from the Aristotle University of Thessaloniki, Greece in 1998, an MSc in Industrial Production and Management from the University of Thessaly in 2004, and M.Sc. and PhD degrees in Electrical & Computer Engineering from the University of Thessaly, in 2008 and 2014 respectively. In 2018, he was awarded a PhD in Intrusion Detection in SCADA systems from the University of Huddersfield. He is featured in Stanford University's list of the world's Top 2% scientists. He is a Senior Member of the Institute of Electrical & Electronics Engineers (IEEE) and is an author of more than 200 papers in scientific magazines and conferences.

William J. Buchanan (Senior Member, IEEE) is currently a Professor with the School of Computing, Edinburgh Napier University. He also leads the Centre for Distributed Computing, Networks, and Security, and the Cyber Academy, and involved in the areas of security, cloud security, web-based infrastructures, e-crime, cryptography, triage, intrusion detection systems, digital forensics, mobile computing, agent-based systems, and security risk. He has one of the most extensive academic sites in the World and is involved in many areas of novel research and teaching in computing. He has published more than 27 academic books and more than 250 academic research articles, along with several awards for excellence in knowledge transfer, and for teaching. He is a fellow of BCS and IET. He was named as one of the Top 100 People for Technology in Scotland from 2012 to 2017. Recently, he was included in the FutureScot Top 50 Scottish Tech People who are changing the world. He was awarded the OBE in the Queen's Birthday Award, in June 2017.

Berk Canberk (Senior Member, IEEE) is a Professor within the School of Computing, Engineering and The Built Environment at Edinburgh Napier University-UK, where he leads interdisciplinary research and initiatives in AI-enabled Digital Twins, IoT Communication, and Smart Wireless Networks. He's also an Affiliated Professor within the Department of Artificial Intelligence and Data Engineering at Istanbul Technical University (ITU) and Adjunct Faculty within the Department of Electrical and Computer Engineering at Northeastern University USA. He is also the Innovation Director of BTS Group, the biggest network automation and cloud computing company in Turkey. He is a distinguished recipient of the UK Royal Academy of Engineering's Global Talent Endorsement. He is an active Associate Editor at several world-leading academic journals such as IEEE Transactions on Vehicular Technology, Elsevier Computer Networks Journal, Elsevier Communication Networks Journal, and IEEE Communications Letters. He's actively involved in several conferences as TPC chair and Organizing Committee Member. He has been a Post-Doctoral researcher at Georgia Institute of Technology USA between 2011-2013. He received his PhD in Computer Science from ITU Turkey in 2011, his MSc in Telecommunications Engineering from the Chalmers University of Technology Sweden in 2005, and his BSc in Electrical Engineering from ITU in 2003. He was an Associate Professor at the Department of Computer Engineering at ITU between 2016-2021 and a full Professor between 2021-2022. He has been involved with several industrial research activities with leading technology companies worldwide, including research scholarship program funding with Google Deepmind, TUBITAK, BTS Group Turkey, Turkcell, Turkish Telekom, and Uniper Energy Germany.

Hyundong Shin (Fellow, IEEE) received the B.S. degree in electronics engineering from Kyung Hee University (KHU), Yongin-si, South Korea, in 1999, and the M.S. and Ph.D. degrees in electrical engineering from Seoul National University, Seoul, South Korea, in 2001 and 2004, respectively. During his Postdoctoral Research at the Massachusetts Institute of Technology (MIT) from 2004 to 2006, he was with the Laboratory for Information Decision Systems (LIDS). In 2006, he joined the KHU, where he is currently a Professor with the Department of Electronic Engineering. His research interests include quantum information science, wireless communication, and machine intelligence. Prof Shin received the IEEE Communications Society's Guglielmo Marconi Prize Paper Award in 2008 and the William R. Bennett Prize Paper Award in 2012. He served as the Publicity Co-Chair for the IEEE PIMRC in 2018 and the Technical Program Co-Chair for the IEEE WCNC (PHY Track 2009) and the IEEE GLOBECOM (Communication Theory Symposium 2012 and Cognitive Radio and Networks Symposium 2016). He was an Editor of IEEE Transactions On Wireless Communications from 2007 to 2012 and IEEE Communications Letters from 2013 to 2015.

Trung Q. Duong (Fellow, IEEE) is a Canada Excellence Research Chair (CERC) and a Full Professor with Memorial University, St. John's, NL, Canada. He is also the Adjunct Chair Professor of Telecommunications with Queen's University Belfast, Belfast, U.K., and a Research Chair of Royal Academy of Engineering, London, U.K. He was a Distinguished Advisory Professor with Inje University, Gimhae, South Korea, from 2017 to 2019, an Adjunct Professor and the Director of Institute for AI and Big Data with Duy Tan University, Da Nang, Vietnam, since 2012, and a Visiting Professor (under Eminent Scholar Program) with Kyung Hee University, Seoul, South Korea, from 2023 to 2025. His current research interests include quantum communications, wireless communications, quantum machine learning, and optimization. Prof. Duong received the Best Paper Award at the IEEE VTC-Spring 2013, IEEE ICC 2014, IEEE GLOBECOM 2016, 2019, 2022, IEEE DSP 2017, IWCMC 2019, 2023, and IEEE CAMAD 2023. He has received the two prestigious awards from the Royal Academy of Engineering (RAEng): the RAEng Research Chair (2021–2025) and the RAEng Research Fellow (2015– 2020). He is the recipient of the Prestigious Newton Prize 2017. He has served as an Editor/Guest Editor for the IEEE Transactions On Wireless Communications, IEEE Transactions On Communications, IEEE Transactions On Vehicular Technology, IEEE Communications Letters, IEEE Wireless Communications Letters, IEEE Wireless Communications, IEEE Communications Magazines, and IEEE Journal On Selected Areas In Communications.