Date of publication MAR-31, 2024, date of current version FEB-06, 2024
www.computingonline.net/ computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.23.1.3443

Novel Intelligent BSM Falsification Attack Detection System Using Trusted Neighbor Vehicle Approach in IoV

HUSSAINI ALIYU IDRIS[1],KAZUNORI UEDA[2],BASSEM MOKHTAR[3,5],SAMIR A. ELSAGHEER MOHAMED[1,4]

[1]Department of Computer Science and Engineering,
Egypt-Japan University of Science and Technology (E-JUST),
New Borg-El-Arab City Postal Code 21934,
Alexandria, Egypt (e-mail: {hussaini.idris,samir.elsagheer}@ejust.edu.eg)
[2]Department of Computer Science and Engineering,
Waseda University Tokyo, Japan. (e-mail:ueda@ueda.info.waseda.ac.jp)
[3]Department of Electrical Engineering, Faculty of Engineering,
Alexandria University Alexandria 21544, Egypt
[4]Faculty of Engineering, Aswan University, Aswan, Egypt
[5]College of Information Technology UAE University,
Al Ain 15551, UAE (e-mail:bassem.mokhtar@uaeu.ac.ae)

Corresponding author: Hussaini Aliyu Idris (e-mail:hussaini.idris@ejust.edu.eg)

ABSTRACT The proliferation of cyberattacks has emerged as a significant obstacle for advancing technologies such as the Internet of Things (IoT) and Internet of Vehicles (IoV) in recent times. Notably, cryptographic security measures have been implemented in IoV to counteract these cyberattacks. However, these security measures are inadequate when it comes to thwarting internal attackers within the network, as these attackers possess the necessary security credentials for authenticating basic safety messages (BSMs). The research community has made substantial contributions by proposing misbehavior detection systems (MDS) based on data-centric machine learning to identify and prevent internal attackers within IoV. Nevertheless, the existing MDSs in the literature rely on BSMs received from a single vehicle, thereby enabling internal attackers to manipulate their falsified BSMs and evade detection, resulting in a high incidence of false alarms. In this study, we introduce a new intelligent system for detecting falsified BSMs, employing a trusted neighbor vehicle approach (**NIBFADS-UTVA**)). Our approach demonstrates exceptional effectiveness, achieving an accuracy, precision, recall, and F1-Score all exceeding 99%.

KEYWORDS Machine learning; Intelligent Transportation System; Misbehavior detection system (MDS); Intrusion detection system (IDS); internet of vehicle (IoV); BSM falsification attack; deep learning; connected and autonomous vehicles (CAVs)

I. INTRODUCTION

The rapid advancement of information and communication technology (ICT) has facilitated the exchange of large volumes of data among physical devices equipped with sensors, forming a network known as the Internet of Things (IoT). This network encompasses a wide range of smart devices, from small wearables to large-scale industrial machinery, smart cities, and transportation systems [1]. Within this IoT framework, the concept of the Internet of Vehicles (IoV) has emerged [2].

In the IoV, connected and autonomous vehicles (CAVs) are equipped with onboard units (OBUs) that enable communication with other CAVs through vehicle-to-vehicle communication (V2V) [3]. They can also exchange information with roadside infrastructure units called road side units (RSUs) through vehicle-to-infrastructure communication (V2I). Other forms of communication, such as vehicle-to-sensor (V2S), vehicle-to-pedestrian (V2P), and vehicle-to-cloud (V2C), collectively known as vehicle-to-everything (V2X), are also possible[4], [5]. These communications

primarily occur wirelessly through protocols like IEEE 802.11P, wireless access in vehicular environments (WAVE), dedicated short-range communication (DSRC), or cellular networks like 4G/LTE, 5G, and Beyond [6]–[8].

The IoV facilitates the operation of intelligent transportation systems (ITS) by enabling real-time exchange of transportation messages for both safety and non-safety applications [9]–[11]. Among these messages, the basic safety message (BSM) is crucial as it contains important kinematic data of vehicles, such as speed, position, heading, acceleration, and other vital information for traffic management and accident prevention through forward collision warning, blind spot caution and intersection warning etc [12] . To ensure secure communication, cryptographic security techniques like public-key infrastructure (PKI) with a security credentials management system (SCMS) are used to digitally sign and authenticate BSMs, allowing communication only among authorized vehicles [13].

However, these cryptographic techniques alone cannot protect against internal attackers who possess valid authentication credentials, posing a risk to user safety and traffic management [14]. To address this vulnerability, an intelligent intrusion detection system or data-centric misbehavior detection system (MDS) that utilizes artificial intelligence (AI) techniques such as machine learning and deep learning is necessary. These systems aim to identify anomalous behaviors exhibited by authenticated users within the network.[15].

Various machine learning and deep learning-based approaches have been proposed in the research community to detect misbehavior in IoV [16], [17]. However, existing approaches have limitations in accurately detecting attackers because they rely solely on BSMs collected from a single vehicle, which could be an attacker's vehicle. This reliance allows attackers to manipulate falsified BSMs and evade detection. To overcome this limitation, we propose a novel data-centric smart anomaly detection system that employs a trusted-neighbor vehicle approach. The contributions of this paper are as follows:

- We propose a smart anomaly detection system for basic safety message (BSM) which can be deployed on both OBUs and RSUs to ensure redundancy and enable implementation in both urban and rural IoV networks.
- We also generated a novel dataset from BurST-ADMA based on trusted-neighbor vehicle approach by using data processing techniques.
- We finally investigated different machine learning and deep learning classifiers to achieve outstanding accuracy, precision, and recall.

. The rest of the paper is organized as follows. We review the related work in Section II. Section III presents the proposed data-centric machine learning-based framework for the detection of false data injection attacks in IoV. Section IV discusses the simulation studies and the obtained results. The paper concludes and a highlight for future work is given in Section V.

II. RELATED LITERATURE REVIEW

The field of intelligent intrusion detection systems or data-centric misbehavior detection systems (MDS) for the Internet of Vehicles (IoV) has seen significant research activity in recent years. Several studies have explored the application of machine learning and deep learning techniques to identify and mitigate false data injection attacks within the IoV network as described by the authors of comprehensive surveys in[18], [19].

For instance, in one study in [20], the authors presented a supervised learning-based MDS to identify position falsification attacks by changing the VeReMi dataset [21] to produce another dataset comprising two successive BSMs.

Moreover,in [22], the authors propose an ensemble random forest classifier called "Ens. RF" that utilizes hyperparameter tuning and majority voting to detect false basic safety messages (BSMs) in IoV. The performance of "Ens. RF" is compared against other classifiers such as DT, CNB, KNN, GB, RCCV, and other related works, demonstrating its superior performance. The suggested deployment of "Ens. RF" is on roadside units (RSUs) for inference.

Similarly, another study in [23] introduces a Randomized Search Optimization Ensemble-based Falsification Detection Scheme (RSO-FDS) for identifying false BSM transmissions by malicious vehicles in the IoV network. The scheme employs an ensemble of Random Forest with majority voting and utilizes the BurST-ADMA dataset for evaluation, considering metrics such as training time, accuracy, precision, and F1-Score.

Furthermore, in [24], an ensemble of AdaBoost classifiers is proposed to detect false messages in IoV using the BurST-ADMA dataset. The performance of this approach is compared with other ensemble-based machine learning classifiers, evaluating metrics such as accuracy, recall, precision, and F-measure.

In a different approach, [25] presents a scheme that utilizes a deep learning binary classification model deployed at the RSU edge server. This model assesses message trustworthiness based on a vehicle's dependability score (VDS), assigned by a Trusted Authority (TA) during vehicle network entry. Additionally, a Graph Temporal Network (GTN) with attention mechanisms is employed to identify potentially malicious vehicles based on time-sequential data.

Lastly, [26] proposes an approach called iRMDS, where a vehicle collects data from internal sensors and Cooperative Aware Messages (CAM) from neighboring vehicles in a noisy traffic scenario. The collected data is processed using a Kalman filter to extract features, which are then utilized to train a multilayer perceptron (MLP) classifier.

To sum up, all the reviewed proposed misbehavior detection systems relied heavily on collecting training and prediction data from a single vehicle's BSM, hence handing the attacker full freedom of manipulating the BSM to

avoid detection by the MDS. To summarize, several studies have focused on the application of machine learning and deep learning techniques for misbehavior detection in IoV. However, a common limitation in these approaches is their reliance on BSMs collected from a single vehicle, which allows attackers to manipulate the data and evade detection

III. THE PROPOSED NIBFADS-UTVA APPROACH

In this section, we present the preliminary assumptions made, the system model used in this proposed approach, the dataset used, the proposed approach, and the methodology.

A. PRELIMINARY ASSUMPTIONS

Within the context of this research, certain assumptions were made, which are outlined in this section. Firstly, it is assumed that all police cars, ambulances, licensed public buses, and licensed public trams have obtained a trust flag during their registration within the Internet of Vehicles (IoV) network. This trust flag is then associated with their unique vehicle identification numbers and corresponding allocated pseudonyms, ensuring that their pseudonyms possess distinct patterns. This essential information is stored in a shared database between a trusted authority (TA) and a local authority (LA). To maintain the integrity of the system, the shared database is regularly updated whenever a trusted vehicle is identified as falsifying Basic Safety Messages (BSMs) through the proposed Misbehavior Detection System (MDS). Consequently, such a vehicle will be reported and subsequently removed from the database.

Secondly, it is assumed that each vehicle and Roadside Unit (RSU) within the network have the capability to retain previously received BSMs for a minimum duration of 1 minute. This enables the retrieval of BSMs received from trusted vehicles and facilitates the calculation of distances between the current BSM and trusted BSMs received within a specific timeframe. This distance calculation aids in determining the nearest trusted vehicle.

B. THE SYSTEM MODEL

This paper adopts a fully functional IoV network that encompasses various communication modalities, as depicted in Figure 1. The vehicles are equipped with Onboard Units (OBUs), enabling the exchange of BSMs with other vehicles (V2V) or with RSUs (V2I) through Dedicated Short-Range Communication (DSRC) or cellular Vehicle-to-Everything (V2X) technologies. Additionally, the RSUs maintain an edge server that provides computational advantages for deploying the proposed model and expedites the processing of stored BSMs for inference. Similarly, the vehicles also possess a small database that allows for easy querying of previous BSMs during inference. Moreover, the network incorporates a local authority (LA) responsible for monitoring traffic and receiving anomalies or misbehavior reports (MR) from vehicles and RSUs. These reports are subsequently transmitted to the trusted authority (TA) via a high-speed communication channel, such as the 5G cellular network.

C. DATASET DESCRIPTION

In this study, the publicly available BurST-ADMA dataset [27] is utilized due to its suitability for IoV scenarios, as it encompasses diverse types of position and speed attacks (BSM falsification attacks). This dataset was generated by simulating a 1000-second SUMO traffic scenario in Burwood, a suburb in Melbourne, Australia, with a 1-second interval by using VEINS [28]. It includes various simulated nodes such as public buses, public trams, trucks, pedestrians, motorcycles, and bicycles. Each BSM entry within the dataset contains false kinematic features of a vehicle, introduced by attackers to cause road crashes and traffic congestion. These features comprise longitude (x), latitude (y), vehicle ID, timestep, speed, acceleration, heading, and label. The dataset encompasses a total of 207,315 BSMs, with 28,189 belonging to seven categories of attacks, namely: (i) constant random position, (ii) positive position offset, (iii) negative position offset, (iv) constant random speed, (v) positive speed offset, (vi) negative speed offset, and (vii) reversed heading attacks, as illustrated in Table 1.

To further enhance the research, a new dataset was derived from the aforementioned BurST-ADMA dataset using **Algorithm 1** . This new dataset includes 13 features, namely: (i-ii) both vehicle and trusted neighbor vehicle (TNV) IDs, (iii-vi) latitude and longitude of the vehicle and NTV, (vii-xii) their speed, heading, and acceleration, and (xiii) the vehicle's label. Notably, the new NTV dataset retains the same number of attacks as the original dataset.

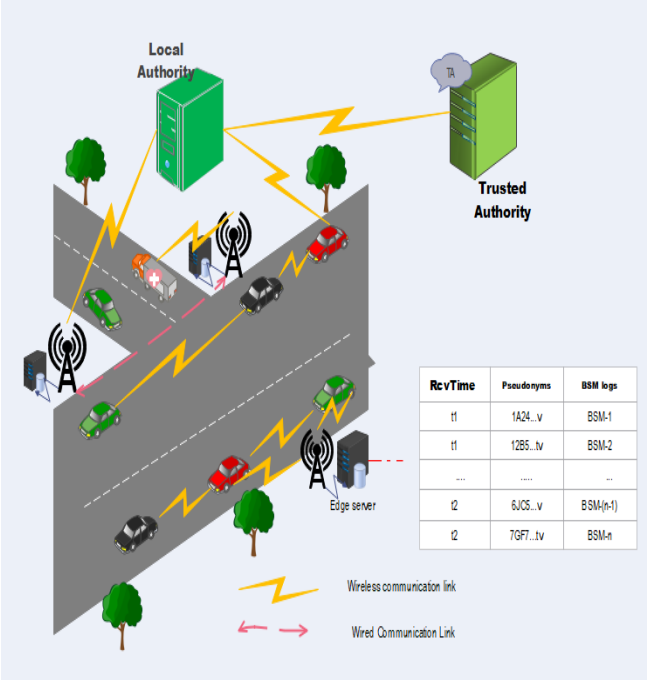

Figure 1. The IoV System Model

Table 1. BurST-ADMA Dataset Showing Attack Distribution

Label	Attack Type	No. of Samples
0	Normal	179126
1	Constant Random position	2110
2	Positive position offset	4130
3	Negative position offset	4512
4	Constant Random speed	4106
5	Positive speed offset	4720
6	Negative speed offset	4755
7	Reversed heading	3856

Algorithm 1: TNV Dataset Creation

Begin
INPUTS:
data ← BurST-ADMA Dataset
OUTPUT:
TNV Dataset
STEPS:
trusted-Id ← BurST-ADMA[*id* contains "ptv"|"amb"|"pol"|"p-tram"]
BSM_{TNV} ← BurST-ADMA[*trusted-id*]
For each *time-step* in data:
  For each BSM in data[*time-step*]:
    distance ← Min(calculate_Distance(BSM, BSM_{TNV}))
    If (distance not zero):
      dataset ← concat([BSM,BSM_{TNV}[distance]])
      TNV Dataset.append(dataset, inplace=True)
  End for
End for
End

D. THE PROPOSED APPROACH

The proposed approach is founded on the observation that vehicles in close proximity within a traffic scenario often exhibit similar driving patterns. Leveraging this insight, machine learning and deep learning algorithms can be employed to analyze Basic Safety Messages (BSMs) data from neighboring vehicles, enabling the detection of anomalous behavior within the network.

In essence, the operation of the proposed approach commences when a suspicious BSM, denoted as BSM_{veh}, is received by another vehicle or Roadside Unit (RSU) at time *t*. To assess the veracity of this BSM, all previous BSMs from trusted vehicles, referred to as $BSM_{trusted}$, received within a specified time range between $t-\alpha$ (where α can be zero) and *t*, are retrieved from the database of previously received BSMs, denoted as **BSM-DB**. In order to determine the nearest neighbor among the trusted vehicles, Equations (1), (2) and (3) are employed to calculate the distance between BSM_{veh} and all $BSM_{trusted}$.

To facilitate the prediction and eventual detection of attack vehicles, a machine learning classifier that has been fine-tuned through hyperparameter optimization is utilized. This classifier possesses the ability to learn the data patterns within the two BSMs. Notably, the haversine formula [29], renowned for its accurate distance calculations on the Earth's surface, is employed in this research, particularly due to the presence of latitude and longitude coordinates in each BSM entry within the original dataset. The equations for distance calculation are as follows:

$$a = \sin^2((\phi B - \phi A)/2) + \cos\phi A \cdot \cos\phi B \cdot \sin^2((\lambda B - \lambda A)/2) \quad (1)$$

$$c = 2 \cdot \arcsin(\sqrt{a}) \quad (2)$$

$$distance = R \cdot c \quad (3)$$

Where ϕA is the latitude of BSM_{veh}, ϕB is the latitude of $BSM_{trusted}$, λA is the longitude of BSM_{veh}, λB is the longitude of $BSM_{trusted}$, and R is the earth's radius (mean radius = 6,371km).

E. METHODOLOGY

The first phase of the methodology begins with the Trusted neighbor vehicle (TNV) dataset generation according to **Algorithm 1** as illustrated in Figure 2. The algorithm takes as input BSMs from BurST-ADMA dataset containing feature set $F = \{f_1 \ldots, f_n\}$ and label set $L = \{l_0, \ldots, l_7\}$. It is worth mentioning that the status of a vehicle *v* in the network must belong to either the set of trusted vehicles (TV) or untrusted vehicles (UTV). The ID column of every BSM in the dataset is checked and if it contains any of ptv, amb, pol or p-tram which are short for public transport vehicle, ambulance, police car, and public tram, respectively, it means that the BSM belongs to TV; and otherwise it belongs to UTV. The reception time *t* of every BSM from non-trusted vehicle BSM_{veh} is used to search for all previous BSMs from trusted vehicles ($BSM_{trusted}$) with the same reception time interval. The haversine formula is used to determine the nearest $BSM_{trusted}$ to the suspicious BSM and both BSMs data consitutes the TNV dataset with the label column of $BSM_{trusted}$ removed.

The next phase of the workflow focuses on preprocessing the data obtained from the previous phase. The missing values are first filled appropriately using domain knowledge and duplicated records are removed to prevent the ML classifiers from being biased. Furthermore, the features are scaled and normalized using Equation (4) to ensure all the features are within the same scale. Lastly, the data is split into 70% for training and 30% for testing with stratified sampling to ensure equal representation of all attack types.

$$X_{Scaled} = \frac{X_i - X_{min}}{X_{max} - X_{min}} \quad (4)$$

where X_{Scaled} is the scaled feature, X_i is the i^{th} feature, X_{max} and X_{min} are maximum and minimum values of the i^{th} feature, respectively.

The hyper-parameter tuning phase sets up hyper-parameters such as criterion, n_estimators, min_samples_split, base_estimator, number of hidden layers, activation function, number of epochs and batch_size according to the classifiers with a range of possible values. The hyper-parameters values are sampled using GridSearchCV with cross-validation and the values with the best score are selected as shown in Table 2. Finally, the values are validated using K-fold cross-validation.

Table 2. GridSearchCV Result for Hyper-parameters Used in this paper

ML Classifier	Hyper-parameter Possible Values	Hyper-parameter Best Values
RF	n_estimators={50,100,200} criterion={gini,entropy, log _loss } Min _samples_split={2,4,8}	n_estimators=50 criterion='gini' min_samples_split=2
KNN	n_neighbors={3,4,5} criterion={gini,entropy, log _loss } Min_samples_split={2,4,8}	n_neighbors=3 criterion='log _loss' min _samples_split=4
DT	max_depth={20,50,100} criterion={gini,entropy, log _loss } Min_samples_split={2,4,8}	max_depth=50 criterion='log _loss' min _samples_split=4
AdaBoost	base_estimators={DT,RF} n_estimators ={20,50,100}	base_estimators=DT n _estimators=50
MLP	Num_hidden_layers={2,3,4} Epochs={20,50,100} batch_size={32,64,128} activation_func={tanh,relu}	Num_hidden_layers=4 Epochs=50 batch _size=64 activation_func=relu

The training phase used the parameters with the best score obtained from the GridSearchCV as presented in Table 2 to train each of random forest (RF), decision tree (DT), K-Nearest neighbor (KNN), AdaBoost, and multilayer perceptron (MLP) classifiers on the training set and utilized the K-Fold cross-validation to validate the model's performance. Finally, the models are saved.

In the final phase, the learned models are loaded and predictions are made on the test data for all the classes since stratified sampling was used during the data split into training set and testing set. For evaluation purposes, confusion matrices of true labels against predicted labels are plotted; and the macro average of accuracy, precision, recall, and F1-Score are used to evaluate the models. The performance metrics are visualized using matplotlib library as illustrated in Section IV.

F. EXPERIMENTAL SETUP

This subsection presents the experimental setup employed in this paper to conduct the experiments. The experiments were conducted on a Dell Precision 5520 machine equipped with an Intel(R) Core (TM) i7-7820HQ CPU running at 2.90GHz. The machine had 4 cores, 8 logical processors, and 16GB of RAM.

The Python scikit-learn library was utilized for various tasks in the experimental setup. This included handling missing values, splitting the data into training and testing sets, applying the Synthetic Minority Oversampling Technique (SMOTE) for handling the imbalanced dataset, and training the machine learning multiclass classifiers, such as Random Forest (RF), Decision Tree (DT), AdaBoost, and K-Nearest Neighbors (KNN).

For hyperparameter tuning, the GridSearchCV method was employed. This technique helps in finding the best combination of hyperparameters for each classifier, optimizing their performance.

In addition to the scikit-learn library, the Keras module from the TensorFlow framework was used to train a multiclass Multilayer Perceptron (MLP) model. The MLP consisted of four hidden layers with 128, 64, 32, and 16 neurons, respectively. The ReLU activation function was applied to all the hidden layers. The model was trained for 50 epochs with a batch size of 64.

To evaluate the models, various metrics were used, including the macro average of accuracy, recall, precision, and F1-score. These metrics provide an overall assessment of the performance of the classifiers.

For result analysis and visualization, the matplotlib library and the scikit-learn confusion matrix function were utilized. These tools helped in analyzing and presenting the experimental results in a clear and informative manner.

By following this experimental setup, the paper ensured a standardized and reproducible environment for conducting the experiments and evaluating the performance of the proposed approach.

IV. RESULT ANALYSIS AND DISCUSSIONS

In this section, the results obtained from the experiments conducted in this paper using the proposed novel intelligent Basic Safety Message (BSM) falsification attack detection System using trusted neighbor vehicles approach (NIBFADS-UTVA) are presented and evaluated. The evaluation metrics used include accuracy, precision, recall, and F1-score, which are calculated using the following equations:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{5}$$

$$Precision = \frac{TP}{TP + FP} \tag{6}$$

$$Recall = \frac{TP}{TP + FN} \tag{7}$$

$$F1 - Score = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall} \tag{8}$$

Where TP, TN, FP, and FN are the true positive, true negative,false positive and false negative respectively.

A. COMPARISON BETWEEN THE CLASSIFIERS

Here,the comparison between different classifiers in this paper is provided, and the performance of each classifier is discussed.

As we have shown in Figure 9 and Table 3, the result obtained when the proposed trusted neighbor vehicle approach is applied is significantly higher compared to when the proposed approach is not employed. For example, the recall of 91.36%,92.03%,78.34%, 90.39% and 92.36% recorded by RF,DT,KNN,AdaBoost and MLP is not good enough for deployment in IoV network.

On the other hand, the classifers have shown a significant improvement in all metrics when the proposed approach is applied. For instance,the Random Forest (RF) multiclass classifier is shown to have the second-best performance, with an accuracy of 99.96% and 99.93% precision, recall, and F1-score. The RF classifier performs well in detecting

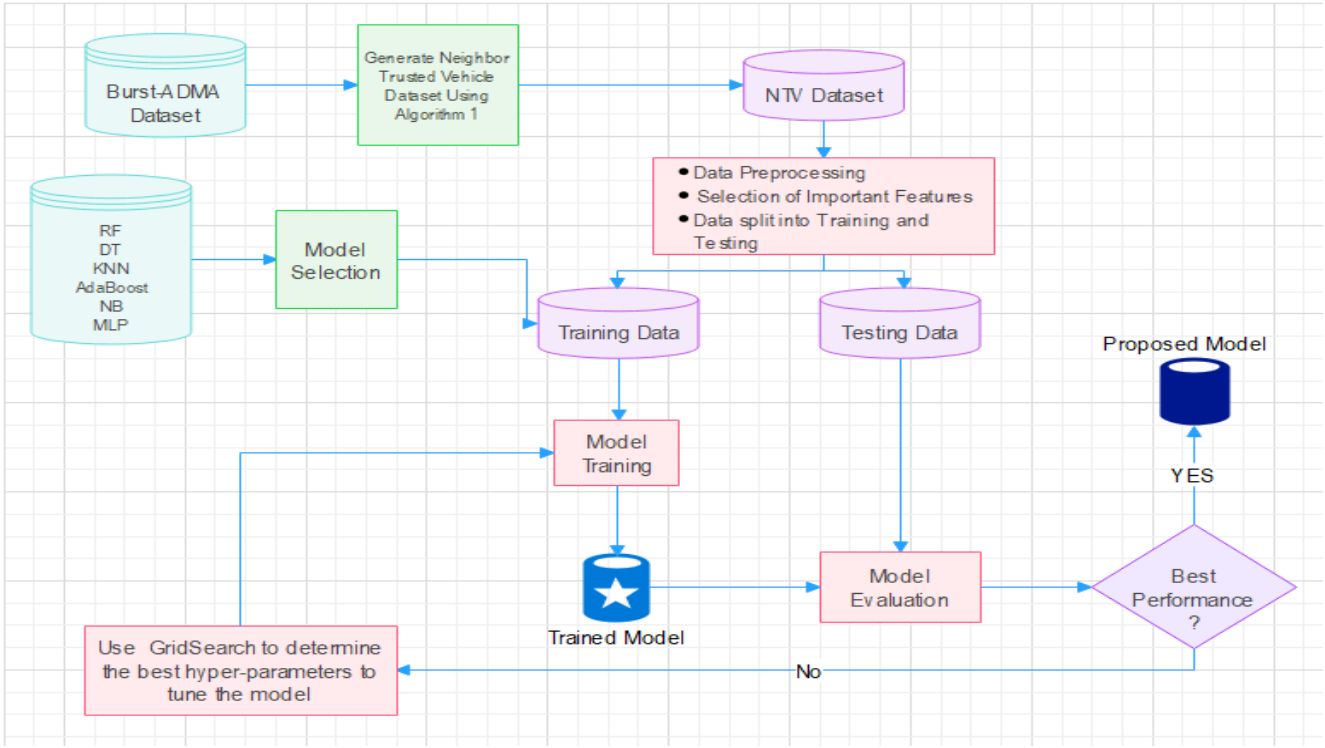

Figure 2. Proposed Approach Workflow

attack type 4 (constant random speed), as depicted in the confusion matrix in 3. However, it misclassifies attack type 3 (negative position offset) as attack type 2 (positive position offset) and attack type 7 (reversed heading) due to certain similarities shared between these attacks. On the other hand, the AdaBoost ensemble classifier exhibits the best performance with an accuracy of 99.98% and impressive precision and recall scores of 99.96% and 99.95%, respectively. This classifier produces the least false negatives and false positives among all the classifiers used in the paper. While attack type 4 is perfectly classified, attack types 2 and 3 are interchangeably misclassified, as shown in the confusion matrix in Figure 4.

The K-Nearest Neighbors (KNN) classifier achieves a decent score with an accuracy of slightly over 98%. However, it struggles with attack type 3 and attack type 7, resulting in a lower accuracy of 95%. Nonetheless, the overall precision, recall, and F1-score of approximately 98% are considered good, as depicted in the confusion matrix in Figure 5. The Decision Tree (DT) classifier demonstrates an accuracy of approximately 99%, which is commendable. However, it misclassifies attack type 7 as attack type 5 (positive speed offset), as observed in Figure 7. The Multilayer Perceptron (MLP) classifier, although expected to outperform all other classifiers, achieves an accuracy of just over 98% and a macro average of 96.75% for precision and recall, as shown in Figure 6. The comparison between all the classifiers in terms of macro average of accuracy, precision, recall, and

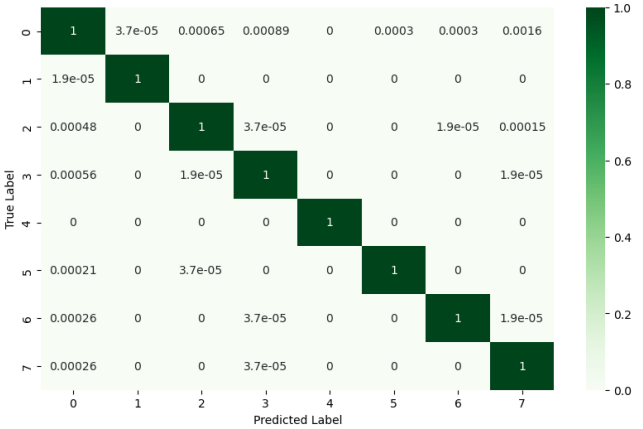

Figure 3. RF Classifier Confusion Matrix Showing Detection of Attack Types

F1-score is depicted in Figure 8 and Table 3.

B. COMPARISON WITH STATE-OF-THE-ART TECHNIQUES

In this subsection, we compared our proposed NIBFADS-UTVA with the state-of-the-art machine learning based MDS techniques available in the literature, particularly misbehavior detection system approaches that used the same dataset for evaluation of their approach for detection of falsified BSM in an IoV network.

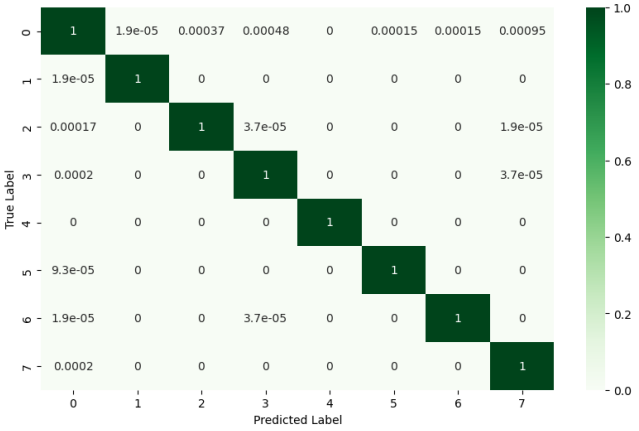

Figure 4. AdaBoost Classifier Confusion Matrix Showing Detection of Attack Types

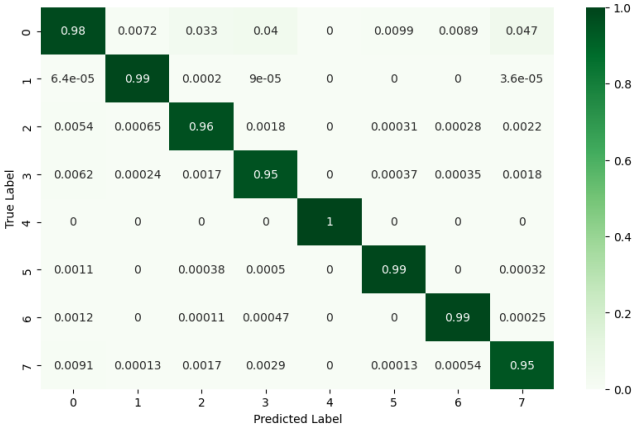

Figure 5. KNN Classifier Confusion Matrix Showing Detection of Attack Types

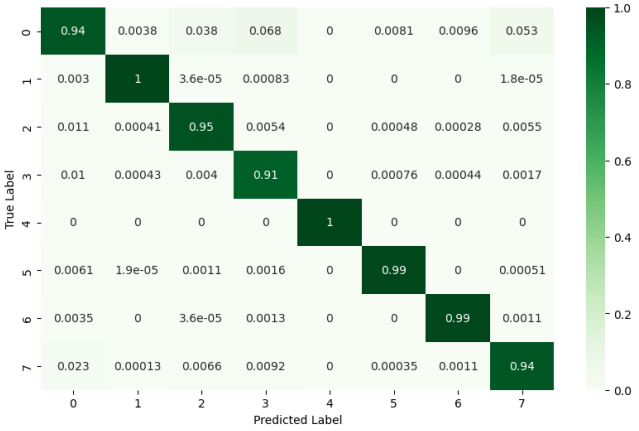

Figure 6. MLP Classifier Confusion Matrix Showing Detection of Attack Types

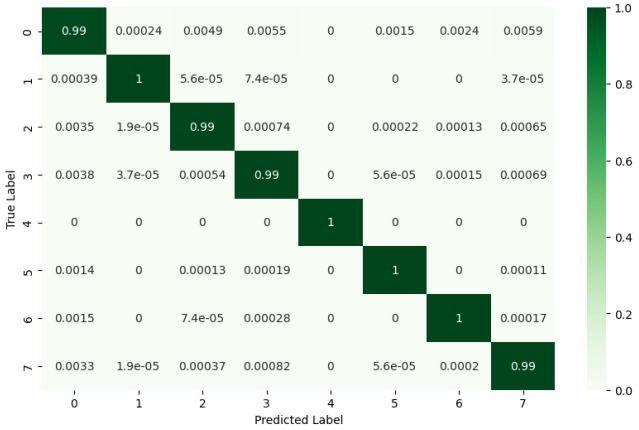

Figure 7. DT Classifier Confusion Matrix Showing Detection of Attack Types

Table 3. Average Performance Comparisons for the Classifiers with and without Trusted Neighbor Vehicle

Approach	ML Classifier	Accuracy	Precision	Recall	F1-Score
Without-Trusted Neighbor	RF	0.97.86	0.9638	0.9136	0.9436
	DT	0.9652	0.9218	0.9203	0.9210
	KNN	0.9512	0.8589	0.7834	0.8147
	AdaBoost	0.9887	0.9787	0.9039	0.9351
	MLP	0.9185	0.9228	0.9236	0.9232
With-Trusted Neighbor	RF	0.9996	0.9993	0.9993	0.9993
	DT	0.9952	0.9952	0.9952	0.9952
	KNN	0.9815	0.9765	0.9792	0.9778
	AdaBoost	0.9998	0.9996	0.9995	0.9995
	MLP	0.9840	0.9676	0.9675	0.9675

We found out that our proposed approach has excelled in all the metrics of accuracy, precision, recall and F1-Score (the best metric is in bold) as illustrated in Table 4. Firstly, we compared our approach with the work of the authors on dataset [27] using their highest performing classifiers (RF, DT, and KNN), and our proposed approach excelled showing that NIBFADS-UTVA is effective in the detection of falsified BSM by insider attackers in an IoV network.

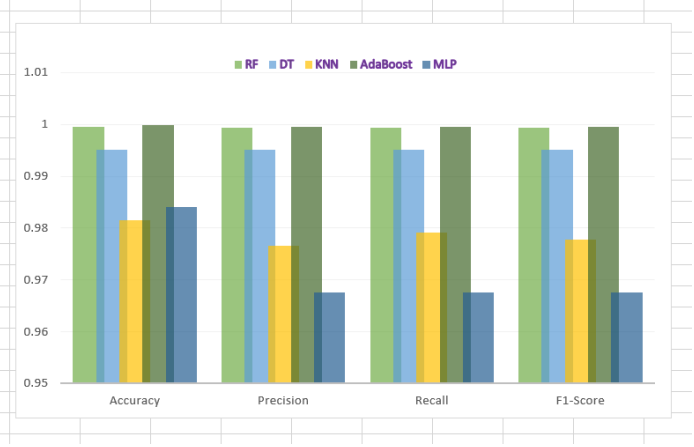

Figure 8. Average Performance Comparison Between the Classifiers

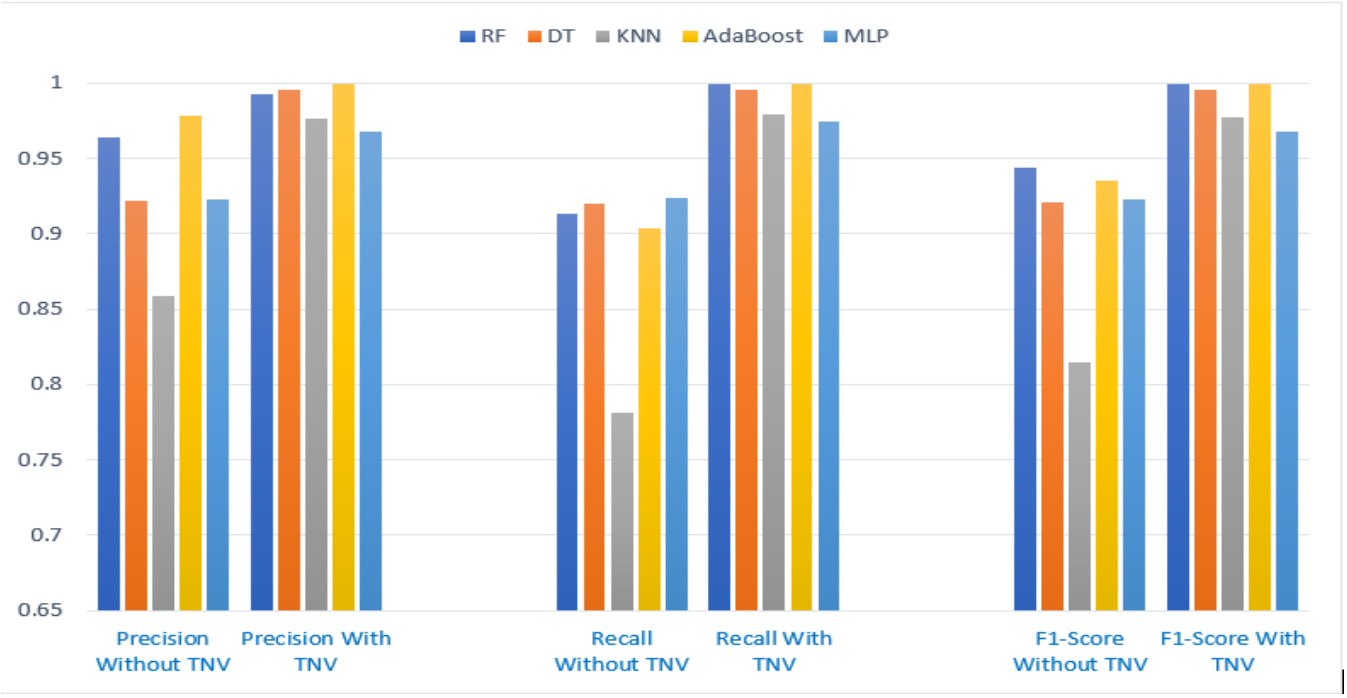

Figure 9. Comparisons Between the Classifiers With and Without Trusted Neighbor Vehicle Approach in Terms of Precision, Recall and F1-Score

Lastly, we compared with the work of [24] where an optimized AdaBoost is used for the same purpose.

Table 4. Performance Comparison with Related Works

Ref	ML Classifier	Accuracy	Precision	Recall	F1-Score
[27]	RF	99.63%	99.88%	97.75%	98.75%
	DT	99.01%	96.63%	96.75%	96.75%
	KNN	98.15%	97.65%	97.92%	97.78%
[24]	AdaBoost	98.9%	NA	NA	NA
Proposed method	RF	99.96%	99.93%	99.93%	99.93%
	DT	99.52%	99.52%	99.52%	99.52%
	KNN	9815%	97.65%	97.92%	97.78%
	AdaBoost	**99.98%**	**99.96%**	**99.95%**	**99.95%**

V. CONCLUSION AND FUTURE WORK

As IoV, a subset of IoT, continues to evolve over recent years, it is faced with security challenges, especially by insider attackers who cannot be detected with cryptographic techniques, prompting a data-centric machine learning intrusion detection system.

In this paper, we have proposed a novel intelligent BSM falsification detection system using a trusted neighbor vehicle approach and showed its effectiveness using accuracy, precision, recall, and F1-score metrics.

In future work, we will augment our novel approach with privacy-preserving techniques such as federated learning or using differential privacy techniques to enhance the privacy of IoV users and prevent our MDS from member inference attacks. As the MLP classifier used in this paper did not perform as expected, we will explore other techniques and algorithms such as recurrent neural networks (RNNs) and convolutional neural networks (CNNs) to capture the spatial-temporal nature of traffic data contained in BSMs.

References

[1] R. S. Rajasekar V., "A study on internet of things devices vulnerabilities using shodan", *International journal of computing*, vol. 22(2), pp. 149–158, 2023. DOI: https://doi.org/10.47839/ijc.22.2.3084.

[2] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions", *Vehicular Communications*, vol. 20, article 100182, 2019. DOI: 10.1016/j.vehcom.2019.100182.

[3] S. A. Elsagheer, K. A. Alshalfan, M. A. Al-hagery, and M. T. Ben Othman, "Safe Driving Distance and Speed for Collision Avoidance in Connected Vehicles", *Sensors*, vol. 22, no. 18, 2022. DOI: 10.3390/s22187051.

[4] Y. L. Morgan, "Notes on DSRC & WAVE standards suite: Its architecture, design, and characteristics", *IEEE Communications Surveys & Tutorials*, vol. 12, no. 4, pp. 504–518, 2010.

[5] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 GHz DSRC-based vehicular safety communication", *IEEE wireless communications*, vol. 13, no. 5, pp. 36–43, 2006.

[6] L. Hobert, A. Festag, I. Llatser, L. Altomare, F. Visintainer, and A. Kovacs, "Enhancements of V2X communication in support of cooperative autonomous driving",

[7] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibanez, "Internet of Vehicles: Architecture, Protocols, and Security", *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3701–3709, 2018. DOI: 10.1109/JIOT.2017.2690902.

[8] S. Chen, J. Hu, Y. Shi, *et al.*, "Vehicle-to-Everything (v2x) Services Supported by LTE-Based Systems and 5G", *IEEE Communications Standards Magazine*, vol. 1, no. 2, pp. 70–76, 2017. DOI: 10.1109/MCOMSTD.2017.1700015.

[9] B. Setiyono, D. R. Sulistyaningrum, D. W. Wicaksono, *et al.*, "Multi vehicle speed detection using euclidean distance based on video processing", *International journal of computing*, vol. 18, no. 4, pp. 431–442, 2019. DOI: https://doi.org/10.47839/ijc.18.4.1613.

[10] S. A. Elsagheer and K. A. AlShalfan, "Intelligent Traffic Management System Based on the Internet of Vehicles (IoV)", *Journal of Advanced Transportation*, vol. 2021, article 4037533, 2021. DOI: 10.1155/2021/4037533.

[11] C. Reshma S, "Optimized Controller Scheme for Autonomous Navigation in Infotainment on Internet-of-Vehicles", *International Journal of Computer Networks and Applications (IJCNA)*, vol. 10(3), pp. 265–276, 2023. DOI: 10.22247/ijcna/2023/221882.

[12] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States", *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[13] B. Brecht and T. Hehn, "A Security Credential Management System for V2X Communications", in *Connected Vehicles: Intelligent Transportation Systems*, R. Miucic, Ed. Springer International Publishing, 2019, pp. 83–115. DOI: 10.1007/978-3-319-94785-3_4.

[14] E. N. ETSI, "302 637-2 v1. 3.1-intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service", *ETSI, Sept*, 2014.

[15] I. Obeidat and M. AlZubi, "Developing a faster pattern matching algorithms for intrusion detection system", *International Journal of Computing*, vol. 18, no. 3, pp. 278–284, 2019.

[16] S. Ercan, M. Ayaida, and N. Messai, "Misbehavior Detection for Position Falsification Attacks in VANETs Using Machine Learning", *IEEE Access*, vol. 10, pp. 1893–1904, 2022. DOI: 10.1109/ACCESS.2021.3136706.

[17] M. Nabil, A. Hajam, O. Boutkhoum, and A. Haqiq, "Game Theory Application for Misbehavior Detection and Prediction in VANET: Review and Challenges", *International Journal of Computer Networks and Applications (IJCNA)*, vol. 10(3), pp. 469–482, 2023. DOI: 10.22247/ijcna/2023/221903.

[18] A. Boualouache and T. Engel, "A Survey on Machine Learning-based Misbehavior Detection Systems for 5G and Beyond Vehicular Networks", *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1128–1172, 2023. DOI: 10.1109/COMST.2023.3236448.

[19] *A Survey on Machine Learning-based Misbehavior Detection Systems for 5G and Beyond Vehicular Networks*, 2022. DOI: 10.1109/OJVT.2021.3138354.

[20] A. Sharma and A. Jaekel, *Machine Learning Based Misbehaviour Detection in VANET Using Consecutive BSM Approach*, 2022. DOI: 10.1109/OJVT.2021.3138354.

[21] R. W. van der Heijden, T. Lukaseder, and F. Kargl, "Veremi: A dataset for comparable evaluation of misbehavior detection in vanets", in *Security and Privacy in Communication Networks: 14th International Conference (SecureComm 2018)*, Springer, Singapore, Aug. 2018, pp. 318–337.

[22] G. O. Anyanwu, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Novel hyper-tuned ensemble Random Forest algorithm for the detection of false basic safety messages in Internet of Vehicles", *ICT Express*, vol. 9, no. 1, pp. 122–129, 2022. DOI: 10.1016/j.icte.2022.06.003.

[23] G. O. Anyanwu, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Falsification detection system for iov using randomized search optimization ensemble algorithm", *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 4, pp. 4158–4172, 2023. DOI: 10.1109/TITS.2022.3233536.

[24] G. O. Anyanwu, C. I. Nwakanma, J.-H. Kim, J.-M. Lee, and D.-S. Kim, "Misbehavior Detection in Connected Vehicles using BurST-ADMA Dataset", in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, 2022, pp. 874–878. DOI: 10.1109/ICTC55196.2022.9952947.

[25] Y. Wu, L. Wu, and H. Cai, "A deep learning approach to secure vehicle to road side unit communications in intelligent transportation system", *Computers and Electrical Engineering*, vol. 105, article 108542, 2023. DOI: 10.1016/j.compeleceng.2022.108542.

[26] M. Alzahrani, M. Y. Idris, F. A. Ghaleb, and R. Budiarto, "An improved robust misbehavior detection scheme for vehicular ad hoc network", *IEEE Access*, vol. 10, pp. 111 241–111 253, 2022. DOI: 10.1109/ACCESS.2022.3214838.

[27] M. A. Amanullah, M. Baruwal Chhetri, S. W. Loke, and R. Doss, "BurST-ADMA: Towards an Australian Dataset for Misbehaviour Detection in the Internet of Vehicles", in *The 20th International Conference on Pervasive Computing and Communications*, Pisa, Italy, Mar. 2022, pp. 624–629. DOI: 10.1109/PerComWorkshops53856.2022.9767505.

[28] P. A. Lopez, M. Behrisch, L. Bieker-Walz, *et al.*, "Microscopic Traffic Simulation using SUMO", vol. 2018-Novem, 2018, pp. 2575–2582. DOI: 10.1109/ITSC.2018.8569938.

[29] C. C. Robusto, "The cosine-haversine formula", *The American Mathematical Monthly*, vol. 64, no. 1, pp. 38–40, 1957.

HUSSAINI ALIYU IDRIS a final year MSc research student at the Department of Computer Science and Engineering, Egypt-Japan University of Science and Technology Alexandria, Egypt.He obtained his bachelor degree in Computer Engineering from Arab Academy for Science, Technology and Maritime Transport Alexandria, Egypt. His research interests include machine learning, intelligent transportation system (ITS), computer vision,natural language processing,Big Data and data science, cyber-security and internet of vehicles.

KAZUNORI UEDA received the M. Eng. and Dr. Eng. degrees in information engineering from the University of Tokyo in 1980 and 1986, respectively. He joined Waseda University, Department of Information and Computer Science in 1993, and has been Professor since 1997 till now and he is a visiting Professor at Egypt-Japan University of Science and Technology (E-JUST) since 2010. His current research interests include design and implementation of programming languages, concurrency and parallelism, high-performance verification, and hybrid systems. His recent project is LMNtal (pronounced ”elemental”), a model of concurrency and a concurrent programming language based on hierarchical graph rewriting, whose implementation has now evolved into a model checker with visualizing tools.

BASSEM MOKHTAR received his PhD in computer engineering from Virgina Tech USA in 2014 and is currently an Assistant professor at United Arab Emirate University. He published many papers in the different research areas including but not limited to network, Vehicular ad-hoc networks (VANETS),intelligent transportation and smart city

SAMIR A. ELSAGHEER MOHAMED received his PhD in computer Networks from Université de Rennes I in 2013 and is currently an Associate professor at the Department of Computer Science and Engineering, Egypt-Japan University of Science and Technology Alexandria, Egypt. He published many papers in the different research areas including but not limited to network, Vehicular ad-hoc networks (VANETS),intelligent transportation, cyber-security, internet of vehicles and smart city.