iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 11 **Issue:** XII **Month of publication:** December 2023

**DOI:** https://doi.org/10.22214/ijraset.2023.57839

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 11 Issue XII Dec 2023- Available at www.ijraset.com*

# Hybrid Features-Based Intrusion Detection for The Internet of Vehicles using Dynamic Adaptation

Geethanjali P[1], Metun[2], Peeyush Kumar Jaiswal[3], Sai Vasanth Kattamuri[4]
[1]*Undergraduate Student Researcher, Bangalore Institute of Technology, Bangalore, India*
[2]*Graduate Student, New York University, New York, USA*
[3]*Ex- Graduate Student, Arizona State University, Arizona, USA*
[4]*Undergraduate Student (CSE), Parul University, Gujarat, India*

***Abstract:*** ***The evolving landscape of the Internet of Vehicles (IoV) has brought to the forefront a discernible array of challenges about network security. In response, this study delves into applying deep learning-based intrusion detection techniques to fortify the IoV against potential network threats. Notably, prevailing approaches often rely on a singular deep learning model for either temporal or spatial feature extraction, with a serial sequence of spatial feature extraction followed by temporal feature extraction. Such methodologies tend to exhibit shortcomings in adequately capturing the Spatiotemporal intricacies inherent in IoV dynamics, thereby adversely impacting intrusion detection efficacy, and contributing to an elevated false-positive rate. To address these challenges, this research proposes an innovative intrusion detection method tailored for the IoV, premised on the parallel analysis of Hybrid features. The methodology commences with the construction of an optimal feature subset based on inter-feature correlations within IoV traffic. Subsequently, a parallelized application of Temporal Convolutional Network (TCN) and Long Short-Term Memory (LSTM) architectures is employed to extract spatio-temporal features from IoV traffic. In acknowledgment of the dynamic nature of IoV environments, a novel Dynamic Adaptation Mechanism is introduced. This mechanism continuously monitors the real-time IoV traffic, detecting feature drifts and triggering adaptations in the spatiotemporal feature extraction process. The adaptation requirements are then seamlessly communicated to the intrusion detection model through a Feedback Loop for Model Updating, ensuring that the model remains adept at discerning emerging network threats. The culmination of this process involves the fusion of parallelly extracted spatiotemporal features, facilitated by the self-attention mechanism. Subsequently, intrusion detection is executed utilizing a Multilayer Perceptron, providing a comprehensive framework that dynamically adapts to the evolving IoV environment. Empirical assessments utilizing the NSL-KDD dataset demonstrate the efficacy of the proposed method, manifesting in a notable 2.05% reduction in the false-positive rate. Additionally, the proposed method surpasses baseline performance metrics, including accuracy and F1 score, thereby affirming its proficiency in enhancing intrusion detection capabilities within the Internet of Vehicles paradigm, especially in the context of the introduced Dynamic Adaptation Mechanism.***

***Keywords: Internet of Vehicles (IoV), Dynamic Adaptation Mechanism, Feedback Loop, Hybrid features, Network security.***

## I. INTRODUCTION

The escalating production of vehicles within the Internet of Vehicles (IoV), coupled with the escalating intricacies of the network environment, has given rise to a notable escalation in security challenges. The emergence of network attacks poses substantial threats to both the data security and communication security domains within the IoV. The compromise of a vehicle's security infrastructure not only exposes the safety and dependability of the vehicle but also carries the potential for dire consequences, including traffic accidents and resultant casualties. In the event of a successful intrusion, malevolent entities can exert remote control over critical vehicular systems, such as brakes, accelerators, steering, and engines. This capability extends to the manipulation or disruption of the vehicle's normal operational functions, thereby posing an imminent risk to road safety and vehicular reliability.

Furthermore, the ramifications extend beyond vehicular operations, encompassing infringements upon user privacy and interests through the illicit acquisition or tampering of the vehicle's data. These multifaceted security challenges underscore the critical need for robust measures within the IoV to mitigate the vulnerabilities inherent in its expanding networked ecosystem. Efforts to fortify data and communication security are imperative to safeguard against the potentially severe consequences arising from malicious exploits in this context.

Intrusion detection methodologies within the Internet of Vehicles (IoV) can be categorized into traditional machine learning and deep learning approaches. Traditional machine learning methods, utilizing decision trees (DTs), and support vector machines (SVM), among others, manually extract features to classify normal and attack sample data. However, these methods exhibit drawbacks, such as low detection performance and extended processing time, particularly when handling extensive and multidimensional intrusion detection data in the IoV. Presently, deep learning represents the predominant approach for IoV intrusion detection, leveraging its capability to mine hidden features from intrusion sample data. Various deep learning models, including convolutional neural network (CNN), autoencoder, recurrent neural network (RNN), long short-term Memory network (LSTM), generative adversarial network, and deep belief network, are employed to implement effective IoV intrusion detection methods [1-6]. While these models have demonstrated commendable intrusion detection performance, a persistent challenge lies in the form of an elevated false-positive rate. This challenge stems from the incomplete extraction of data features within the IoV dataset and a limited consideration of inter-feature correlations. In response to these challenges, researchers propose combining CNN and LSTM [7] to extract spatio-temporal behavioral features from IoV data, aiming to enhance intrusion detection performance and reduce the false-positive rate. However, existing schemes often concatenate these two models without nuanced consideration of their distinct attributes and respective advantages in capturing temporal and spatial features. A more sophisticated approach that acknowledges the divergent characteristics of temporal and spatial features is needed to address the limitations in IoV intrusion detection schemes effectively. Moreover, it is noteworthy that the features extracted by the preceding model can exert an influence on subsequent models. Consequently, any limitations inherent in the preceding model can propagate and impact the overall intrusion detection performance of the composite model.

To tackle the challenges confronted by Intrusion Detection in the Internet of Vehicles (IoV), a novel IoV intrusion detection method is proposed, leveraging parallel analysis of spatio-temporal features. Initially, a correlation-based feature selection method is introduced to identify features highly correlated with behavior categories, culminating in the construction of an optimal feature set and thereby reducing feature dimensionality. Subsequently, Temporal Convolutional Network (TCN) and Long Short-Term Memory (LSTM) architectures are concurrently employed for the parallel extraction of spatial and temporal features. Finally, the extracted spatio-temporal features are fused using the self-attention mechanism and inputted into a Multi-Layer Perceptron (MLP) for intrusion detection.

The primary contributions of this research are enumerated as follows:

*1)* Introduction of a Dynamic Adaptation Mechanism tailored for intrusion detection in the Internet of Vehicles (IoV). The method employs a recursive elimination approach to discern and retain a pertinent feature subset, effectively eliminating redundant features & adding a feedback loop.

*2)* Development of a novel spatio-temporal feature parallel extraction architecture utilizing Temporal Convolutional Network (TCN) and Long Short-Term Memory (LSTM) models. The parallelized design enhances reliability in comparison to conventional serial architectures.

*3)* Proposition of a spatio-temporal feature fusion approach incorporating the self-attention mechanism. This method assigns attention weights to spatio-temporal features, facilitating efficient fusion and significantly augmenting the efficacy of the IoV intrusion detection model.

*4)* Execution of experimental evaluations on an intrusion detection dataset, demonstrating superior accuracy and F1 score, coupled with a reduced false-positive rate when compared to existing methods.

## II. RELATED WORK

In the realm of the Internet of Vehicles (IoV), intrusion data encompasses numerous spatio-temporal features that potentially reflect distinctive characteristics of attackers. Consequently, researchers have turned to leveraging deep learning methods, such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM), to extract and process these intricate spatio-temporal features. For instance, Hu et al. [8] devised an intrusion detection technique employing CNN with a split convolution module, enhancing spatial characteristic diversity and mitigating the impact of information redundancy across channels on the model. Park et al. [9] transformed network traffic into a grayscale image, constructed a Siamese CNN based on small sample learning, and determined attack types through similarity scores of attack samples. To capture time-dependent dynamic features in network traffic, Zhou et al. [10] proposed an incremental LSTM network intrusion detection method, introducing state changes into LSTM to process network data by acquiring dynamic information from the hidden layers. Combining LSTM and autoencoder, Ashraf et al. [11] extracted timing features from IoV network traffic, thereby improving intrusion detection accuracy. However, these approaches typically employ either CNN or LSTM in isolation, leading to potential limitations in feature extraction.

In response, some researchers advocate for a hybrid model integrating both CNN and LSTM for enhanced spatio-temporal feature extraction. Wang et al. [12] proposed a hierarchical intrusion detection system based on spatio-temporal features. They initially utilized CNN to discern spatial features in network traffic packets, followed by LSTM to capture temporal features between multiple network traffic packets, ultimately yielding a more accurate spatio-temporal feature vector. Notably, these solutions overlook the issue of variable time intervals between data packets in the flow. Addressing this concern, Han et al. [13] introduced a spatially and temporally aware intrusion detection model, devising a time- and length-sensitive LSTM method to capture a broader range of temporal characteristics from intermittent streams.

Deep learning, with its capacity to discern intrinsic patterns within sample data, proves effective in adapting to higher-dimensional learning and prediction requirements. Constructing a nonlinear network structure comprising multiple hidden layers enables its proficiency. Researchers [14–16] have applied deep learning methods and edge computing technologies to analyze the traffic and speed of vehicles in the Internet of Vehicles (IoV), providing personalized safety information for drivers and establishing a foundational dataset for IoV intrusion detection. Acknowledging the potential improvement in intrusion detection performance, deep learning methods are extensively utilized in IoV intrusion detection [17–19]. Yang et al. [20] introduced an intrusion detection method for in-vehicle networks based on federated deep learning, leveraging network message periodicity, employing the ConvLSTM model for intrusion detection, and training the model through federated deep learning. Li et al. [21] proposed an IoV intrusion detection scheme based on transfer learning, utilizing both cloud-assisted and local update modes. Shone et al. [22] devised an unsupervised deep learning intrusion detection technology utilizing an asymmetric deep autoencoder to construct a classification model. However, this approach requires enhanced classification performance in unbalanced samples. Xu et al. [23] designed a Log-Cosh variational autoencoder method, incorporating a logarithmic hyperbolic chordal function to enhance detection accuracy by generating diverse intrusion data. Despite these advancements, existing deep learning-based solutions still grapple with a high false-positive rate, attributed to the insufficient extraction of relevant features in the IoV context.

Commonly, contemporary intrusion detection methods that rely on spatio-temporal features often employ deep learning techniques such as Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) to establish sequential intrusion detection models. However, the collective performance of these methods is susceptible to the influence of the preceding model and tends to overlook the comprehensive nature of spatio-temporal features. The extraction of spatial-temporal features necessitates a more holistic approach. Consequently, to mitigate the adverse impact of a singular model in sequential feature extraction and fully leverage the advantages of spatio-temporal features, we advocate the parallel extraction of such features. This parallelized approach enhances the effectiveness of intrusion detection in the Internet of Vehicles (IoV) and concurrently diminishes the incidence of false positives.

## III. RESEARCH METHODOLOGY

Figure 1 illustrates the comprehensive architecture of our proposed method, the Parallel Analysis of Spatio-Temporal Features (PA-STF). The method is delineated into three key components. In the initial segment, IoV traffic is preprocessed to derive the original characteristics of network traffic. Subsequently, feature selection is executed based on the correlation method to discern the optimal feature subset. The second segment involves the simultaneous utilization of the Temporal Convolutional Network (TCN) and Long Short-Term Memory (LSTM) to extract spatio-temporal characteristics from the preprocessed data. The third segment employs the self-attention mechanism to assess the relative importance of spatio-temporal information. The amalgamated features are then inputted into a multilayer perceptron to determine whether the detected traffic is normal or subjected to an attack.

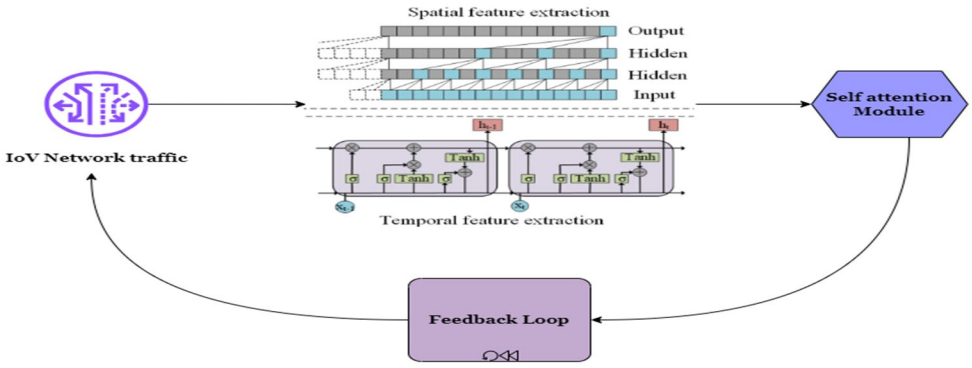



Figure 1. Proposed Architecture of Hybrid Features Method.

In the communication traffic within the Internet of Vehicles (IoV), the extraction of intrusion data features typically relies on fundamental features, content features, and statistical features derived from network traffic. Notably, features of the same type often exhibit discernible aggregation patterns, thereby manifesting specific spatial characteristics. Temporal Convolutional Network (TCN) is adept at local spatial feature extraction through its receptive field, making it well-suited for processing and extracting spatial features from IoV traffic. Furthermore, IoV traffic, being a form of time series data, inherently possesses temporal dependencies that can significantly contribute to intrusion detection. Long Short-Term Memory (LSTM), renowned for its proficiency in handling time data, is particularly suited for extracting temporal features from IoV traffic. The extraction of spatio-temporal features enables the identification of deep-level behavioral patterns within IoV traffic, thereby holding considerable significance for the efficacy of intrusion detection in the IoV context.

### *A. TCN-based Spatial Feature Extraction*

Traditional methods for spatial feature extraction commonly employ Convolutional Neural Network (CNN) models, which mimic the structure of biological neural networks and consist of convolutional layers, pooling layers, and fully connected layers. The performance of the model in fitting data is enhanced by stacking multiple network layers, leading to successful applications in speech and image recognition. However, an excessive number of layers can result in an abundance of model parameters, making the model prone to overfitting. This not only prolongs model training time but is also impractical for the Internet of Vehicles (IoV) environment. Temporal Convolutional Network (TCN) presents a novel CNN structure designed to process sequence data by incorporating causal convolution. The introduced expanded convolution and residual modules endow TCN with the ability to memorize historical information. In contrast to traditional CNNs, which require the preprocessing of network traffic data into two-dimensional images for spatial feature extraction, TCN can directly extract spatial features from one-dimensional data. This approach offers advantages such as reduced computing resource requirements and stable gradients. Hence, the proposed method utilizes TCN for spatial feature extraction in IoV traffic. The specific process is outlined as follows. The TCN model employs a one-dimensional fully convolutional network to extract spatial features from the data. In the TCN model, a causal convolution structure is utilized, enabling the modeling of sequence data by ensuring that the output of the current layer depends solely on the convolution of the previous layer and the previous t time. This causal convolution operation in TCN can be represented by the following formula:

$$F * X(xt) = \sum_{n=0}^{N} f_n \cdot x_t + n - N$$

where F represents the filter set, $F = \{f1, f2, \ldots, fN\}$, $f$ is the individual filter, and N is the number of filters; $X$ is the input sequence, $X = \{x1, x2, \ldots, xT\}$, where $x$ is the input item, and $T$ is the size of the input sequence; and $*$ is the convolution operation, and $n$ is the size of the convolution kernel. When the scale of input data continues to expand, the number of convolutional network layers also increases, which gives rise to several problems such as complex training and gradient disappearance. To this end, the TCN model introduces the concept of dilated convolution, which stipulates that the convolution input must be sampled at intervals so that the effective window size increases exponentially with the increase in the number of network layers; thus, only a few convolution layers are needed to obtain a larger receptive field. The expansion convolution operation on the t-th element in the input sequence can be expressed by the following formula:

$$F(t) = \sum_{i=0}^{k-1} f(i) \cdot x_{t-d.i}$$

Among these, k is the size of the filter, $i$ is the current filter size, $xt$ is the t-th element of the input sequence, f is the convolution operation, d is the defined expansion factor used to control the sampling rate when $d = 1$ is a conventional convolution operation, and $t - d \cdot i$ represents the past direction. The IoV traffic data are input into the TCN module, and the spatial feature vector of the IoV data can be extracted. Compared with traditional CNN, TCN has a flexible receptive field and stable gradient, which can enhance the feature extraction ability. The extracted features can train a higher-performance intrusion detection model.

### *B. LSTM-based Temporal Feature Extraction*

For temporal feature extraction, Recurrent Neural Networks (RNN) are commonly employed due to their ability to handle sequence data with evolving characteristics, distinguishing them from general neural networks. As an enhanced iteration of RNN, Long Short-Term Memory (LSTM) effectively addresses the long-term dependency challenge inherent in prolonged sequence training [28],

earning widespread adoption by researchers. Consequently, LSTM is utilized in our methodology to extract temporal features from Internet of Vehicles (IoV) data.

The forget gate is mainly used to control whether the unit discards the unit state of the previous layer, which the following formula can express:

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f)$$

where $\sigma$ is the sigmoid activation function, $t$ is the current moment, $f$ is the forget gate, $xt$ is an element in the input sequence, $ht-1$ is the state of the preceding sequence, $Wf$ is the weight, and bf is the bias. The forget gate outputs a vector ranging from 0 to 1, which is used to control the information of the units in the previous layer: 0 is no reservation, while 1 is all reservations.

### *C. Spatio-Temporal Feature Fusion and Intrusion Detection*

Following the parallel extraction of spatio-temporal features in Internet of Vehicles data using TCN and LSTM, the subsequent step involves inputting these features into a Multilayer Perceptron (MLP) for intrusion detection model training. However, given the distinct emphasis of spatio-temporal features, not all features hold equal importance in distinguishing various attack types. Take, for instance, the features of synack, ackdat, and tcprtt in the Internet of Vehicles traffic, all of which reflect the time-dependent state characteristic of TCP connections and exhibit a significant correlation in detecting time-sensitive attacks. Enhancing the detection performance of such attacks is achievable by elevating the weight of their pertinent features.

To address this, the self-attention mechanism is leveraged to discern the importance of different features. This entails compressing various components into a unified representation by assigning attention weights to spatio-temporal features. The self-attention mechanism dynamically adjusts these features based on the semantic and scale information of different spatio-temporal feature weights, thereby achieving spatio-temporal feature fusion. By doing so, the self-attention mechanism ensures that the fused spatio-temporal features suppress extraneous information, resulting in a more robust representation for both normal and attack traffic.

Through the softmax operation of the inner product of $q$ and each $ki$, the similarity between q and each vi is obtained, where $\sqrt{dk}$ is a scaling factor to prevent the gradient of the softmax function from disappearing, n is the number of key-value pairs, ki is the i-th key, and $vi$ is the i-th value. Through the self-attention module, we can assign attention scores to spatio-temporal features and fuse the features extracted with the TCN and LSTM models according to the attention scores. The feature fusion method can be expressed by the following formula:

$$F_{fusion} = \lambda_{TCN} F_{spatial} + \lambda_{LSTM} F_{temporal}$$

where $Ff$ fusion is the fused feature; $Fspatial$ and $Ftemporal$ are the spatial features and temporal features extracted by the TCN model and the LSTM model, respectively; and $\lambda TCN$ and $\lambda LSTM$ are their respective weights. Fusion weights are normalized using the softmax method. The feature fusion method based on the self-attention mechanism adds weight constraints to the extracted spatiotemporal features of the IoV communication traffic. This method can obtain information more conducive to intrusion detection and classification. Based on the features obtained by the above spatio-temporal feature fusion process, we input them into a multilayer perceptron neural network to complete the classification task of intrusion detection in the IoV. We use the cross-entropy loss function as the loss function of the multilayer perceptron. The fusion of spatio-temporal features makes the model complex and can easily cause over-fitting. Therefore, we add an L2 regularization term to the loss function to reduce over-fitting. The degree of integration reduces the complexity of the model. The loss function is defined as follows:

$$L = \frac{1}{N}\sum_{i} L_i + \eta\|\omega\|^2 = -\frac{1}{N}\sum_{i}\sum_{c=1}^{M} y_{ic}\log(p_{ic}) + \eta\|\omega\|^2$$

Here, $M$ is the number of categories, $yic$ is a sign function, $y$ is the predicted probability distribution, $p$ is the real probability distribution, $i$ is the index of the sample, $c$ is the index of the category, and $N$ is the total number of samples. When the real category of sample $i$ is equal to $c$, it takes 1; otherwise, it takes 0. Furthermore, pic is the predicted probability that sample $i$ belongs to category $c$, ω is the model parameter, and $\eta$ is the penalty item. Through continuous training iterations, the loss function of the model is converged to obtain the optimal intrusion detection model.

## IV. RESULTS & DISCUSSION

The proposed method was implemented using Python language, the Numpy library to preprocess the data set, and Scikit-learn and Tensorflow to realize the spatio-temporal feature extraction and intrusion detection classification model based on deep learning. The main parameter settings of the model are shown in Table 1.

Table 1. Main parameters of the model.

| Parameter | Value | Description |
|---|---|---|
| Learning-rate | 0.01 | Gradient descent steps during model training |
| Epoch | 50 | Number of training rounds |
| Dropout | 0.2 | Dropout rate of neural network unit |
| MLP-layer | 4 | Number of layers of the MLP model |
| LSTM-Unit | 48 | Number of LSTM model units |
| TCN-layer | 4 | Number of layers of the TCN model |

Accuracy, FPR, and F1 score is used to evaluate the performance of the proposed intrusion detection method. Among these, accuracy is the proportion of the correctly classified samples to all samples, FPR is negative samples predicted as the proportion of positive samples to the total negative samples, and F1 score is the harmonic mean of precision and recall.

$$FPR = \frac{FP}{FP + TN}$$

$$F1 = \frac{2TP}{2TP + FP + TN}$$

*A. Performance Comparison*

The methods employed in the comparative analysis are as follows: SVM [24], utilizing support vector machines, a traditional machine learning approach, to categorize packets into trusted or malicious categories; CNN [25], relying solely on convolutional neural networks for spatial feature extraction, utilizing a loss function and tailored error metrics designed around the spatial characteristics of link load for intrusion detection; LSTM [26], exclusively utilizing long short-term memory networks for training to capture temporal changes in traffic data for intrusion detection; and CNN-BiSRU [27], employing two sequential deep learning models, with the first being a convolutional neural network for spatial feature extraction from the original data and the second being a bidirectional simple recurrent unit for subsequent temporal feature extraction. The classification results are then output through softmax to accomplish intrusion detection.

Table 2. Performance comparison of the different methods on the NSL-KDD dataset.

| Methods | Accuracy | FPR | F1 Score |
|---|---|---|---|
| SVM | 89.64 | 5.64 | 5.64 |
| CNN | 93.17 | 4.38 | 92.69 |
| LSTM | 92.77 | 5.34 | 92.83 |
| CNN-BiSRU | 95.34 | 2.16 | 96.21 |
| Hybrid features | 98.88 | 0.31 | 98.97 |

Table 2 presents a performance comparison of each method in terms of intrusion detection on the NSL-KDD dataset. The proposed hybrid feature method exhibits optimal results, outperforming other schemes in Accuracy, F1 score, and False Positive Rate (FPR). Specifically, the hybrid feature method attains an accuracy of 98.88%, surpassing the next best method by 3.38%. Additionally, the F1 score of the hybrid feature method reaches 98.97%, exceeding the next best method by 2.76%. Notably, the false-positive rate of the proposed hybrid feature method on the NSL-KDD dataset is only 0.31%, remaining exceptionally low and 2.05% lower than the next least performing method.

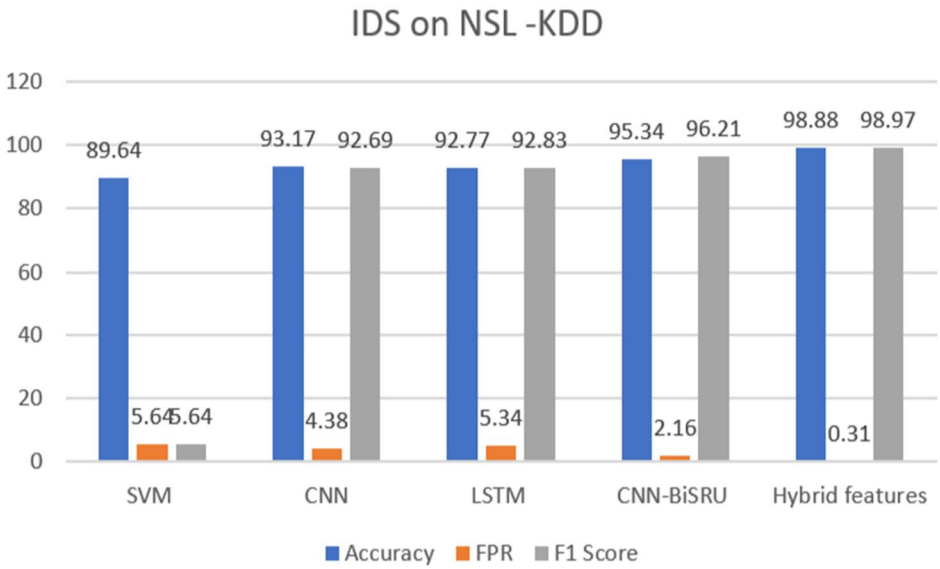



Figure 2. Performance comparison of each method under different attack type.

Fig. 2 depicts Accuracy, FPR, F1 Score of SVM, CNN, LSTM, CNN-BiSRU, and Hybrid Features(spatial-temporal). The proposed hybrid feature method demonstrates superior performance in comparison to alternative approaches, showcasing notable achievements in Accuracy, F1 score, and False Positive Rate (FPR). Specifically, the hybrid feature method attains an accuracy of 98.88%, representing a significant improvement of 3.38% over the subsequent best-performing method. Furthermore, the F1 score achieved by the hybrid feature method stands at 98.97%, surpassing the next best method by 2.76%. Remarkably, the false-positive rate associated with the proposed hybrid feature method on the NSL-KDD dataset is merely 0.31%, underscoring its exceptional efficacy and marking a substantial 2.05% reduction compared to the next least performing method.

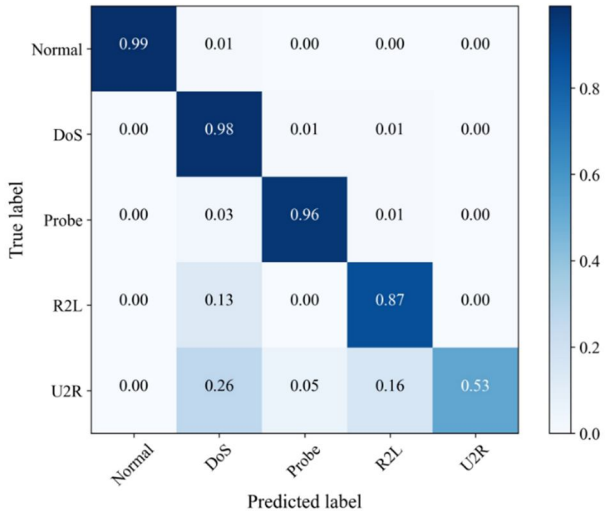



Figure 3. Confusion matrix of the Hybrid feature method on NSL-KDD dataset.

Figure 3 is the confusion matrix obtained using the proposed method on the NSL-KDD dataset. The proposed method achieved a correct recognition rate of 99% for normal samples in the NSL-KDD dataset. Moreover, 98% of DoS attacks could be detected correctly, and 96% of Probe attacks could be detected correctly. Due to the small sample size of R2L and U2R, the detection rate was low. However, the proposed method had a very low probability of misidentifying the four attack types as normal, making the false-positive rate of the proposed method very low, which proves the effectiveness of the proposed method.

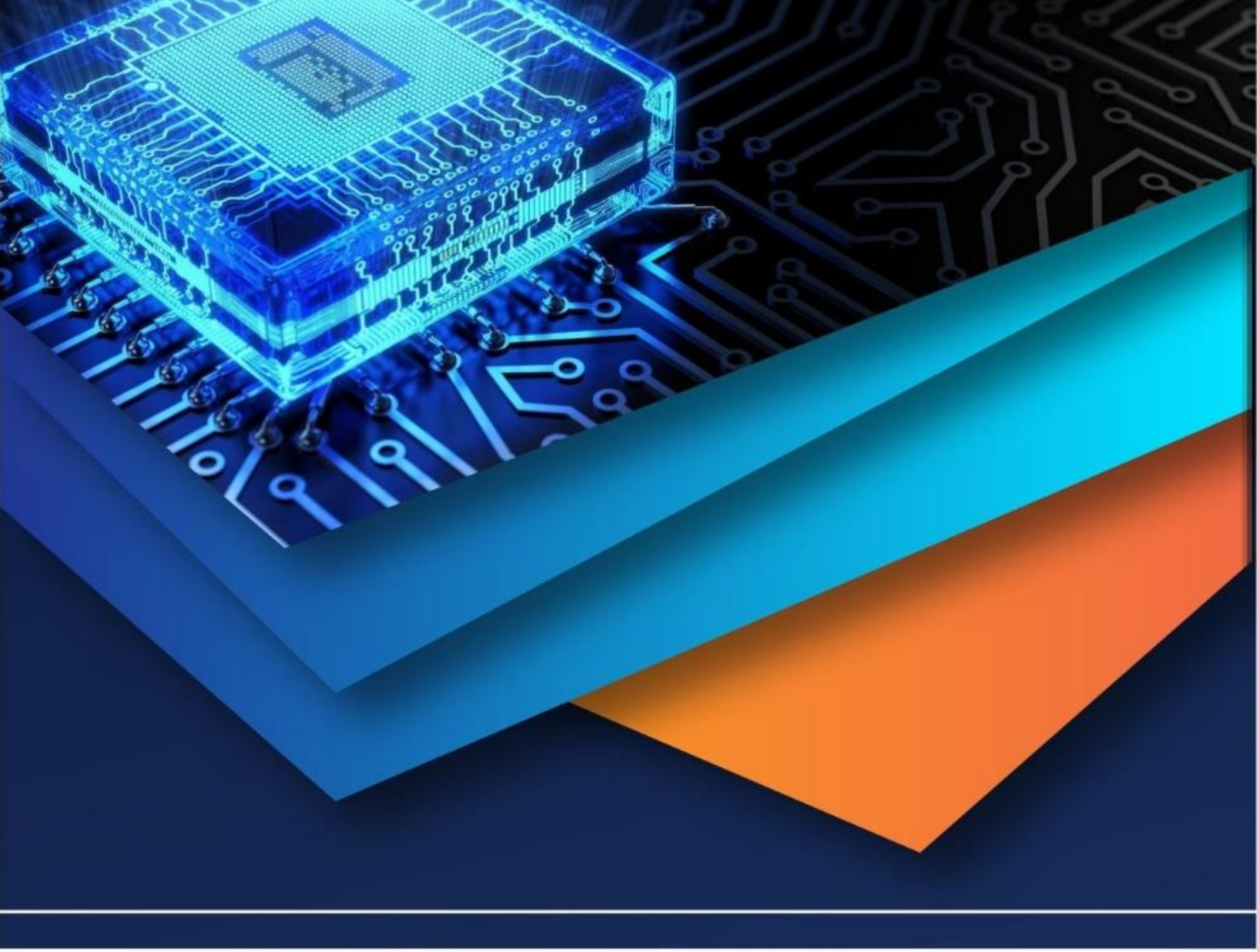
## V. CONCLUSION

This paper introduces an intrusion detection method for the Internet of Vehicles (IoV) based on the parallel analysis of spatio-temporal features, incorporating dynamic adaptation mechanisms and a feedback loop for model updating. The approach involves the extraction of spatio-temporal features from intricate and multidimensional IoV traffic using Temporal Convolutional Network (TCN) and Long Short-Term Memory (LSTM) architectures in parallel. In contrast to prior methods that rely on a single deep learning model or employ serial feature extraction methods, the proposed approach ensures a more comprehensive extraction of spatio-temporal features, leading to enhanced IoV intrusion detection performance and a reduction in false positives. Initially, feature selection is conducted based on the feature correlation present in IoV traffic to identify the optimal feature subset. Subsequently, instead of utilizing a single model or sequentially extracting spatio-temporal features through methods like Convolutional Neural Network (CNN) or LSTM, the methodology employs TCN and LSTM simultaneously for parallel extraction of spatio-temporal features in IoV traffic. To address the evolving landscape of IoV and its security challenges, a dynamic adaptation mechanism is introduced, enabling the model to adapt to changing conditions in the network environment. Furthermore, a feedback loop for model updating is incorporated, ensuring that the intrusion detection model remains adaptive and effective over time. The self-attention mechanism is utilized to fuse the extracted spatio-temporal features, employing a multilayer perceptron network for intrusion detection. Experimental evaluations conducted on the NSL-KDD dataset demonstrate that the method achieves superior intrusion detection results in a more efficient timeframe compared to previous approaches, affirming the efficacy of the proposed methodology. The introduction of dynamic adaptation mechanisms and feedback looping enhances the model's ability to adapt to changing IoV conditions and further bolsters its overall performance. Despite the positive outcomes, the escalating number of vehicles in the IoV and the growing complexity of network environments necessitate a focus on enhancing intrusion detection response speed. Future research endeavors will explore the integration of edge intelligence into IoV intrusion detection to address this requirement. Additionally, the incorporation of novel feature extraction techniques, encompassing behavioral and contextual features alongside existing spatio-temporal features, will be investigated to bolster the overall performance and robustness of IoV intrusion detection.

## REFERENCES

[1] Xiao, Y.; Xing, C.; Zhang, T.; Zhao, Z. An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks. IEEE Access 2019, 7, 42210–42219.
[2] Abdel-Basset, M.; Moustafa, N.; Hawash, H.; Razzak, I.; Sallam, K.M.; Elkomy, O.M. Federated Intrusion Detection in Blockchain-Based Smart Transportation Systems. IEEE Trans. Intell. Transp. Syst. 2022, 23, 2523–2537.
[3] Anzer, A.; Elhadef, M. Deep Learning-Based Intrusion Detection Systems for Intelligent Vehicular Ad Hoc Networks. In Lecture Notes in Electrical Engineering,Proceedings of the Advanced Multimedia and Ubiquitous Engineering—MUE/FutureTech 2018, Salerno, Italy, 23–25 April 2018; Park, J.J., Loia, V., Choo, K.R., Yi, G., Eds.; Springer: Berlin/Heidelberg, Germany, 2018; Volume 518, pp. 109–116.
[4] Zekry, A.; Sayed, A.; Moussa, M.; Elhabiby, M. Anomaly Detection using IoT Sensor-Assisted ConvLSTM Models for Connected Vehicles. In Proceedings of the 93rd IEEE Vehicular Technology Conference, VTC Spring 2021, Helsinki, Finland, 25–28 April 2021; pp. 1–6.
[5] Shu, J.; Zhou, L.; Zhang, W.; Du, X.; Guizani, M. Collaborative Intrusion Detection for VANETs: A Deep Learning-Based Distributed SDN Approach. IEEE Trans. Intell. Transp. Syst. 2021, 22, 4519–4530.
[6] Tan, Q.S.; Huang, W.; Li, Q. An intrusion detection method based on DBN in ad hoc networks. In Wireless Communication and Sensor Network: Proceedings of the International Conference on Wireless Communication and Sensor Network (WCSN 2015); World Scientific: Singapore, 2016; pp. 477–485.
[7] Lo, W.; AlQahtani, H.; Thakur, K.; Almadhor, A.; Chander, S.; Kumar, G. A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic. Veh. Commun. 2022, 35, 100471.
[8] Hu, Z.; Wang, L.; Qi, L.; Li, Y.; Yang, W. A novel wireless network intrusion detection method based on adaptive synthetic sampling and an improved convolutional neural network. IEEE Access 2020, 8, 195741–195751.
[9] Park, D.; Kim, S.; Kwon, H.; Shin, D.; Shin, D. Host-Based Intrusion Detection Model Using Siamese Network. IEEE Access 2021, 9, 76614–76623.
[10] Zhou, H.; Kang, L.; Pan, H.; Guo, W.; Feng, Y. An intrusion detection approach based on incremental long short-term memory. Int. J. Inf. Sec. 2023, 22, 433–446.
[11] Ashraf, J.; Bakhshi, A.D.; Moustafa, N.; Khurshid, H.; Javed, A.; Beheshti, A. Novel Deep Learning-Enabled LSTM Autoencoder Architecture for Discovering Anomalous Events from Intelligent Transportation Systems. IEEE Trans. Intell. Transp. Syst. 2021, 22, 4507–4518.
[12] Wang, W.; Sheng, Y.; Wang, J.; Zeng, X.; Ye, X.; Huang, Y.; Zhu, M. HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection. IEEE Access 2018, 6, 1792–1806.
[13] Han, X.; Yin, R.; Lu, Z.; Jiang, B.; Liu, Y.; Liu, S.; Wang, C.; Li, N. STIDM: A Spatial and Temporal Aware Intrusion Detection Model. In Proceedings of the 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020, Guangzhou, China, 29 December 2020–1 January 2021; pp. 370–377.
[14] Spandonidis, C.C.; Fotis, G.; Sedikos, E.; Dimitris, R.; Theodoropoulos, P. Development of a MEMS-Based IoV System for Augmenting Road Traffic Survey. IEEE Trans. Instrum. Meas. 2022, 71, 1–8.
[15] Busacca, F.; Grasso, C.; Palazzo, S.; Schembra, G. A Smart Road Side Unit in a Microeolic Box to Provide Edge Computing for Vehicular Applications. IEEE Trans. Green Commun. Netw. 2023, 7, 194–210.

[16] Wan, S.; Ding, S.; Chen, C. Edge computing enabled video segmentation for real-time traffic monitoring in internet of vehicles. Pattern Recognit. 2022, 121, 108146.
[17] Loukas, G.; Vuong, T.; Heartfield, R.; Sakellari, G.; Yoon, Y.; Gan, D. Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning. IEEE Access 2018, 6, 3491–3508.
[18] Gui, G.; Liu, M.; Tang, F.; Kato, N.; Adachi, F. 6G: Opening New Horizons for Integration of Comfort, Security, and Intelligence. IEEE Wirel. Commun. 2020, 27, 126–132.
[19] Alladi, T.; Agrawal, A.; Gera, B.; Chamola, V.; Sikdar, B.; Guizani, M. Deep Neural Networks for Securing IoT Enabled Vehicular Ad-Hoc Networks. In Proceedings of the ICC 2021—IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
[20] Yang, J.; Hu, J.; Yu, T. Federated AI-Enabled In-Vehicle Network Intrusion Detection for Internet of Vehicles. Electronics 2022, 11, 3658.
[21] Li, X.; Hu, Z.; Xu, M.; Wang, Y.; Ma, J. Transfer learning-based intrusion detection scheme for Internet of vehicles. Inf. Sci. 2021, 547, 119–135.
[22] Shone, N.; Tran, N.N.; Phai, V.D.; Shi, Q. A Deep Learning Approach to Network Intrusion Detection. IEEE Trans. Emerg. Top. Comput. Intell. 2018, 2, 41–50.
[23] Xu, X.; Li, J.; Yang, Y.; Shen, F. Toward Effective Intrusion Detection Using Log-Cosh Conditional Variational Autoencoder. IEEE Internet Things J. 2021, 8, 6187–6196.
[24] Cabelin, J.D.; Alpaño, P.V.; Pedrasa, J.R. SVM-based Detection of False Data Injection in Intelligent Transportation System. In Proceedings of the International Conference on Information Networking, ICOIN 2021, Jeju Island, Republic of Korea, 13–16 January 2021; pp. 279–284.
[25] Nie, L.; Ning, Z.; Wang, X.; Hu, X.; Cheng, J.; Li, Y. Data-Driven Intrusion Detection for Intelligent Internet of Vehicles: A Deep Convolutional Neural Network-Based Method. IEEE Trans. Netw. Sci. Eng. 2020, 7, 2219–2230.
[26] Zhang, Y.Y.; Shang, J.; Chen, X.; Liang, K. A self-learning detection method of Sybil attack based on LSTM for electric vehicles. Energies 2020, 13, 1382.
[27] Ding, S.; Wang, Y.; Kou, L. Network intrusion detection based on BiSRU and CNN. In Proceedings of the IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems, MASS 2021, Denver, CO, USA, 4–7 October 2021; pp. 145–147.
[28] Sun, H.; Chen, M.; Weng, J.; Liu, Z.; Geng, G. Anomaly Detection for In-Vehicle Network Using CNN-LSTM with Attention Mechanism. IEEE Trans. Veh. Technol. 2021, 70, 10880–10893.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY