Journal of Autonomous Intelligence (2024) Volume 7 Issue 4
doi: 10.32629/jai.v7i4.1220

ORIGINAL RESEARCH ARTICLE

Using deep learning to address the security issue in intelligent transportation systems

Raja Sarath Kumar Boddu[1], Radha Raman Chandan[2], M. Thamizharasi[3], Riyaj Shaikh[4], Adheer A. Goyal[5], Pragya Prashant Gupta[6], Shashi Kant Gupta[7,*]

[1] *Computer Science Engineering, Lenora College of Engineering, Rampachodavaram 533288, Andhra Pradesh, India*

[2] *Department of Computer Science, School of Management Sciences (SMS), Varanasi 221011, India*

[3] *Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai 600089, Tamil Nadu, India*

[4] *Department of Analytics, Vodafone, Pune 411014, India*

[5] *Department of Commerce & Management, G H Raisoni University, Saikheda, Chhindwara 480106 (MP), India*

[6] *School of Management, BBD University, Lucknow, Uttar Pradesh 226028, India*

[7] *Post-Doctoral Fellow, CSE, Eudoxia Research University, New Castle 19702, USA*

*** Corresponding author:** Shashi Kant Gupta, raj2008enator@gmail.com

ABSTRACT

The lives of people are at risk from security and safety risks with Intelligent Transportation Systems (ITS), particularly Autonomous Vehicles. In contrast to manual vehicles, the Security of an AV's computer and communications components may be penetrated using sophisticated hacking methods, preventing us from employing AVs in our daily lives. The Internet of Vehicles, which connects manual automobiles to the Internet, is vulnerable to cyber-attacks such as lack of service, spoofing, sniffer, widespread denial of service and repeat attacks. This paper presents a unique intrusion detection system for ITS, using Enhanced Cuttle Fish Optimized Multiscale Convolution Neural Network (ECFO-MCNN), that uses vehicles to identify networks and infrastructure and detects careful network activity of in-vehicle networks. The primary goal of the suggested strategy is to identify forward events emanating through AVs' central network gateways. Two benchmark datasets, namely the UNSWNB15 dataset for external network communications and the car hacking dataset for in-vehicle communications, are used to assess the proposed IDS. The evaluation's findings showed that the performance of our suggested system is superior to that of traditional intrusion detection methods.

Keywords: intelligent transport systems; CAN bus; deep learning; enhanced cuttlefish optimized Multiscale convolution neural network; autonomous vehicles; intrusion detection system

ARTICLE INFO

Received: 6 September 2023
Accepted: 27 November 2023
Available online: 1 March 2024

1. Introduction

The ITS completely transforms travel and communication with transportation systems. The ITS is improved travel's effectiveness, safety, and, sustainability by seamlessly integrating cutting-edge technology. Through real-time data collection, processing, and transmission, ITS allows transportation systems to make informed decisions and respond rapidly to changing situations. ITS combines smart infrastructure, vehicle connection, and intelligent applications to establish a seamless and integrated transportation environment, improving public transit operations, streamlining traffic flow, and decreasing congestion[1]. A small group of transportation experts developed the concept of ITS, initially known as intelligent vehicle-highway systems, in the 1980s to acknowledge the influence of

computers and communications in transportation. The ITS has had a significant impact on the world during the last ten years, and its applications go past only highway traffic. Navigation, rail, maritime, and aviation systems are all enhanced with the aid of ITS. As a consequence, a lot of data is generated[2]. Transportation studies have developed more sophisticated systems known as ITS due to recent advancements in autonomous technology and growing urbanization. The primary objective of ITS is to provide participants with efficient, dependable, and safe transportation options. Authorities seek autonomy in ITS for various reasons, including safety for all users, energy savings for the environment, and time savings for users[3]. In today's increasingly linked society, security concerns are a major worry. As technology develops quickly, many industries, including transportation, are vulnerable to security and privacy breaches. Additionally, there are potential hazards associated with integrating smart devices and sensors into infrastructure, such as unconstitutional access to sensitive data or disruption of essential operations. Strong cyber security measures, including encryption, authentication methods, and frequent system upgrades, are crucial to addressing these security concerns[4].

Everyday communities and highways are changing in both look and usefulness thanks to the ITS. Thanks to the ITS, travelers worldwide may have a more efficient, safe, and enjoyable experience. Many companies and local governments have started initiatives to promote the development of ITS technology. Because of the increasing integration of unprotected devices and apps, transportation systems provide attackers with greater opportunity to exploit vulnerabilities. The physical repercussions of ITS attacks include infrastructure damage, an extension in emergency response, injuries, and even concerns to national security[5]. According to many, the most eagerly awaited smart city services are ITSs. The foundation of ITSs is that giving motors and transportation infrastructure connection, sensing, and autonomy would provide safer driving conditions and efficient transit. It is necessary to outfit cars and transportation infrastructure with smart sensors to gather and interpret heterogeneous data collection about each vehicle, its occupants, and its surroundings to make this ITS vision a reality[6].Transportation has always been important to human civilization since it fosters cross-cultural understanding and knowledge of the globe. Humans can go further in terms of distance and civilization thanks to the advancement of transportation. ITS are created for human safety and convenience in contemporary life, particularly in the metropolitan transportation network. As the foundation of ITS, sensors are extensively dispersed for signal collecting. And only if sensors are functional across the system can big data and subsequent processing be used for scheduling transportation, a process known as intellectualization[7]. Identifying security concerns early on in this study, we introduce a new Cuttle fish optimized Multiscale convolution neural network (ECFO-MCNN) for ITS based-on Intrusion Detection System (IDS) to identify malicious traffic in In-Vehicle Networks (IVNs), V2Is, and other networks.

The article's subsequent sections are arranged as follows: Section 2 provides a summary of relevant publications; Section 3 provides a more in-depth description of the approach; and Section 4 presents and discusses simulation findings. The study is concluded in Section 5 with recommendations for more research.

2. Related works

Yu et al.[8] offered an ITS with a combination of autonomous and human-driven automobiles with a Deep Learning (DL) based safety in-traffic solution. In a 5G-enabled ITS, long-term memory networks produce probability matrices using the trajectory dataset and the vehicle's natural-driving dataset as network resources. The final intended probability is then provided by combining the mean rule with the decision layer. The advancement of ITS research as a result of deep learning while also offering a review and in-depth insight into the uses of DL models on ITS. The current uses of these approaches in ITS are studied in depth after providing a variety of methods for DL and the present state of the field in Haghighat et al.[9]. Chen et al.[10] combined techniques for tracking and recognizing moving cars into a real time counter for automotive tracking. The accuracy and efficacy of the framework are then evaluated by installing a network for tracking numerous

objects and a network for detecting vehicles on a Jetson TX2 edge device. The test results reveal that their model has a 92.0% detection rate for traffic flow on edge devices and an average processing speed of 37.9 frames per second (FPS). A potential technology that seeks to enhance conventional transport management systems is called Cooperative Intelligent Transport System (C-ITS). The study proposes a private preserving oriented safe architecture for C-ITS infrastructure that combines Security and privacy to overcome these issues. Using blockchain technology and DL modules, the proposed architecture offers two levels of Security and anonymity[11].

Veres and Moussa[12] emphasized the usage of DL modeling techniques in ITS. They focus on the challenges that practitioners have faced in addressing these diverse problems and go into depth on the structural and problem-specific elements that were involved in developing solutions. They believe that by connecting the machine learning and transport fields, this survey will provide light on emerging topics and aspects. Tan et al.[13] addressed these issues, it was recommended that an ITS with SER-enhanced traffic efficiency be built on the space-air-ground integrated network, which is 5G capable. Data on the voice of the car is first converted into spectrograms to acquire the high-level characteristics of the vehicle speech acoustic model. The effort will evaluate the Machine Learning (ML) technologies and data mining employed in research and industry to address traffic's immediate and long-term consequences on individuals and society. According to the study's approach, 165 papers will be thoroughly reviewed, critiqued, and grouped into chronological and comprehensible categories[14]. Mollah et al.[15] provided a current analysis of the most recent developments in blockchain technology for the IoV. They thoroughly analyze the current research before highlighting the many IoV application situations. They also go at a few significant problems while blockchain is used in IoV. They also discuss the prospects for IoV as a crucial ITS enabler and future research objectives.The open Internet of Things (IoT) and its associated IoV will be made possible by 5G in this fashion. This discussion will go into depth about the potential effects of 5G wireless networks on smart cities, ITS, driverless or semi-autonomous cars, and vehicular communications, as well as on its technical, financial, and governmental challenges Guevara and Auat[16].

A safe energy trading ecosystem that can be utilized for activities like charging and discharging from the enabling smart grids is one of the critical hurdles to the overall usefulness of autonomous cars, as outlined by Chaudhary et al.[17]. Electric cars and uncrewed aerial aircraft are examples of uncrewed vehicles. The majority of the solutions available today were built on centralized, traditional security methods, which may not be appropriate for distributing energy in a smart city setting. Arthurs et al.[18] analyzed the literature on cloud computing utilization with ITS and connected cars and offered taxonomies in addition to their use cases. As a conclusion, they highlight research gaps that need to be filled before automobiles and ITS can make regulated and automated use of edge cloud computing. They looked at 496 publications published during seven years, starting in 2013 and finishing in 2019. Yang et al.[19] analyzed the various Energy management strategies (EMSs) for conventional hybrid electric vehicles (HEV) and plug in hybrid electric vehicles (PHEV) as well as those that use V2I and vehicle to vehicle (V2V) information. The EMSs for HEV and PHEV under the intelligent transport system are in-depth studied in terms of single-vehicle and multiple-vehicle situations. The massive, quickly growing volume of data to generate by ITS makes coordinating various transportation networks difficult. Therefore, the ancient cloud-centric storage architecture is no longer adequate. Meanwhile, a lack of confidence in retention across ITS devices and servers at the edge may result in security difficulties with data storage Qiao et al.[20]. Shukla et al.[21] developed a new spatially induced-long-short-term memory (SI-LSTM) model to forecast present traffic and weather. A dynamic pricing mechanism is offered to improve the vehicle owners' (VO) quality of experience (QoE). The Markov model, the SI-LSTM, the lanes, and the vehicles themselves all feed into this algorithm. Many parties are interested in vehicle-to-everything (V2X) communication and services since they will be included in future ITSs. Neither the V2X service placement challenge nor the nodes' computing capabilities have been taken into account in any previous effort. The

Greedy vehicle-to-everything Service Placement Algorithm (G-VSPA) is a low-complexity greedy-based heuristic approach created to address this issue Moubayed et al.[22].

In this study we employed ECFO-MCNN may outperform conventional MCNNs in terms of network architecture and parameter optimization by using the CFO algorithm. The CFO technique may enhance the neural network's overall performance and convergence speed during training by imitating the foraging activity of cuttlefish.

Problem statement

Complex security risks are difficult to correctly identify and mitigate using traditional approaches for handling security concerns in intelligent transportation systems (ITS). The dynamic nature of contemporary ITS security concerns outpace these approaches, which include rule-based systems, encryption techniques, and conventional anomaly detection algorithms, making them ineffective for threat identification and response. Additionally, traditional methods may not be able to manage the complex patterns and variances in the data, leading to a larger number of false positives and negatives and compromising the transportation network's overall security posture. Thus, we propose the implementation of the Fish Optimized Multiscale Convolution Neural Network (ECFO-MCNN) based Intrusion Detection System to improve security and accuracy in detecting suspicious network activities within in-vehicle networks, vehicle-to-infrastructure communication, and other network components in intelligent transportation systems (ITS).

3. Methodology

This part begins by discussing the preliminary processes of the study, which include data collection, data preprocessing, and data feature extraction. This study on creating a successful IDS for ITS is built on these fundamental goals. Provide the ECFO-MCNN, a cutting-edge method designed to solve the ubiquitous security issues in ITS. IVNs, V2I networks, and other pertinent networks are among the network components that IDS tries to detect and identify attackers' interiors (**Figure 1**).

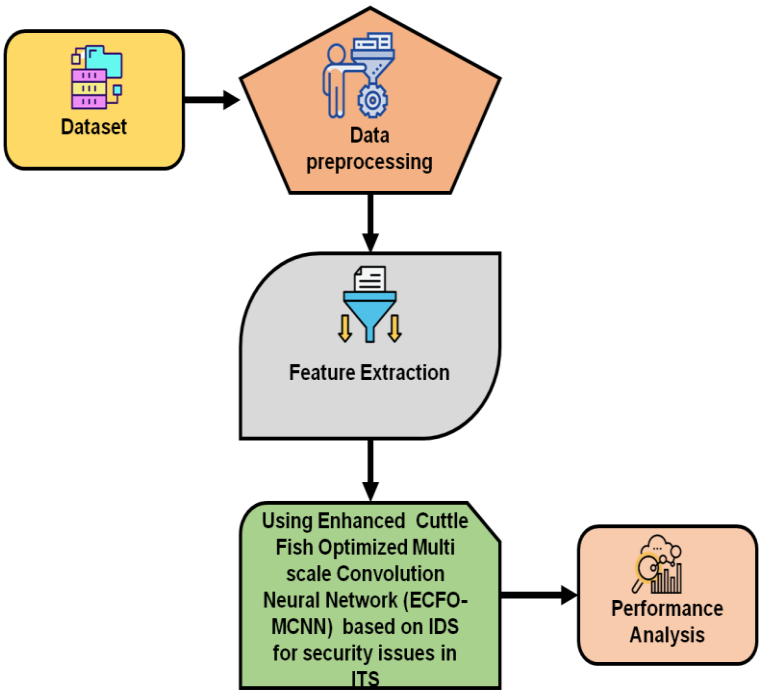

Figure 1. Analyses of the Proposed Methods and Procedures.

First, we collected the UNSWNB15 dataset, which contains data on various network activities. Next, we preprocessed the data using normalization techniques to standardize the values and ensure uniformity.

Following this, we extracted pertinent features from the processed data to identify key patterns and behaviors indicative of potential security threats within in-vehicle networks. Finally, we proposed a novel approach that aims to enhance both the security and accuracy of detecting suspicious network activities. By leveraging our method, we aim to identify and thwart potential threats more effectively, thereby bolstering the overall security measures within in-vehicle networks. Then we have analyzed the performance of our proposed approach.

Central gateways allow the networks to interact with outside networks. For example, gateways provide communication between vehicles, making various services possible. Additionally, V2I communication enhances the Security of automobiles, passengers, drivers, and walkers. Malicious hackers may attack IoVs via IVNs due to the inadequate security measures implemented by IVNs, such as the absence of encryption and authentication methods and the vast and continually expanding number of interfaces. Due to the vehicle's limited memory and processing power, installing an IDS or equivalent software proved difficult. The temporal non-linearity and latent spatial in the set of feature vectors could be found using the ECFO-MCNN layer. Normal traffic data is encoded and rebuilt by the auto encoder layer. The sliding temporal window created by the statistical characteristics is then fed into ECFO-MCNN. After many training rounds, validation losses and training are decreased to zero, and it is presumed that the compressed representation of typical traffic has acquired satisfaction.

3.1. Datasets

The UNSWNB15 dataset for anomaly detection originating through external connections and the vehicle hacking dataset for testing detection of irregularities in intra-vehicle communication are the two datasets used for evaluating the suggested ECFO-MCNN based on IDS. The 2 datasets are described as follows. The vehicle Hacking Dataset is the information regarding the automobile hacking dataset shown in **Table 1**.

Table 1. Data types and sizes of car hacking dataset.

Attack type	Overall Messages	Standard Messages	inject Messages
DoS assault	3,665,771	3,078,250	587,521
Gear Spoofing	4,443,143	3,845,891	597,253
Normal	988,988	988,873	-
Fuzzy assault	3,838,861	3,347,014	491,848
RPM guage spoofing	4,621,703	3,966,806	654,898

This information was created by gathering CAN traffic records from an actual vehicle's On-Board Diagnostics 2 (OBD-II) port. As the attacks were happening, the logs were taken. The dataset was produced for Network Based Intrusion Detection System (NIDS) assessment by building a synthetic laboratory setting. A mix of regular and attack traffic was made using the IXIA Perfect Storm program. Nine significant attack families' network traffic statistics are included in the collection. The necessary characteristics were extracted from the network data's pcap files using the Bro-IDS and Argus programs. The dataset used to assess the suggested IDS is detailed in **Table 2**.

Table 2. Unsw-Nb15 dataset categories and levels of data.

Type of Attack	Packets Number
Exploits attack	5409
DoS attack	1168
Recon attack	1760
Normal	677786
Generic attack	7523
Fuzzer attack	5,052

3.2. Data preprocessing

In this study we utilize Normalization data preprocessing technique that is commonly used to scale the values of numerical features to a standard range, typically between 0 and 1. This process ensures that all the features have a similar scale, which can be beneficial for many machine learning algorithms, including deep learning models. The unprocessed data gathered from IoVs and related network traffic pre-processed to develop an effective intrusion detection system.

3.3. Feature extraction

The extraction of essential data components is also required to implement the recommended DL-enabled detection strategy. The data selection of characteristics utilized for more analysis initiates a feature extraction step. These qualities are input in the statistical feature extraction process to filter out a sizable number of representative features, such as patterns of assault occurrences. To guarantee the remarkable effectiveness of the suggested ECFO-MCNN-based IDS, a 3-sec image with additional information is acquired to ascertain the actions of servers that interacted via data packets.

1) Enhanced cuttle fish optimized multiscale convolution neural network (ECFO-MCNN)
2) In a 5G-enabled ITS, long-term memory networks produce probability matrices using the trajectory dataset and the vehicle's natural-driving dataset as network resources.
3) Greedy vehicle-to-everything Service Placement Algorithm (G-VSPA)
4) Greedy vehicle-to-everything Service Placement Algorithm (G-VSPA)

Enhanced Cuttle Fish Optimized Multiscale Convolution Neural Network (ECFO-MCNN) based Intrusion Detection System (IDS) tailored for ITS. The proposed system aims to efficiently detect suspicious network activities within In-Vehicle Networks (IVN), Vehicles to Infrastructure (V2I) connections, and other related networks. Notably, the primary objective of this strategy is to identify potential security breaches originating from the central network gateways of AVs. Typical components of a CNN framework include an input layer, an output layer, and many hidden layers. Convolutional, pooling and fully linked hidden layer options are available. Because of the sparse connection between neurons in neighboring layers, local features in the convolutional layer are produced by convolutional kernels. Due to comparable statistical characteristics across the feature maps, it is possible to reconfigure and mine the necessary features via a sequence of convolutions. After convolution, a non-linear activation function is applied (Equation (1)).

$$C_i^k = \varphi\left(\sum_j C_i^{k-1} * f_{ji}^k + p_i^k\right) \tag{1}$$

where $*$ denotes the convolution operator, and C_i^{k-1} and C_i^k represent the j^{th} input and $k-1$ output feature maps for layer i^{th} and layer$k$, respectively, in the convolution process. A nonlinear activation function is used as the convolution kernel and bias φ.

In the pooling layer (PL), to use sub-sampling to make the output feature map insensitive to minor variations in the input characteristic map. Additionally, the smaller size of the feature map increases computing efficiency. Max-pooling is used, and it is described as

$$C_i^{k+1}(v,t) = \max_{0 \le b,o < n}\{C_i^k(v.n+b, t.n+o\} \tag{2}$$

where C_i^k and C_i^{k-1} are layer F's layer i^{th} output feature map and layer k layer i^{th}input feature map $k+1$ respectively. The set of size $n \times n$ of the pooling filter is to 2×2.

The ITS is susceptible to criminal actions like hacking, data breaches, and system manipulations since it depends on linked networks, communication systems, and digital infrastructure. These assaults can potentially interfere with transportation services, damage private data, and even endanger public safety. The possibility of

illegal access and manipulation of crucial systems is another issue. To solve this issue, use ECFO-MCNN that produces a mixed layer by combining the previous pooling layer with the final convolutional layer (CL). The fully-connected layer then comes after this mixed layer. This may maintain the synchronization of local and global data and provide more accurate regression results. The MSCNN construction is shown in **Figure 2**.

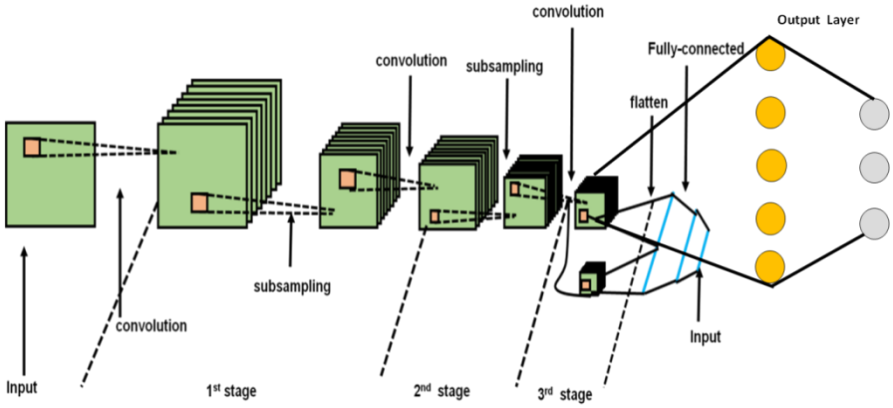

Figure 2. Structure of MSCNN.

The hidden layers have 3 CL, 2 PL, and a mixed layer. The third CL and the following one PL's characteristics are accepted by the mixed layer. Consequently, the mixed layer's output is determined as

$$C_{final} = \varphi\left(\sum_j l_j^1 . u_{ji}^1 + \sum_j l_j^1 . u_{ji}^2 + p_i\right) \tag{3}$$

where, respectively, l_j^l, u_{ji}^l, l_j^l, and u_{ji}^2 Consider the neurons and weights of the last pooling layer and the final CL. To execute Remaining Useful Life (RUL) estimation, C_{final} is finally delivered into the regression layer. As defined by MSE, the loss function is

$$F(\theta; C_{final}, x) = \frac{1}{2}\left\|z_\theta(C_{final}) - x\right\|^2 \tag{4}$$

where x is the RUL ground truth output. The last layer's regression function (RF) for RUL prediction is called z_θ.The θstands for the regression function's parameters.

A fish descended from squids, and octopuses took the ECFO-MCNN. Squids could always change their skin tone, either to blend in with their surroundings or to produce eye-catching displays. This fish, sometimes known as a cuttlefish or a squid, imitates the hues of its environment. The cuttlefish uses three levels of cell layers to generate its colors and shapes. The program mimics the cuttlefish's manner of color-changing behavior to address security challenges in ITS. Visibility and Reflection are the two key processes that comprise the suggested method. The visibility process provides a simulation of the cuttlefish's pattern-matching vision, while the reflection process provides a simulation of the Reflection of light between layers of cells. The method used to identify security problems in ITS.

The ECFO processes are broken down and shown in **Figure 2** provides a summary of it. The state of each cell is brought up to date by Equation (5).

$$H_m[i] = rec_m[j] + vit_m[j] \tag{5}$$

where j is the pint index in the i^{th} cell, i is the cell index, m is the group index, rec is the Reflection, and it is the visibility. Equations (6) and (7) are used to calculate the visibility vit_m and reflection of H_l and H_{la}.

$$rec_j = T \times H_1[i] \times b[j] \tag{6}$$

$$vit_j = D \times (Gbest[j] - H_1[i] \times S[j] \tag{7}$$

where S denotes the study group of points, T represents the cell reflection degree, and D is the pattern visibility degree. Following are the calculations for the variables T and D (Equation (8) and Equation (9)):

$$T = rand \times (t_1 - t_2) + t_2 \tag{8}$$

$$D = rand \times (d_1 - d_2) + d_2 \tag{9}$$

where t_1, t_2, d_1, and d_2 are user-specified constants, and the rand is a random integer between (0, 1). Equations for Reflection and visibility for the third group H_3 are as follows (Equation (10) and Equation (11)):

$$rec_j = T \times Gbest[j] \tag{10}$$

$$vit_j = D \times (Gbest[j] - AVSbest) \tag{11}$$

There was no estimate for visibility and Reflection for the fourth group H_4. **Figure 3** displays the flowchart for the algorithm.

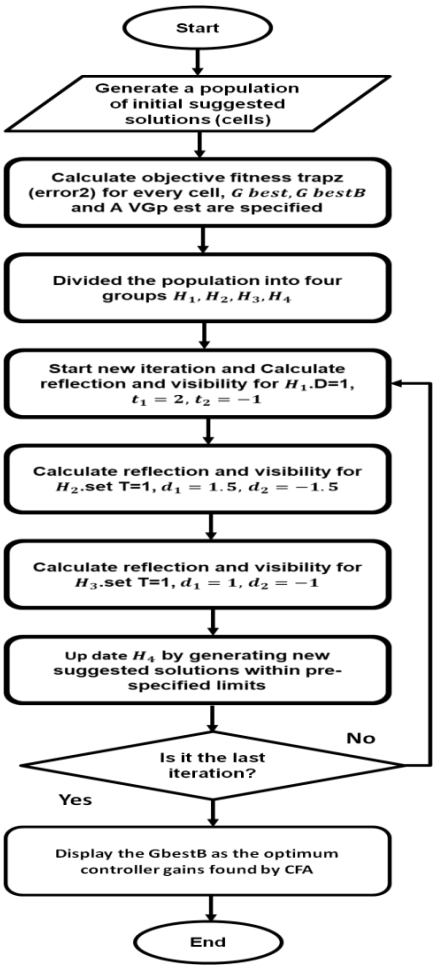

Figure 3. Flowchart of the ECFO.

4. Result and discussion

To predict potential security issues and offer a novel ECFO-MCNN for ITS based on an IDS to detect hostile traffic in IVNs, V2Is, and other networks. The efficiency of the proposed technique is shown by comparing the results of the ECFO-MCNN with those of existing methods like SI-LSTM and G-VSPA. Accurate and precision evaluation of the proposed system's adaptability, responsiveness, and prediction is shown by the presented technique.

4.1. Accuracy

Accuracy is essential to ITS, as multiple parts, including sensors, communication networks, and control systems, interact to ensure the efficiency and safety of the transportation infrastructure. It includes the system's capacity to accurately detect, gather, analyze, and send data and carry out instructions and reach judgments with little variation from the planned course of action (Equation (12)).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{12}$$

where,

- TP represented as True Positives
- TN represented as True Negatives
- FP represented as False Positives
- FN represented as False Negatives

The accuracy of the suggested system is shown in **Table 3**. Both the proposed method and the existing systems' accuracy of consumption forecasts are shown. To compared SI-LSTM's 79% and G-VSPA's 81%, both get below the desired 95% accuracy for the suggested method. It shows that the proposed method of procedure is better than the existing one.

Table 3. Numerical outcomes of accuracy.

Method	Accuracy (%)
SI-LSTM [21]	79
G-VSPA [22]	81
ECFO-MCNN [Proposed]	95

4.2. Precision

Precision is essential for differentiating between legal actions and harmful behaviors in ITS, as identifying and preventing possible security breaches are key. While avoiding false positives or misclassifications, high precision ensures that security measures properly detect and react to true threats.

$$\text{Precision} = \frac{TP}{TP + FN} \tag{13}$$

The suggested system's precision is shown in **Table 4**. Where FP and TP stand for a true positive value and a false positive, respectively. The suggested system and existing systems' predictions of precision usage are discussed. SI-LSTM has attained 79%, G-VSPA has attained 81%, and the suggested system has attained 94%. It demonstrates that the proposed strategy is more successful than the existing one.

Table 4. The exact numerical results of precision.

Methods	Precision (%)
SI-LSTM [21]	86
G-VSPA [22]	72
ECFO-MCNN [Proposed]	94

4.3. Training and hyper parameter tuning

The length of the sliding window L_{en} = 11 was suitable to facilitate latent encoding and later reconstruction for both datasets. Compared to CAN, the UNSW dataset required significantly longer epochs to bring validation losses and average training under control.

Table 5 and **Figure 4** display the two dataset's most current setting of hyper parameters and the training loss direction.

Table 5. The ECFO-MCNN Model's Hyper parameters for the Can and Unsw Dataset.

	F	Z	P	$\mathcal{F}(h, \hat{h})$	Epochs
UNSW	11	101	51	ϵ_2	2001
CAN	11	51	101	ϵ_2	501

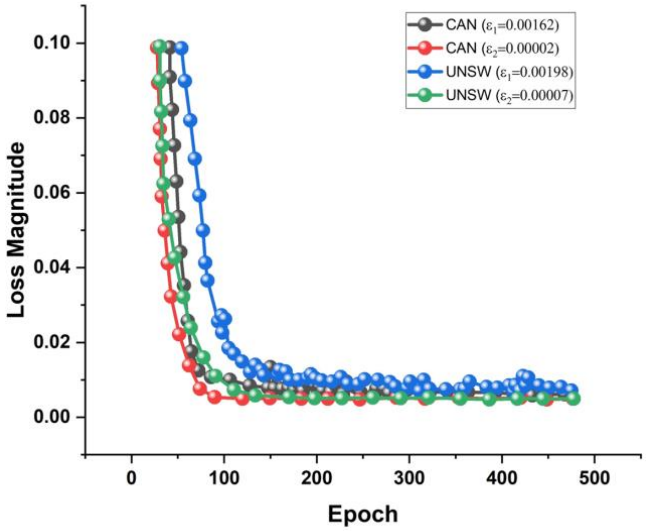

Figure 4. Loss's trajectory during the course of the autoencoder's training on the CAN and UNSW datasets.

In accordance with the results of the quick search for grids, a batch quantity of between 11 and 100 was suitable for development, still, for the UNSW and CAN datasets. Accordingly, b = 100 and b = 50 were chosen while considering the appropriate training time. The UNSW dataset's normalized likelihood transformation required four times as many epochs and significantly more hidden ECFO-MCNN units due to its greater spatiotemporal complexity to reconstruct the input batches accurately without over-fitting the model and lowering accuracy.

4.4. Selection of optimal threshold

The accuracy of the error surfaces depends on the selection of the threshold σ, and they may be linearly separated for both datasets with varied degrees of error. As illustrated in **Figure 5**, the best threshold σ_{opt} is discovered using Receiver Operating Characteristics (ROC) and grid search to apply the decision statistic.

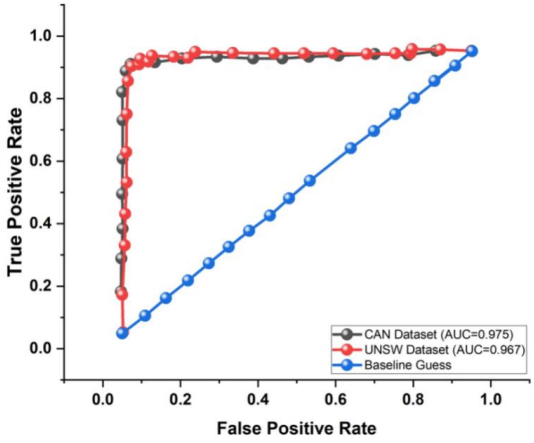

Figure 5. Grid search for the best threshold σ.

The estimation of the True positive rate and false positive rate, respectively, and the following formulas were used to derive the detection probabilities over the complete collection of $S = \sigma\epsilon[0.06, 0.94]$ and ROC curves (Equation (14) and (15)):

$$TPR = \frac{TP}{TP + FN} \tag{14}$$

$$FPR = \frac{FP}{FP + TN} \tag{15}$$

where the appropriately recognized normal and attack vectors are, respectively, TP and TN. FN, on the other hand, refers to those attack vectors that the classifier incorrectly misclassifies as genuine regular traffic considering that the problem may be reduced to a binary classification, with all attack pathways being considered fraudulent. Last but not least, FP is regular sequences that are mistakenly labeled as aberrant.

4.5. Discussion

The G-VSPA's security flaws are a major drawback of the protocol. G-VSPA's selfish character causes it to put a premium on near-term and regional optimization of service placement while ignoring the dangers that may arise from doing so. As a result, the security of the V2X network's data transmissions may be compromised by malicious assaults or unauthorized access. As a result, G-VSPA has its limits, hence a stronger security framework is necessary to guarantee the safe and secure functioning of ITS. The SI-LSTM's susceptibility to hostile assaults is a severe drawback. In order to modify the input data or produce malicious results, adversaries might take advantage of the spatial dependencies that SI-LSTM has learnt. SI-LSTM may not sufficiently take into account possible security concerns and may not be able to identify or neutralize hostile activity since it mainly focuses on collecting spatial correlations. Anomaly detection and intrusion detection systems, which assist in identifying and mitigating possible security breaches inside the ITS environment, are included in ECFO-MCNN's increased security mechanisms. By offering real-time network activity monitoring, the ECFO-MCNN makes it possible to quickly identify and address any questionable activity or possible intrusions. This skill is essential for maintaining the security of in-vehicle networks at all times since failing to recognize security risks in a timely manner may have disastrous results, such as compromised data or malfunctioning systems. Additionally, the ECFO-MCNN's Multiscale convolutional neural network design enables accurate and fast analysis of complicated transportation data, allowing the real-time identification of anomalous or suspicious patterns.

5. Conclusion

Deep learning may be used to address several ITS security-related issues, including detection of intrusions, anomaly detection, and risk prediction. As a result, risks are reduced, and vital transportation infrastructure is protected via proactive monitoring and quick reaction to security issues. The IoVs are vulnerable to numerous cyber-attacks due to their pervasiveness and inadequate security implementation in the technologies being employed. IoVs may be effectively protected against a variety of assaults with the use of IDSs. This study aimed to create an IDS model that could recognize attacks by looking for changes in the latent representations of messages and network flows that were learned to behave normally in IVNs. We suggested IDS based on ECFO-MCNN auto encoder for identifying odd occurrences in IoVs. The recommended method combines and integrates the strength of statistical features of network activity with the reliable learning mechanism of ECFO-MCNN auto encoder to construct a potent model for learning typical traffic flow in IoVs. For the UNSWNB-15 and automobile hacking datasets, respectively, the suggested ECFO-MCNN-based IDS's overall average accuracy is 95%. Our method has outperformed well than other existing methods. ECFO-MCNN offers a promising approach for addressing complex and challenging tasks in image processing, intelligent transportation systems, and other domains that require robust and efficient deep learning solutions. DL models could be hard to understand, which makes it hard to comprehend the reason for making judgments and can

make users and stakeholders less likely to trust and accept them. Concentrating on these areas of future study creates the foundation for an ecosystem of ITS that is strong and secure, able to endure changing security threats, and safeguards infrastructure and human life.

Author contributions

Conceptualization, SKG and RSKB; methodology, RRC; software, MT; validation, RS, AAG and PPG; formal analysis, AAG; investigation, PPG; resources, RS; data curation, MT; writing — original draft preparation, SKG; writing — review and editing, RRC; visualization, SKG; supervision, RSKB; project administration, SKG. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Gohar A, Nencioni G. The Role of 5G Technologies in a Smart City: The Case for Intelligent Transportation System. Sustainability. 2021, 13(9): 5188. doi: 10.3390/su13095188
2. Kaffash S, Nguyen AT, Zhu J. Big data algorithms and applications in intelligent transportation system: A review and bibliometric analysis. International Journal of Production Economics. 2021, 231: 107868. doi: 10.1016/j.ijpe.2020.107868
3. Gaur L, Sahoo BM. Introduction to Explainable AI and Intelligent Transportation. In: Explainable Artificial Intelligence for Intelligent Transportation Systems: Ethics and Applications. Springer International Publishing. pp. 1-25.
4. Pal S, Jadidi Z. Analysis of Security Issues and Countermeasures for the Industrial Internet of Things. Applied Sciences. 2021, 11(20): 9393. doi: 10.3390/app11209393
5. Zeddini B, Maachaoui M, Inedjaren Y. Security Threats in Intelligent Transportation Systems and Their Risk Levels. Risks. 2022, 10(5): 91. doi: 10.3390/risks10050091
6. Rammohan A. 2023. Revolutionizing Intelligent Transportation Systems with Cellular Vehicle-to-Everything (C-V2X) Technology: Current Trends, Use Cases, Emerging Technologies, Standardization Bodies, Industry Analytics and Future Directions. Vehicular Communications. 2023, 43: 100638. doi: 10.1016/j.vehcom.2023.100638
7. Du YL, Yi TH, Li XJ, et al. Advances in Intellectualization of Transportation Infrastructures. Engineering. 2023, 24: 239-252. doi: 10.1016/j.eng.2023.01.011
8. Yu K, Lin L, Alazab M, et al. Deep Learning-Based Traffic Safety Solution for a Mixture of Autonomous and Manual Vehicles in a 5G-Enabled Intelligent Transportation System. IEEE Transactions on Intelligent Transportation Systems. 2021, 22(7): 4337-4347. doi: 10.1109/tits.2020.3042504
9. Haghighat AK, Ravichandra-Mouli V, Chakraborty P, et al. Applications of Deep Learning in Intelligent Transportation Systems. Journal of Big Data Analytics in Transportation. 2020, 2(2): 115-145. doi: 10.1007/s42421-020-00020-1
10. Chen C, Liu B, Wan S, et al. An Edge Traffic Flow Detection Scheme Based on Deep Learning in an Intelligent Transportation System. IEEE Transactions on Intelligent Transportation Systems. 2021, 22(3): 1840-1852. doi: 10.1109/tits.2020.3025687
11. Kumar R, Kumar P, Tripathi R, et al. A Privacy-Preserving-Based Secure Framework Using Blockchain-Enabled Deep-Learning in Cooperative Intelligent Transport System. IEEE Transactions on Intelligent Transportation Systems. 2022, 23(9): 16492-16503. doi: 10.1109/tits.2021.3098636
12. Veres M, Moussa M. Deep Learning for Intelligent Transportation Systems: A Survey of Emerging Trends. IEEE Transactions on Intelligent Transportation Systems. 2020, 21(8): 3152-3168. doi: 10.1109/tits.2019.2929020
13. Tan L, Yu K, Lin L, et al. Speech Emotion Recognition Enhanced Traffic Efficiency Solution for Autonomous Vehicles in a 5G-Enabled Space–Air–Ground Integrated Intelligent Transportation System. IEEE Transactions on Intelligent Transportation Systems. 2022, 23(3): 2830-2842. doi: 10.1109/tits.2021.3119921
14. Alsrehin NO, Klaib AF, Magableh A. Intelligent Transportation and Control Systems Using Data Mining and Machine Learning Techniques: A Comprehensive Study. IEEE Access. 2019, 7: 49830-49857. doi: 10.1109/access.2019.2909114
15. Mollah MB, Zhao J, Niyato D, et al. Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey. IEEE Internet of Things Journal. 2021, 8(6): 4157-4185. doi: 10.1109/jiot.2020.3028368
16. Guevara L, Auat Cheein F. The Role of 5G Technologies: Challenges in Smart Cities and Intelligent Transportation Systems. Sustainability. 2020, 12(16): 6469. doi: 10.3390/su12166469
17. Chaudhary R, Jindal A, Aujla GS, et al. BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system. Computers & Security. 2019, 85: 288-299. doi: 10.1016/j.cose.2019.05.006

18. Arthurs P, Gillam L, Krause P, et al. A Taxonomy and Survey of Edge Cloud Computing for Intelligent Transportation Systems and Connected Vehicles. IEEE Transactions on Intelligent Transportation Systems. 2022, 23(7): 6206-6221. doi: 10.1109/tits.2021.3084396
19. Yang C, Zha M, Wang W, et al. Efficient energy management strategy for hybrid electric vehicles/plug‐in hybrid electric vehicles: review and recent advances under intelligent transportation system. IET Intelligent Transport Systems. 2020, 14(7): 702-711. doi: 10.1049/iet-its.2019.0606
20. Qiao F, Wu J, Li J, et al. Trustworthy Edge Storage Orchestration in Intelligent Transportation Systems Using Reinforcement Learning. IEEE Transactions on Intelligent Transportation Systems. 2021, 22(7): 4443-4456. doi: 10.1109/tits.2020.3003211
21. Shukla A, Bhattacharya P, Tanwar S, et al. DwaRa: A Deep Learning-Based Dynamic Toll Pricing Scheme for Intelligent Transportation Systems. IEEE Transactions on Vehicular Technology. 2020, 69(11): 12510-12520. doi: 10.1109/tvt.2020.3022168
22. Moubayed A, Shami A, Heidari P, et al. Edge-Enabled V2X Service Placement for Intelligent Transportation Systems. IEEE Transactions on Mobile Computing. 2021, 20(4): 1380-1392. doi: 10.1109/tmc.2020.2965929