Hindawi
Mathematical Problems in Engineering
Volume 2022, Article ID 3424819, 8 pages
https://doi.org/10.1155/2022/3424819

Research Article

Distributed Deep CNN-LSTM Model for Intrusion Detection Method in IoT-Based Vehicles

Ali Alferaidi,[1] Kusum Yadav,[1] Yasser Alharbi,[1] Navid Razmjooy,[2] Wattana Viriyasitavat,[3] Kamal Gulati,[4] Sandeep Kautish,[5] and Gaurav Dhiman[6,7]

[1] *College of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia*
[2] *Department of Electrical Engineering, Ardabil Branch, Islamic Azad University, Ardabil, Iran*
[3] *Department of Statistics, Chulalongkorn Business School, Faculty of Commerce and Accountancy, Bangkok, Thailand*
[4] *Amity School of Insurance, Banking and Actuarial Science, Amity University, Noida, India*
[5] *LBEF Campus, Kathmandu, Nepal*
[6] *Department of Computer Science, Government Bikram College of Commerce, Patiala 147001, Punjab, India*
[7] *University Centre for Research and Development, Department of Computer Science and Engineering, Chandigarh University, Gharuan, Mohali, India*

Correspondence should be addressed to Sandeep Kautish; dr.skautish@gmail.com

Received 25 November 2021; Revised 15 January 2022; Accepted 3 February 2022; Published 19 March 2022

Academic Editor: Ramin Ranjbarzadeh

As 5G and other technologies are widely used in the Internet of Vehicles, intrusion detection plays an increasingly important role as a vital detection tool for information security. However, due to the rapid changes in the structure of the Internet of Vehicles, the large data flow, and the complex and diverse forms of intrusion, traditional detection methods cannot ensure their accuracy and real-time requirements and cannot be directly applied to the Internet of Vehicles. A new AA distributed combined deep learning intrusion detection method for the Internet of Vehicles based on the Apache Spark framework is proposed in response to these problems. The cluster combines deep-learning convolutional neural network (CNN) and extended short-term memory (LSTM) network to extract features and data for detection of car network intrusion from large-scale car network data traffic and discovery of abnormal behavior. The experimental results show that compared with other existing models, the algorithm of this model can reach 20 in the fastest time, and the accuracy rate is up to 99.7%, with a good detection effect.

1. Introduction

With the practical application of emerging technologies in the field of the Internet of Vehicles, the development of the Internet of Vehicles has become more rapid. Due to its particularity, that is, the car itself does not consider network security enough, the capacity of the vehicle is limited, the application environment is complex, the number of distributed nodes and sensor networks are many, and the safety requirements are incredibly high. Therefore, the security issue of the Internet of Vehicles has increasingly become a stumbling block to its application. Ensuring the security of car G road G cloud communications in the car networking security system, identifying various malicious attacks, has become the focus of close attention by industry insiders and information security experts. Intrusion detection is a network security technology used to detect intruders and aggression in any communication system through various identifications or detections.

Attack behavior, monitor and analyze network traffic, classify normal and abnormal behavior, and identify strange activities such as threats in the network are all roles played by the Internet of Vehicles. As an active defense technology, this technology has become one of the primary mechanisms to ensure the safety of the Internet of Vehicles. The application of machine learning algorithms in traditional Internet intrusion detection systems is the current mainstream research direction. Wisanwanichthan and Thammawichai [1] apply the machine learning method to intrusion detection systems (IDS), and use SVM and Naive Bayes algorithms for normalization and feature reduction for analysis and comparison. However, the key disadvantage of the machine learning-based intrusion detection mechanism is that it requires a lot of training time to process many datasets of previous data streams in the network. In the network environment, deep learning technology has good self-learning functions, Lenovo storage functions, and high-speed optimization functions, which are very suitable for processing the current complex network traffic data, especially in the complex car networking environment.

At the moment, there is a great deal of research being conducted on intrusion detection using deep learning and distributed big data technologies. Chen et al. [2] developed a hybrid deep neural network (DNN) model for classifying and detecting unknown network threats. Chen et al. [2] think that deep learning has received a lot of attention recently, and they compared conventional techniques to new deep learning methods. Chen et al. [3] constructed an intelligent intrusion detection system using deep learning's intelligent capabilities. Vijayanand et al. [3] presented a technique for detecting anomalous intrusions using a hybrid MLP/CNN. Parimala and Kayalvizhi [4] developed a deep learning-based technique for detecting network intrusions. The KDD-CUP99 dataset was examined using the BP neural network to identify the kinds of invasions. Karatas et al. [5] developed an intrusion detection technique based on deep convolutional neural networks, which lowers the dimensionality of network data by converting it to pictures. The detection accuracy, false alarm rate, and detection rate are all enhanced via training and recognition. Shettar et al. [6] utilized Keras on top of TensorFlow to categorize various assaults using supervised deep learning and achieved the best accuracy using RNN deep learning technology. Zhang et al. [7] implemented random forests and SVMs using the Spark framework. Other machine learning methods were evaluated and compared to multilayer deep perceptions. We may conclude from studies that although deep learning algorithms are more accurate than conventional machine learning algorithms, they need more time to examine data. The static network in its traditional form intrusion detection is often classified as either host-based or network-based. The Internet of cars' intrusion detection is accomplished by filtering the data transferred between vehicles. Due to the fact that the Internet of Vehicles is also linked to the Internet or to a specialized network, traditional harmful attack techniques are also successful on the Internet. They are more damaging, which necessitates more stringent standards for intrusion detection protection. Combining the features of the Internet of Vehicles' massive traffic and multidimensional complexity, the application of deep neural network detection. Due to the benefits of distributed parallel computing and its rapid and influential features, this article proposes using a combined deep learning algorithm with the Spark framework [8, 9] for intrusion detection. By utilizing the Spark architecture, the traditional deep learning algorithm is improved. Combining CNN and LSTM, Dey [10] proposed the CNNGLSTM algorithm model, which was used to analyze the NSL-KDD dataset [11] and the UNSW-NB15 dataset [12–15] in order to minimize security attacks on connected vehicles. Its primary objective is to decrease the time needed to identify assaults and increase the accuracy of classification jobs, which is more appropriate for the Internet of Vehicles' real environment. Each indication has been enhanced as a result of experimental research. Researchers are proposing various protocol schemes [16–20] to maintain the integrity, confidentiality, and security of the information shared among users and servers.

The rest of this paper is structured as follows: Section 2 describes the CNN-LSTM algorithm. The Spark framework and NSL-KDD dataset are mentioned in Sections 3 and 4, respectively. Result analysis is given in Section 5, followed by the conclusions in Section 6.

2. CNN-LSTM Algorithm

CNN is suitable for extracting data features; LSTM is suitable for processing time series, solving the dependency problem between time-series data, and improving recognition accuracy. This paper combines the advantages of the two algorithms and proposes the CNNGLSTM algorithm. Convolution neural network (CNN) [21] evolved from multilayer perception (MLP) [22]. Compared with traditional feature selection algorithms, this algorithm can learn features better. The more traffic data CNN can learn, the more useful features there are, the better the classification, which is suitable for large-scale network environments. As shown in Figure 1, its structure is divided into a convolution layer, a pooling layer, and a fully connected layer. The role of the convolution layer is to extract features, and the role of the pooling layer is to sample the features. Finally, the fully connected layer is responsible for connecting the extracted features and obtaining the classification results through the classifier.

The long-term memory network (LSTM) is an improved recurrent neural network (RNN) method, which aims to alleviate the explosion gradient problem. Compared with traditional RNN units, LSTM uses a set of gate functions to control feedback so that short-term errors will eventually be deleted while persistent features will be retained. The data processing flow is shown in Figure 2.

The LSTM is abstracted into four subnets (p-net, g-net, f-net, and q-net), a collection of gate controllers, and a link to the memory component. The figure's input and output are controlled by the vector's size, $x\ (t)$. The state $s\ (t)$ contains information about the present learning.

The CNN-LSTM method is capable of expressing both temporal and spatial information. Due to the fact that an intrusion assault occurs in real time, the methods of attack are varied, as is the target or point of attack. To extract features, a CNN is utilized, and high-level features may be retrieved using the convolution kernel operation, which has been successfully used in image processing [23–25]. Additionally, LSTM utilizes gate functions to regulate the remembering and forgetting of previous data, making it ideal for processing long-term sequence data and increasing detection accuracy [26, 27]. As a result, the CNN-LSTM algorithm model is suitable for intrusion detection processing in this study. Figure 3 illustrates the CNN-LSTM algorithm paradigm, and the particular stages are as follows:

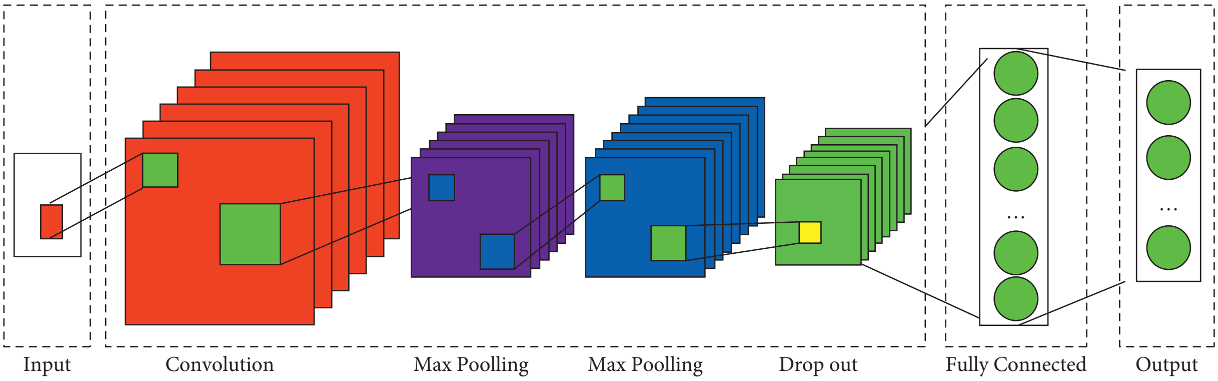

Figure 1: CNN architecture.

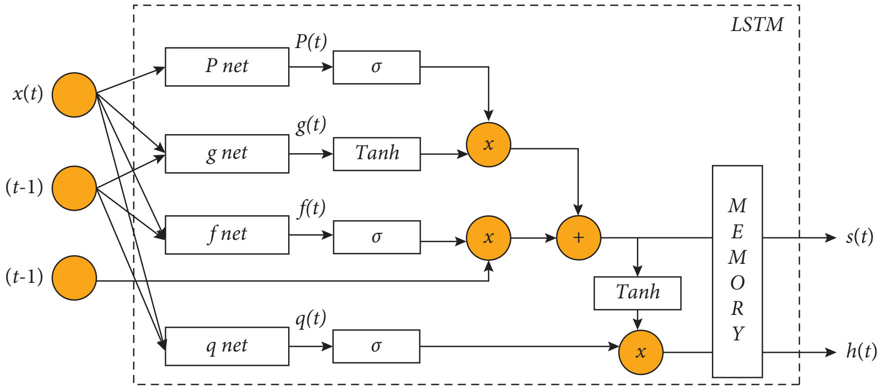

Figure 2: LSTM data processing diagram.

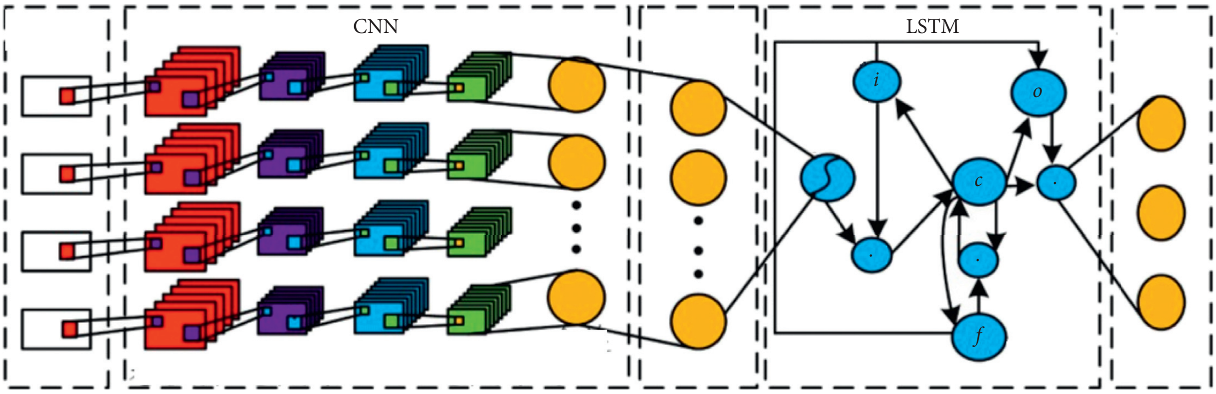

Figure 3: CNN-LSTM model architecture.

(1) The input layer collects real-time Internet of Vehicles data through the flow data collection module. This article uses the dataset to analyze characteristics, including network protocol types, network service types, network connection status, and connection time [28, 29].

(2) According to the data processing steps, the data are respectively preprocessed, digitized, and normalized. The specific operation steps will be described in detail later.

(3) It sends the processed data to the convolution layer for feature extraction and outputs the features through a one-dimensional convolution operation. Each convolution layer is accompanied by a pooling layer to reduce feature dimensions, accelerate convergence, and remove redundancy features to prevent network overfitting. Then all local features are integrated through the fully connected layer to form an overall feature. Finally, the leaky ReLU activation function in the fully connected layer is operated [30–32].

(4) Input the features extracted by CNN into LSTM. After the SoftMax function, the classification result of network data is obtained [23, 33, 34].

3. Spark Framework

To enhance detection efficiency, this study makes use of the Apache Spark framework, a large data processing platform focused on speed, simplicity of use, and sophisticated analysis. It was created in 2009 [8–10] at the University of California, Berkeley, and became one of the Apache open-source projects. In comparison to other big data technologies such as Hadoop, Storm, and MapReduce, Spark offers the following advantages [35–37]:

(a) Spark offers a consistent and comprehensive framework for handling diverse datasets and data sources (batch or real-time streaming data) with varying characteristics (text data, chart data, etc.) [38, 39].

(b) Spark improves the performance of Hadoop cluster apps operating in memory by 100 times and the speed of Hadoop cluster applications running on the disc by ten times [14, 40].

(c) When compared to MapReduce, Spark performs quicker data calculations and offers more robust functions [25, 41].

When the quantity of processed data surpasses the capacity of a single machine (for example, a computer with 4 GB of memory must process more than 100 GB of data), or when the amount of processed data is trivial, nonetheless, the calculation is difficult and time-consuming. As a result, the Spark cluster can use its massive computational capabilities to perform the analysis in an organized fashion. The architecture's schematic design is shown in Figure 4.

Using the Spark distributed open-source framework, the experimental PCs are connected to form a master-slave control structure. The master node performs task scheduling, distribution, and fault tolerance on the slave nodes, and the slave nodes realize parallel computing. This structure has been proven to be an owner of a distributed design with high reliability, high concurrency, and high-performance computing capabilities. The HDFS storage system of the node is then used to store the data, and the combined deep learning algorithm is used for intrusion detection.

4. NSL-KDD Dataset

In contrast to a conventional network, the heterogeneous communication network created by vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication are formed by the self-organization of vehicle nodes. Driving, fast channel fading, strong Doppler effect, and rapid network topology changes are all examples of rapid network topology changes. However, the attack techniques used against the Internet of Vehicles throughout the communication process are very similar to those used against conventional networks, including backdoor assaults and denial of service attacks. To evaluate the proposed Spark-based distributed combined deep learning intrusion detection method for the Internet of Vehicles, the proposed deep learning algorithm is applied to two intrusion detection benchmark datasets, namely, NSL-KDD [11] and UNSW-NB15 [12], in order to develop an effective intrusion detection system for the Internet of Vehicles' external communication. There are a total of 21,473 pieces of training data and 51,025 pieces of test data in the experimental dataset.

The NSL-KDD dataset is a refinement of the KDD CUP 99 data collection [12]. It eliminates redundant records from the CUP 99 dataset and addresses the classifier's bias for repeating records. In comparison to the KDD 99 dataset, the usage of NSL classification of the KDD dataset will provide comparable or superior accuracy. As a result, it is widely regarded as one of the most effective datasets for intrusion detection studies. The dataset's assaults are classified into four groups.

(1) Denial of service (DoS): the intruder will send many malicious requests to the server, causing the machine's memory and computational resources to become insufficiently full or busy to handle genuine traffic, thus denying regular users services.

(2) User-to-root (U2R): this is a kind of attack in which the attacker tries to acquire administrator privileges through regular user access.

(3) Remote-to-local attack (R2L): the attacker wishes to transmit data to a computer via a network in order to obtain access to the machine fraudulently.

(4) Detection attack (Probe): the network is scanned to obtain detailed information about the user's device.

In addition, the dataset contains 49 features, which constitute the traffic that exists between the host and the network data packet and are used to distinguish normal or abnormal observation results. Compared with other datasets, it contains both real-scene data and synthetic data. Attack behavior and the complexity of UNSW-NB means dataset are valid and reliable.

5. Result Analysis

The CNNGLSTM algorithm and SVM, RNN, CNN, and LSTM algorithms are used to compare the accuracy rate (AC) and false alarm rate (FPR) of different attack types. The CNN-LSTM method has a high classification detection rate. Compared with other algorithms, it has a lower false alarm rate.

To verify the overall effectiveness and comparison of the experiment, this paper uses two datasets of NSL-KDD and UNSW GNB15 to compare the accuracy rate (AC) and false alarm rate (FPR) of the above five algorithms. The experimental results are shown in Figures 5 and 6.

It can be seen from Figures 7 and 8 that CNN-LSTM performs well in the NSL-KDD dataset and UNSWGNB15 dataset reaching 7% and 99%, respectively. The accuracy rate of 4% also has the lowest false alarm rate of two, respectively, 24% and 2.17%. Therefore, this algorithm has better performance characteristics among similar algorithms.

All the deep learning algorithms discussed in this article are implemented in a distributed manner under Apache Spark. The experimental results are shown in Figures 7 and 8.

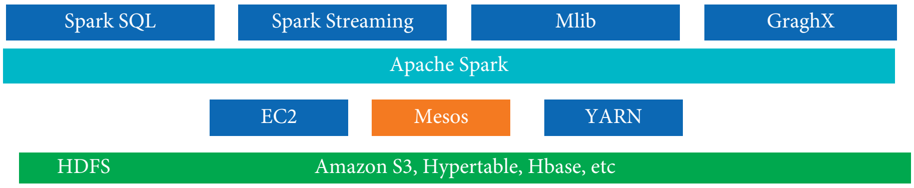

Figure 4: Apache spark architecture.

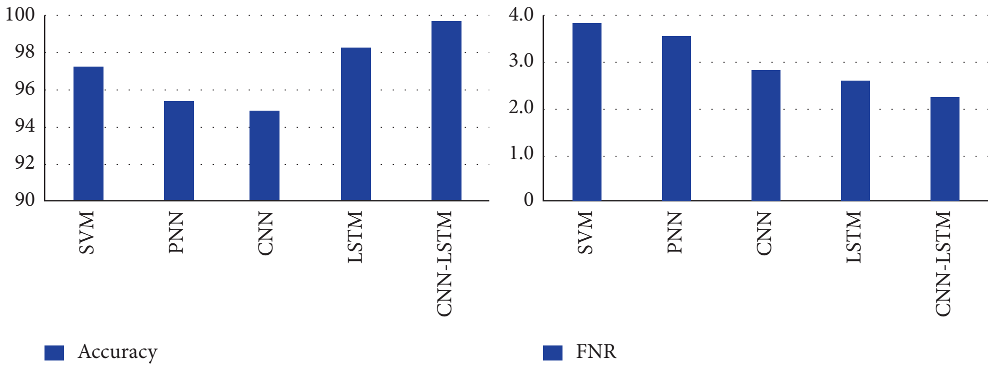

Figure 5: Performance comparison of various algorithms under NSL-KDD dataset.

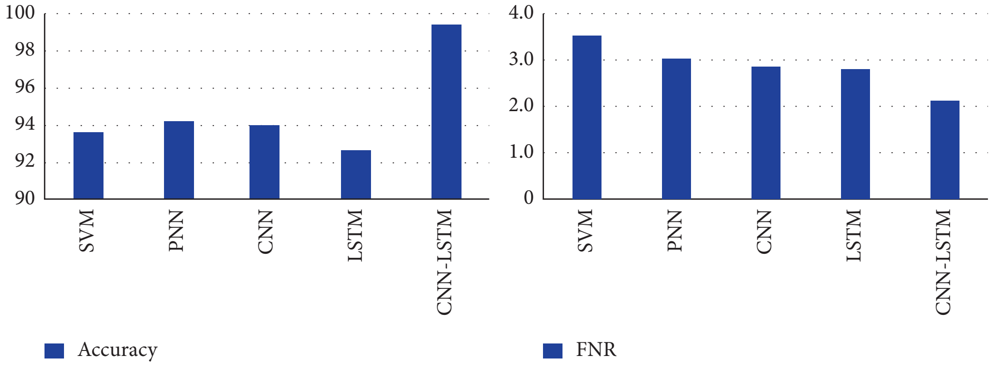

Figure 6: UNSW-NB15 dataset performance comparison of each algorithm.

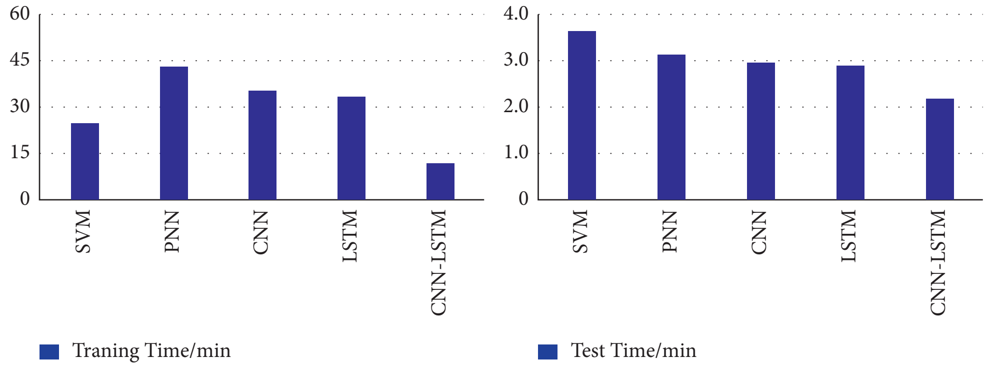

Figure 7: Detection time of each algorithm under the NSL GKDD dataset.

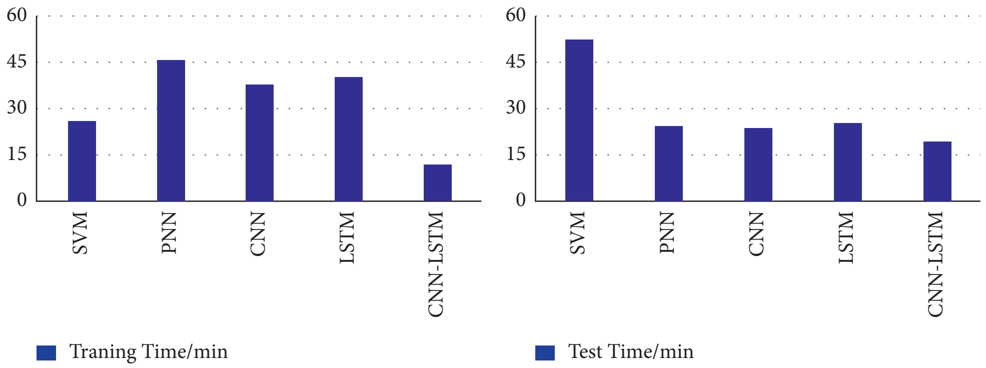

Figure 8: Detection time of each algorithm under UNSWGNB15 dataset.

It can be seen that compared with traditional nonparallel machines and deep learning algorithms, the training and testing time is significantly shortened. Furthermore, the experimental results show that the training time and test time used by the CNN-LSTM algorithm are the shortest.

6. Conclusion

Comparative experiments found that because of the slow detection speed and low detection efficiency of big data in intrusion detection systems, the advantages of distributed frameworks and deep learning algorithms are fully considered, and the distributed architecture is combined with the deep learning CNN-LSTM algorithm. Through data, the detection efficiency and detection time are improved after the data is standardized by preprocessing and other methods. Experimental verification on the NSL-KDD dataset and the UNSW-NB15 dataset shows that the deep learning algorithm of CNN-LSTM using the Spark framework is comparable to other deep learning algorithms. It reduces the training time and test time, improves the detection rate, can well meet the real-time requirements of intrusion detection, and more satisfies the actual needs of the Internet of Vehicles for intrusion detection. In the next step, this article will improve based on intrusion detection performance and reduction of detection time, and we will further focus on the detection capabilities of deep learning algorithms, conduct intrusion detection on distributed platforms, and explore suitable distributed deep learning algorithms to meet the needs of intrusion detection for car network information security. A more efficient algorithm handles the network data traffic of the Internet of Vehicles and enhances the adaptability of the algorithm [42].

Data Availability

The data used to support the findings of this study are available from the author upon request (kusumasyadav0@gmail.com).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] T. Wisanwanichthan and M. Thammawichai, “A double-layered hybrid approach for network intrusion detection system using combined naive Bayes and SVM,” *IEEE Access*, vol. 9, pp. 138432–138450, 2021.

[2] P. Chen, Y. Guo, J. Zhang, Y. Wang, and H. Hu, “A novel preprocessing methodology for DNN-based intrusion detection,” in *Proceedings of the 2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, pp. 2059–2064, Chengdu, China, December 2020.

[3] L. Chen, X. Kuang, A. Xu, S. Suo, and Y. Yang, “A novel network intrusion detection system based on CNN,” in *Proceedings of the 2020 Eighth International Conference on Advanced Cloud and Big Data (CBD)*, pp. 243–247, Taiyuan, China, December 2020.

[4] R. Vijayanand, D. Devaraj, and B. Kannapiran, “A novel deep learning based intrusion detection system for smart meter communication network,” in *Proceedings of the 2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, pp. 1–3, Tamilnadu, India, April 2019.

[5] G. Parimala and R. Kayalvizhi, “An effective intrusion detection system for securing IoT using feature selection and deep learning,” in *Proceedings of the 2021 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–4, Coimbatore, India, January 2021.

[6] G. Karatas, O. Demir, and O. Koray Sahingoz, “Deep learning in intrusion detection systems,” in *Proceedings of the 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)*, pp. 113–116, Ankara, Turkey, December 2018.

[7] P. Shettar, A. V. Kachavimath, M. M. Mulla, and D. G. Narayan, “Intrusion detection system using MLP and chaotic neural networks,” in *Proceedings of the 2021 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–4, Coimbatore, India, January 2021.

[8] H. Zhang, S. Dai, Y. Li, and W. Zhang, “Real-time distributed-random-forest-based network intrusion detection system using Apache Spark,” in *Proceedings of the 2018 IEEE 37th International Performance Computing and Communications Conference (IPCCC)*, pp. 1–7, Orlando, FL, USA, November 2018.

[9] S. V. Siva reddy and S. Saravanan, “Performance evaluation of classification algorithms in the design of Apache Spark based intrusion detection system,” in *Proceedings of the 2020 5th International Conference on Communication and Electronics Systems (ICCES)*, pp. 443–447, Coimbatore, India, June 2020.

[10] A. Dey, “Deep IDS : a deep learning approach for Intrusion detection based on IDS 2018,” in *Proceedings of the 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, pp. 1–5, Dhaka, Bangladesh, December 2020.

[11] P. S. Bhattacharjee, A. K. Md Fujail, and S. A. Begum, “A comparison of intrusion detection by K-means and fuzzy C-means clustering algorithm over the NSL-KDD dataset,” in *Proceedings of the 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, pp. 1–6, Coimbatore, India, December 2017.

[12] N. Moustafa and J. Slay, “UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” in *Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS)*, pp. 1–6, Canberra, ACT, Australia, November 2015.

[13] T. Alladi, V. Kohli, V. Chamola, F. R. Yu, and M. Guizani, “Artificial intelligence (AI)-empowered intrusion detection architecture for the Internet of Vehicles,” *IEEE Wireless Communications*, vol. 28, no. 3, pp. 144–149, 2021.

[14] M. Mahdavisharif, S. Jamali, and R. Fotohi, “Big data-aware intrusion detection system in communication networks: a deep learning approach,” *Journal of Grid Computing*, vol. 19, no. 4, pp. 1–28, 2021.

[15] S. Jamali and R. Fotohi, “DAWA: defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system,” *The Journal of Supercomputing*, vol. 73, no. 12, pp. 5173–5196, 2017.

[16] R. Nair, M. Soni, B. Bajpai, G. Dhiman, and K. M. Sagayam, “Predicting the death rate around the world due to COVID-19 using regression analysis,” *International Journal of Swarm Intelligence Research*, vol. 13, no. 2, pp. 1–13, 2022.

[17] P. K. Vaishnav, S. Sharma, and P. Sharma, “Analytical review analysis for screening COVID-19 disease,” *International Journal of Modern Research*, vol. 1, no. 1, pp. 22–29, 2021.

[18] I. Chatterjee, “Artificial intelligence and patentability: review and discussions,” *International Journal of Modern Research*, vol. 1, no. 1, pp. 15–21, 2021.

[19] R. Kumar and G. Dhiman, “A comparative study of fuzzy optimization through fuzzy number,” *International Journal of Modern Research*, vol. 1, no. 1, pp. 1–14, 2021.

[20] M. Soni, G. Dhiman, B. S. Rajput, P. Rajan, and T. Nitesh Kumar, “Energy-Effective and Secure Data Transfer Scheme for Mobile Nodes in Smart City Applications,” *Wireless Pers Commun*, 2021.

[21] W. Cao, “CNN-based intelligent safety surveillance in green IoT applications,” *China Communications*, vol. 18, no. 1, pp. 108–119, 2021.

[22] M. Ganesan and N. Sivakumar, “IoT based heart disease prediction and diagnosis model for healthcare using machine learning models,” in *Proceedings of the 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*, pp. 1–5, Pondicherry, India, March 2019.

[23] R. Fotohi, S. Firoozi Bari, and M. Yusefi, “Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol,” *International Journal of Communication Systems*, vol. 33, no. 4, Article ID e4234, 2020.

[24] A. Derhab, A. Aldweesh, A. Z. Emam, and F. A. Khan, “Intrusion detection system for Internet of Things based on temporal convolution neural network and efficient feature engineering,” *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 6689134, 16 pages, 2020.

[25] R. Fotohi and S. F. Bari, “A novel countermeasure technique to protect WSN against denial-of-sleep attacks using firefly and Hopfield neural network (HNN) algorithms,” *The Journal of Supercomputing*, vol. 76, pp. 1–27, 2020.

[26] M. Zaminkar and R. Fotohi, “SoS-RPL: securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism,” *Wireless Personal Communications*, vol. 114, 2020.

[27] G. D. L. T. Parra, P. Rad, K. K. R. Choo, and N. Beebe, “Detecting Internet of Things attacks using distributed deep learning,” *Journal of Network and Computer Applications*, vol. 163, Article ID 102662, 2020.

[28] R. Fotohi, E. Nazemi, and F. S. Aliee, “An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks,” *Vehicular Communications*, vol. 26, Article ID 100267, 2020.

[29] M. Roopak, G. Y. Tian, and J. Chambers, “An intrusion detection system against ddos attacks in iot networks,” in *Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0562–0567, IEEE, Las Vegas, NV, USA, January 2020.

[30] T. Alladi, A. Agrawal, B. Gera, V. Chamola, B. Sikdar, and M. Guizani, “Deep neural networks for securing IoT enabled vehicular ad-hoc networks,” in *Proceedings of the ICC 2021-IEEE International Conference on Communications*, pp. 1–6, IEEE, Montreal, QC, Canada, June 2021.

[31] G. Bovenzi, G. Aceto, D. Ciuonzo, V. Persico, and A. Pescapé, “A hierarchical hybrid intrusion detection approach in iot scenarios,” in *Proceedings of the GLOBECOM 2020-2020 IEEE Global Communications Conference*, pp. 1–7, IEEE, Taipei, Taiwan, December 2020.

[32] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, “Kitsune: an ensemble of autoencoders for online network intrusion detection,” 2018, https://arxiv.org/abs/1802.09089.

[33] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, “Hybrid intrusion detection system based on the stacking ensemble of c5 decision tree classifier and one class support vector machine,” *Electronics*, vol. 9, no. 1, p. 173, 2020.

[34] G. J. M. Ariyathilake, M. H. R. Sandeepanie, and P. L. Rupasinghe, “SQL injection detection and prevention solution for web applications,” 2021, http://ir.kdu.ac.lk/handle/345/5253.

[35] A. A. Diro and N. Chilamkurti, “Distributed attack detection scheme using deep learning approach for Internet of Things,” *Future Generation Computer Systems*, vol. 82, pp. 761–768, 2018.

[36] G. Bovenzi, G. Aceto, D. Ciuonzo, V. Persico, and A. Pescapé, “A big data-enabled hierarchical framework for traffic classification,” *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2608–2619, 2020.

[37] G. Aceto, D. Ciuonzo, A. Montieri, V. Persico, and A. Pescapé, “Know your big data trade-offs when classifying encrypted mobile traffic with deep learning,” in *Proceedings of the 2019 Network traffic measurement and analysis conference (TMA)*, pp. 121–128, IEEE, Paris, France, June 2019.

[38] Z. S. Alwan and M. F. Younis, “Detection and prevention of SQL injection attack: a survey,” *International Journal of Computer Science and Mobile Computing*, vol. 6, no. 8, pp. 5–17, 2017.

[39] M. Nasereddin, A. ALKhamaiseh, M. Qasaimeh, and R. Al-Qassas, “A systematic review of detection and prevention techniques of SQL injection attacks,” *Information Security Journal: A Global Perspective*, pp. 1–14, 2021.

[40] V. Hajisalem and S. Babaie, “A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection,” *Computer Networks*, vol. 136, pp. 37–50, 2018.

[41] R. Fotohi and H. Pakdel, “A lightweight and scalable physical layer attack detection mechanism for the internet of things (IoT) using hybrid security schema,” *Wireless Personal Communications*, vol. 119, pp. 1–18, 2021.

[42] M. Lei, X. Li, B. Cai, Y. Li, L. Liu, and W. Kong, “P-DNN: an effective intrusion detection method based on pruning deep neural network,” in *Proceedings of the 2020 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–9, Glasgow, UK, July 2020.