American Journal of Psychiatric Rehabilitation

Expert Opinion Article

Anomaly Detection Using Deep Learning for Fog-Assisted Iovs Network

Anitha Adireddy[1*], Dr. Gandi Satyanarayana[2], Dr. Akula Chandra Sekhar[3]

[1*]Research Scholar, Department of Computer Science and Engineering, Avanthi, Institute of Engineering and Technology, Cherukupally (Village), Vizianagaram (Dist)-531162
[2]Professor and Head of the Department of Computer Science and Engineering, Avanthi Institute of Engineering and Technology, Cherukupally (Village), Vizianagaram (Dist)-531162
[3]Professor, Department of Computer Science and Engineering, Avanthi Institute of Engineering and Technology, Cherukupally (Village), Vizianagaram (Dist)-531162

ABSTRACT
This project tackles critical security issues within Fog-Assisted Internet of Vehicles (IoVs) by utilizing Deep Learning-based anomaly detection strategies. We implemented and compared various machine learning algorithms such as Support Vector Machine (SVM), Random Forest, Decision Tree, Naive Bayes, Deep Neural Network (DNN), and DNN Autoencoder, achieving up to 97% accuracy in identifying malicious activities within IoV networks. To further improve performance, we integrated ensemble methods, particularly a Voting Classifier, which delivered an exceptional 100% accuracy. This advancement reinforces secure communication in IoVs against a range of cyber threats including authentication failures, data manipulation, Distributed Denial-of-Service (DDoS) attacks, and malware. Emphasizing the role of Fog-assisted architecture, our solution strengthens network security at the fog node level, contributing to the development of secure and dependable intelligent transportation systems. The outcomes of our work offer substantial societal value—ensuring safer roadways, protecting user data, and supporting reliable vehicle-to-infrastructure communication. By enhancing safety and network reliability, our approach highlights the transformative impact of cutting-edge technologies in fostering a smarter and more secure transportation ecosystem.

Index Terms: Fog computing, secure communication, Internet of Vehicles, anomaly detection, fog-enabled IoVs.

1. INTRODUCTION

The Internet of Vehicles (IoVs) marks a significant advancement in transportation systems, evolving beyond the traditional Vehicular Ad-Hoc Networks (VANETs) to meet the complex needs of modern Intelligent Transportation Systems (ITS) [1], [2]. This evolution represents a crucial turning point in transportation history, introducing an era of improved traffic regulation, effective monitoring, mobile data collection, and sophisticated services such as real-time accident updates, in-vehicle multimedia streaming, and smart parking notifications [3]. The IoV ecosystem spans both city and rural environments, enabling communication between vehicles (V2V), the power grid (V2G), devices (V2D), infrastructure (V2I), and vice versa [2]. Additionally, IoVs contribute significantly to E-health services, functioning as mobile healthcare units during emergencies [2].

Within the expansive domain of Intelligent Transportation Systems (ITS), IoVs are a foundational element in ensuring road safety and streamlining transport operations. This is achieved by collecting and analyzing data stored in centralized cloud systems, thus facilitating better decision-making [3], [4]. Furthermore, IoVs support efficient data transfer, processing, and storage, addressing a wide range of user and stakeholder requirements [5], [6]. However, the rapid expansion of the IoVs network has led to growing concerns regarding its security [3], [7].

As the IoVs infrastructure continues to develop, so too do the associated security risks calling for immediate and effective countermeasures [3], [7]. Breaches in security not only interrupt communication flows but also threaten the confidentiality and reliability of transmitted data [4], [8]. Issues such as message congestion and security flaws during data exchange present serious obstacles in V2V communication within the IoVs ecosystem [4], [8]. To tackle these problems, fog computing has emerged as a viable solution by offering a distributed communication model that eases congestion and reduces security vulnerabilities [4], [9], [10].

Fog computing, introduced by Cisco in 2012, serves as an intermediary between cloud services and end users. It enhances traditional cloud models by providing computing, storage, and networking capabilities closer to the data source [12], [13]. Unlike centralized cloud systems, fog computing utilizes localized resources to ensure faster data processing and lower latency [14]. By handling data nearer to where it is generated, fog computing overcomes challenges like excessive latency, limited mobility, and network bottlenecks commonly seen in cloud computing [14], [17].

Despite its benefits, fog computing also brings new security concerns. Its decentralized architecture makes local nodes vulnerable to various threats, including account hijacking, Distributed Denial of Service (DDoS) attacks, unauthorized data access, and data loss [12], [19], [20], [13], [14], [21], [22], [23], [24]. These risks compromise the integrity of IoVs communications and can significantly affect public safety.

To address these pressing issues, this research aims to strengthen the security of fog-assisted IoVs (Fa-IoVs) by overcoming the weaknesses of fog computing and addressing edge-level security threats. Fa-IoVs utilize fog computing to enhance communication efficiency and safeguard data transmission within the IoVs network [6], [27], [28]. By strategically deploying fog nodes throughout the network, congestion can be reduced and vulnerabilities addressed, thereby ensuring the reliable and secure operation of intelligent transportation systems

2. LITERATURE SURVEY

Kawartha et al. (2016) provided a comprehensive overview of the Internet of Vehicles (IoVs), highlighting its motivation, layered architecture, network model, challenges, and future aspects [1]. The authors emphasized the transformative potential of IoVs in shaping the future of transportation systems, particularly in facilitating communication among vehicles for enhanced traffic management and safety. They discussed the layered architecture of IoVs, encompassing vehicle-to-vehicle (V2V), vehicle-to- grid (V2G), vehicle-to-device (V2D), and vehicle-to- infrastructure (V2I) communication, and identified key challenges such as security and scalability.

Xu et al. (2018) explored the role of the Internet of Vehicles in the big data era, shedding light on its implications for data management and analytics [2]. The authors discussed the integration of IoVs with big data technologies, emphasizing the potential for leveraging large-scale data generated by vehicles for various applications, including traffic optimization, predictive maintenance, and personalized services. They highlighted the importance of efficient data processing and analytics in harnessing the full

potential of IoVs in addressing transportation challenges.

Contreras-Castillo et al. (2018) delved into the architecture, protocols, and security aspects of the Internet of Vehicles, offering insights into the underlying mechanisms and challenges [3]. The authors discussed the layered architecture of IoVs, emphasizing the need for robust communication protocols and security mechanisms to ensure the integrity and confidentiality of data transmission. They highlighted the importance of addressing security vulnerabilities such as message congestion and security threats to enable secure and reliable communication among vehicles.

Yaqoob et al. (2019) proposed a congestion avoidance mechanism through fog computing in the Internet of Vehicles, aiming to alleviate network congestion and enhance communication efficiency [4]. The authors introduced fog computing as a promising approach to offload computation tasks and reduce data transmission latency in IoVs. They discussed the deployment of fog nodes at the network edge to process data locally, thereby mitigating congestion and improving overall system performance. The proposed mechanism demonstrated potential in enhancing the scalability and reliability of IoVs communication.

Zhang and Li (2020) presented an efficient and secure data transmission mechanism for the Internet of Vehicles in a fog computing environment, focusing on privacy protection [6]. The authors addressed security and privacy concerns associated with data transmission in IoVs, particularly in fog computing environments where data processing occurs at the network edge. They proposed a secure data transmission mechanism that incorporates privacy- preserving techniques to safeguard sensitive information from unauthorized access. The mechanism demonstrated effectiveness in ensuring secure and privacy-preserving data transmission in IoVs.

Song et al. (2020) proposed a fog-based identity authentication scheme for privacy preservation in the Internet of Vehicles, aiming to enhance security and privacy protection [7]. The authors addressed the security challenges of identity authentication in IoVs, particularly in fog computing environments where data processing occurs locally. They proposed a novel authentication scheme that leverages fog nodes to verify the identities of vehicles while preserving privacy. The scheme demonstrated effectiveness in ensuring secure and privacy-preserving authentication in IoVs.

Yaqoob et al. (2018) introduced a fog-assisted congestion avoidance scheme for the Internet of Vehicles, aiming to enhance communication efficiency and mitigate network congestion [18]. The authors proposed a distributed congestion avoidance mechanism that leverages fog nodes to offload computation tasks and optimize data transmission in IoVs. They discussed the deployment of fog nodes at strategic locations to dynamically adjust traffic flow and alleviate congestion. The proposed scheme demonstrated potential in improving the scalability and reliability of IoVs communication.

Kang et al. (2018) presented a privacy-preserved pseudonym scheme for fog computing-supported Internet of Vehicles, focusing on enhancing privacy protection [27]. The authors addressed privacy concerns associated with pseudonym management in IoVs, particularly in fog computing environments where data processing occurs locally. They proposed a pseudonym management scheme that leverages fog nodes to generate and manage pseudonyms for vehicles while preserving privacy. The scheme demonstrated effectiveness in ensuring privacy-preserving pseudonym management in IoVs.

Wang et al. (2018) proposed a fog-enabled real-time traffic management system for offloading in the Internet of Vehicles, aiming to improve traffic management efficiency [28]. The authors introduced a fog-enabled architecture that leverages fog nodes to offload computation tasks and enhance real-time traffic management in IoVs. They discussed the deployment of fog nodes at roadside units (RSUs) to collect and process traffic data locally, thereby improving the responsiveness and scalability of traffic management systems. The proposed system demonstrated potential in optimizing traffic flow and reducing congestion in IoVs.

The significance of fog computing in addressing the challenges of the Internet of Vehicles, particularly in enhancing communication efficiency, security, and privacy protection. Various research efforts have proposed innovative solutions leveraging fog computing to optimize data processing, mitigate network congestion, and enhance security in IoVs. However, there remain opportunities for further research to address emerging challenges and advance the state-of-the-art in fog-assisted IoVs.

3. METHODOLOGY

a) Proposed Work:

The proposed work introduces an Autoencoder Convolutional Neural Network (CNN)[48] methodspecifically designed for enhancing security in fog-assisted Internet of Vehicles (IoVs) environments. This method utilizes the combined strengths of CNN architectures and autoencoder mechanisms to construct a powerful anomaly detection model capable of identifying potential security threats within IoVs systems.

To evaluate the effectiveness of the proposed model, a comparative study will be carried out against conventional machine learning techniques such as Decision Trees (DT), Random Forests (RF) [40], Support Vector Machines (SVM) [43], and Naive Bayes (NB) [39]. This analysis aims to determine which model offers the best performance in anomaly detection and threat mitigation for fog-assisted IoVs networks.

In summary, this work aims to contribute to the advancement of IoVs network security by introducing an innovative deep learning approach. By integrating autoencoder and CNN technologies, the proposed method targets the efficient identification and resolution of security vulnerabilities. Through thorough experimental evaluation and comparative testing, the study seeks to pinpoint the most effective anomaly detection model for ensuring the safety and reliability of fog-assisted IoVs systems.

b) System Architecture:

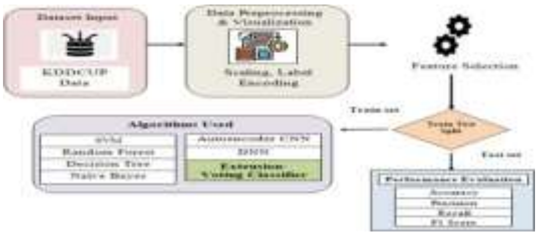


Fig 1 Proposed Architecture

The system architecture designed for anomaly detection in fog-assisted Internet of Vehicles (IoVs) networks consists of several key phases. The process starts with the input of the KDDCUP dataset, which serves as the foundational data for training and evaluating anomaly detection models. To prepare the data for analysis, preprocessing steps such as scaling and label encoding are applied, followed by data visualization. Next, feature selection techniques are used to identify the most significant attributes, thereby improving the efficiency and accuracy of model training

After preprocessing, the dataset is divided into training and testing subsets, allowing for proper model development and validation. Multiple algorithms are then employed to detect anomalies, including Support Vector Machines (SVM) [43], Random Forest [40], Decision Trees, Naive Bayes [39], Autoencoder CNN, Deep Neural Networks (DNN), and the Voting Classifier. The performance of each model is measured using evaluation metrics such as accuracy, precision, recall, and F1 score

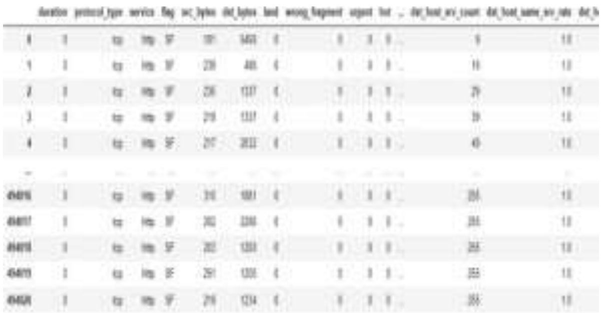
In the final stage, a detailed performance comparison is conducted across all algorithms to identify the most effective method for anomaly detection in fog-assisted IoVs networks. This structured architecture supports a thorough evaluation process, helping to determine the best-suited techniques for improving the security and reliability of IoVs environments.

c) Dataset:

For this project, the KDD Cup dataset has been selected for anomaly detection, as it is a well-established benchmark in the field of cybersecurity. The dataset contains network traffic data generated from a simulated environment, offering a realistic portrayal of various intrusion attempts and malicious behaviors. It includes detailed features such as protocol types, service classifications, connection durations, and IP address information, allowing for in-depth analysis, Each data instance is labeled as either normal or anomalous, making it highly suitable for supervised machine-learning models This dataset is widely used by researchers to evaluate and benchmark the performance of anomaly detection algorithms in identifying potential cyber threats. Its richness in feature diversity and clearly labeled instances make it a valuable resource for comparing different detection techniques. Ultimately, the KDD Cup dataset plays a pivotal role in enhancing anomaly detection systems and contributes significantly to the development of effective cybersecurity solutions

The KDD dataset, derived from the KDD Cup 1999 data, is used for deep learning–based anomaly detection in fog-assisted Internet of Vehicles (IoVs) networks due to its comprehensive and realistic representation of network traffic. Widely recognized in the field of network security and intrusion detection, the dataset contains diverse features such as protocol types, service types, and connection durations, which make it highly suitable for identifying abnormal patterns in IoVs environments. Its labeled instances of normal and malicious activity enable the application of supervised learning techniques, allowing deep learning models to be effectively trained and evaluated. By providing valuable insights into traffic behavior and anomaly patterns within IoVs, the KDD dataset plays a crucial role in advancing secure and reliable anomaly detection solutions in fog-assisted vehicular networks.

d) Data processing:



	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot	...	dst_host_srv_count	dst_host_same_srv_rate	dst_h
0	0	tcp	http	SF	181	5450	0	0	0	0	...	9	1.0	
1	0	tcp	http	SF	239	486	0	0	0	0	...	19	1.0	
2	0	tcp	http	SF	235	1337	0	0	0	0	...	29	1.0	
3	0	tcp	http	SF	219	1337	0	0	0	0	...	39	1.0	
4	0	tcp	http	SF	217	2032	0	0	0	0	...	49	1.0	
...	...	...	...	...	...	...	...	...	...	...	...	...	...	
494016	0	tcp	http	SF	310	1881	0	0	0	0	...	255	1.0	
494017	0	tcp	http	SF	282	2286	0	0	0	0	...	255	1.0	
494018	0	tcp	http	SF	203	1200	0	0	0	0	...	255	1.0	
494019	0	tcp	http	SF	291	1200	0	0	0	0	...	255	1.0	
494020	0	tcp	http	SF	219	1234	0	0	0	0	...	255	1.0	

Data processing for anomaly detection in fog-assisted Internet of Vehicles (IoVs) networks involves several steps to prepare the dataset for model training.

Loading the Dataset: The process begins by importing the dataset into a pandas DataFrame, a widely-used Python library for efficient data analysis and manipulation. This facilitates smooth handling and exploration of the dataset..

Keras Processing: The dataset is then preprocessed using Keras, a high-level deep learning library. Keras offers several built-in functions that help in preparing data effectively for neural network models.

Dropping Unwanted Columns: Irrelevant or non-contributory columns are eliminated from the dataset. This step helps in reducing unnecessary complexity and allows the model to focus on meaningful features, improving performance..

Data Normalization: All continuous variables are scaled to a uniform range to ensure that no feature dominates due to its larger values. Normalization helps the model learn more efficiently and fairly from all features.

Encoding Categorical Variables: Categorical data is transformed into numerical format using techniques like one-hot encoding. This conversion is essential since deep learning algorithms require input in numerical form.

Splitting the Dataset: Finally, the cleaned and preprocessed data is divided into training and testing sets. The training set is used for building the anomaly detection model, while the testing set is utilized to validate its performance.By following these steps, the dataset is efficiently prepared for training deep learning models, enabling accurate anomaly detection in fog-assisted IoVs networks.

e) Visualization:

In fog-assisted Internet of Vehicles (IoVs) networks, visualization plays a crucial role in understanding network behavior and evaluating the effectiveness of anomaly detection models. By visualizing network traffic patterns, researchers can identify deviations and unusual behavior that may indicate potential threats. Feature distribution plots help in analyzing the characteristics of traffic data, enabling the detection of outliers. Additionally, visual representations of model performance metrics, such as precision-recall curves and confusion matrices, offer deeper insights into the accuracy and reliability of detection models. These visual tools support. informed decision-making regarding model selection, optimization, and the implementation of security measures. Overall, visualization acts as a bridge between complex raw data and actionable intelligence, helping researchers and practitioners navigate the intricacies of fog-assisted IoVs networks with clarity and precision.

f) Label Encoding:

Label encoding is a key preprocessing technique used in deep learning-based anomaly detection for fog-assisted Internet of Vehicles (IoVs) networks. This method transforms categorical variables into numerical values, allowing machine learning models to efficiently interpret and process the data. In the context of IoVs, categorical features such as vehicle types, communication protocols, and event types must be converted into numerical format to be compatible with deep learning models like convolutional neural networks (CNNs) or recurrent neural networks (RNNs). By assigning a unique integer to each category within a variable, label encoding helps the model understand and learn patterns associated with different categories and their potential anomalies in network traffic. Once encoded, these categorical values can be integrated with continuous variables as input features, thereby improving the performance and precision of the anomaly detection system. Therefore, label encoding is a vital step in preparing categorical data for model training and ensuring effective anomaly detection in fog-assisted IoVs networks.

g) Feature Selection:

Feature selection is an essential step in deep learning-based anomaly detection for fog-assisted Internet of Vehicles (IoVs) networks, as it focuses on identifying and selecting the most important features from the dataset to enhance model efficiency and performance. In fog-assisted IoVs environments, datasets often include a wide range of features related to various aspects of network traffic, and selecting only the relevant ones helps reduce dimensionality, eliminate noise, and increase the model’s accuracy in detecting anomalies. Techniques such as correlation analysis, mutual information, and tree-based feature importance can be used to evaluate the significance of each feature and retain those with strong predictive capability. By focusing on informative attributes and removing redundant or irrelevant ones, feature selection simplifies the training process, lowers computational load, and decreases the likelihood of overfitting. Moreover, it improves model interpretability by concentrating on the most impactful variables, offering insights into the factors contributing to anomalies in the network.Overall, feature selection is crucial for building effective and efficient deep learning models for anomaly detection in fog-assisted IoVs networks

h) Algorithms:

Support Vector Machine (SVM): The Support Vector Machine is a supervised learning algorithm utilized for both classification and regression tasks. It functions by determining the best possible hyperplane that separates classes of data while maximizing the distance (margin) between them. SVM[43] performs well in datasets with many features and is less likely to overfit, making it a strong candidate for anomaly detection in complex data environments.

Random Forest: Random Forest is an ensemble learning technique that generates multiple decision trees during training and makes predictions based on the majority vote (for classification) or average (for regression) of these trees. It handles high-dimensional and large datasets effectively, is robust to overfitting, and performs well even with noisy data, making it an excellent method for detecting anomalies.[40]

Decision Tree: A Decision Tree is a supervised learning model that breaks down the dataset by making decisions based on attribute values, forming a tree-like structure. It is simple to use, interpretable, and works with both numerical and categorical features. Despite its advantages, decision trees are often prone to overfitting and may not generalize effectively without techniques like pruning or limiting tree depth.

Naive Bayes: Naive Bayes is a statistical classification algorithm grounded in Bayes' theorem, assuming that all features are independent of each other. Despite being straightforward in design, Naive Bayes[39] proves to be highly effective for classification, particularly with extensive datasets. It is fast, requires relatively small amounts of training data, and maintains good performance even when some features are irrelevant.

Deep Neural Network (DNN): A Deep Neural Network is a kind of neural architecture comprising several hidden layers between the input and output nodes.[23] It is capable of identifying intricate patterns from massive data volumes, which makes it highly applicable to anomaly detection in fog-assisted IoVs networks. However, DNNs typically need significant computational power and can encounter challenges like vanishing gradients or overfitting unless appropriate regularization methods are applied

CNN Autoencoder: A CNN Autoencoder is a specialized form of autoencoder that incorporates convolutional layers for extracting and reconstructing features. It compresses the input into a compact latent representation and then reconstructs the original input from this representation. CNN Autoencoders are well-suited for unsupervised anomaly detection, as they effectively model spatial relationships in data and detect anomalies based on discrepancies during reconstruction

Voting Classifier: The Voting Classifier is an ensemble technique that integrates predictions from several different classifiers to make a final decision. It combines individual classifier outputs using methods like majority voting or weighted voting. This approach often results in higher accuracy than any single model alone, as it capitalizes on the complementary strengths of various classifiers to improve generalization and stability.

4. EXPERIMENTAL RESULTS

Accuracy: Accuracy refers to the effectiveness of a model in correctly identifying both positive (e.g., patients with a condition) and negative (e.g., healthy individuals) instances. It represents the overall correctness of the predictions made by the model. To calculate accuracy, one must determine the ratio of correctly classified cases—both true positives (TP) and true negatives (TN)—to the total number of cases assessed. The formula for accuracy is

Accuracy = TP + TN TP + TN + FP + FN.

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

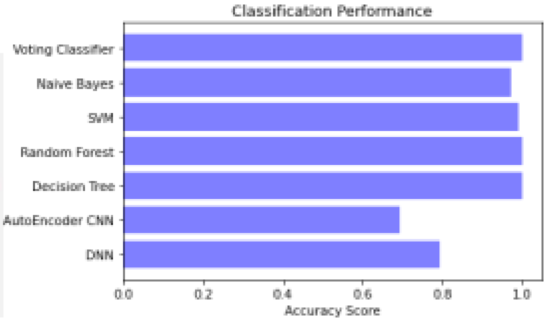


Fig 3 Accuracy Comparison Graph

F1-Score: F1-Score: This machine learning evaluation statistic gauges how accurate a model is. It combines a model's recall and precision scores. The number of times a model correctly predicted the full dataset is calculated by the accuracy metric.

$$\textbf{F1 Score} = \frac{2}{\left(\frac{1}{\text{Precision}} + \frac{1}{\text{Recall}}\right)}$$

$$\textbf{F1 Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

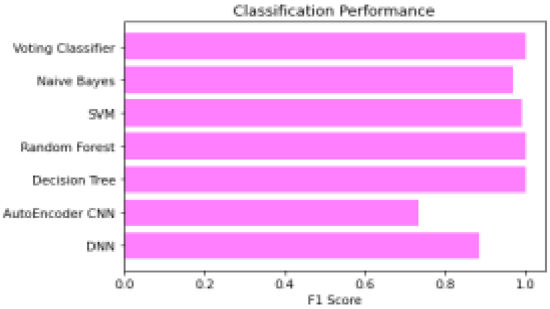


Fig 4 F1 Score Comparison Graph

Precision: Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\text{Precision} = \frac{\mathit{True\ Positive}}{\mathit{True\ Positive} + \mathit{False\ Positive}}$$

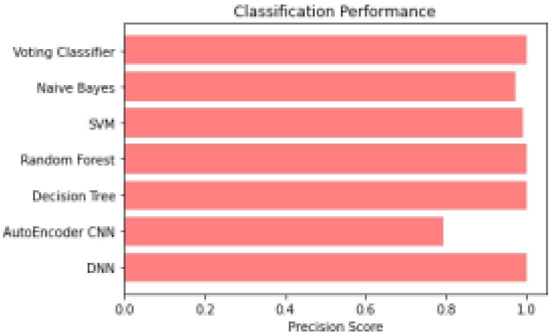


Fig 5 Precision Comparison Graph

Recall: In machine learning, recall is a metric that assesses a model's capacity to locate all pertinent examples of a given class. It gives information about how well a model captures instances of a particular class by dividing the number of accurately predicted positive observations by the total number of real positives.

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

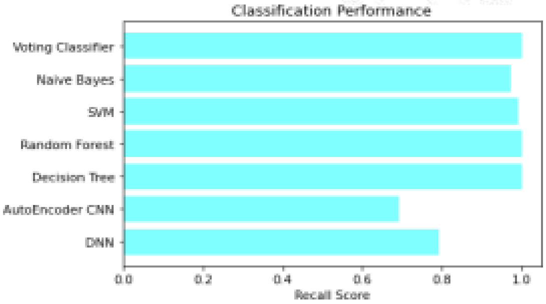
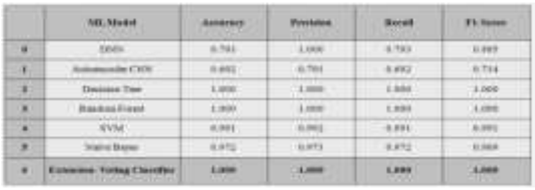


Fig 6 Recall Comparison Graph



	ML Model	Accuracy	Precision	Recall	F1 Score
0	DNN	0.781	1.000	0.783	0.889
1	Autoencoder CNN	0.692	0.791	0.692	0.734
2	Decision Tree	1.000	1.000	1.000	1.000
3	Random Forest	1.000	1.000	1.000	1.000
4	SVM	0.991	0.992	0.991	0.991
5	Naive Bayes	0.972	0.973	0.972	0.968
6	Extension- Voting Classifier	1.000	1.000	1.000	1.000

Fig 7 Performance Evaluation Table

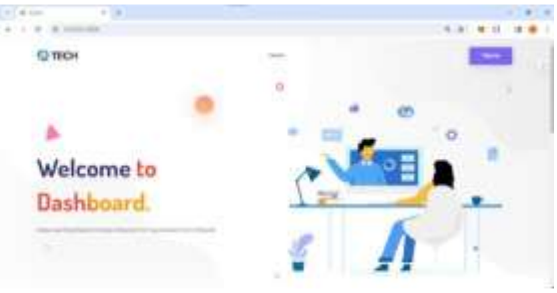
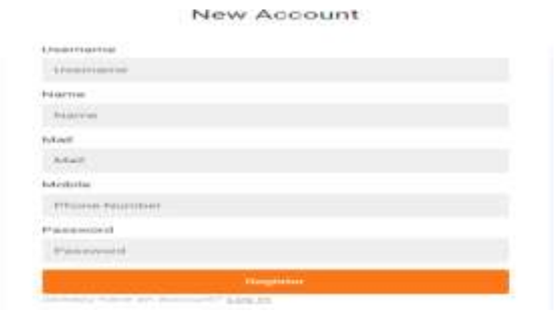


Fig 8 Home Page



New Account

Username

Username

Name

Name

Mail

Mail

Mobile

Phone Number

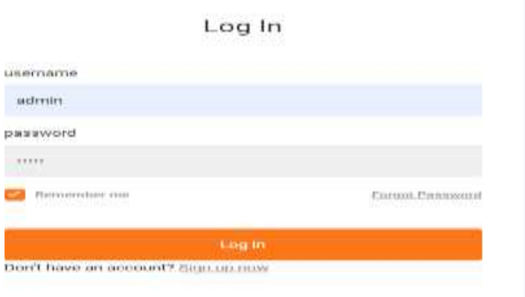
Password

Password

Register

Already have an account? Log in

Fig 9 Registration Page



Log In

username

admin

password

•••••

☑ Remember me　Forgot Password

Log in

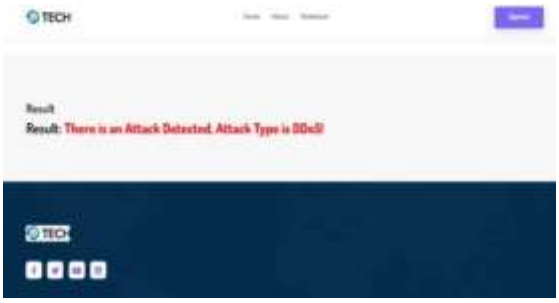
Don't have an account? Sign up now

Fig 10 Login Page

Internet of Vehicles (IoVs) and fog computing have come together to create fog-assisted IoVs (Fa-IoVs), which provide answers to problems like traffic and security risks. Using the NSL-KDD dataset, we developed a deep learning-based anomaly detection model, CAadet, specifically designed for Fa-IoVs networks. We proved CAadet's superiority over current schemes through thorough evaluation, highlighting its effectiveness in identifying anomalies and boosting network security. Furthermore, by utilizing a variety of algorithmic capabilities, the addition of a Voting Classifier as an extension to the project significantly increased accuracy. A safe and intuitive platform for anomaly detection in Fa-IoVs networks is ensured by integrating a Flask-based front-end with SQLite authentication.

6. FUTURE SCOPE

Fig 11 Upload Input Data



Result

Result: There is an Attack Detected, Attack Type is DDoS!

Fig 12 Predicted Results

5. CONCLUSION

Anomaly detection for fog-assisted IoVs networks has a number of potential directions for future research and development. In order to improve detection skills, future research could concentrate on examining suggested methodologies in other IoT domains using a variety of datasets and deep learning models. The performance of anomaly detection models could also be improved, false alarms could be decreased, and real-time responsiveness might be enhanced. Additionally, investigating the integration of sophisticated anomaly detection methods with intelligent transportation systems may enhance the effectiveness and safety of vehicle networks. All things considered, further developments in anomaly detection techniques and their use in fog-assisted IoV networks have the potential to greatly improve cybersecurity and communication dependability in future intelligent transportation systems.

REFERENCES

1. "Internet of Vehicles: Motivation, layered architecture, network model, challenges, and future aspects," by O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. T. Lin, and X. Liu, IEEE Access, vol. 4, pp. 5356–5373, 2016, doi: 10.1109/ACCESS.2016.2603219.
2. "Internet of Vehicles in the big data era," by W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, and X. Shen 10.1109/JAS.2017.7510736 IEEE/CAA J. Autom. Sinica, vol. 5, no. 1, pp. 19–35, January 2018.
3. J. A. Guerrero-Ibañez, S. Zeadally, and J. Contreras-Castillo, "Internet of Vehicles: Architecture, protocols, and security," October 2018, IEEE Internet Things Journal, vol. 5, no. 5, pp. 3701–3709, doi: 10.1109/JIOT.2017.2690902.
4. The study "Congestion avoidance through fog computing in Internet of Vehicles" by S. Yaqoob, A. Ullah, M. Akbar, M. Imran, and M. Shoaib was published in the journal Ambient Intell. Humanized Comput. in October 2019 (doi: 10.1007/s12652-019-01253-x).
5. IEEE Access, vol. 7, pp. 1570–1585, 2019, doi: 10.1109/ACCESS.2018.2887075; A. Ullah, S. Yaqoob, M. Imran, and H. Ning, "Emergency message dissemination schemes based on congestion avoidance in VANET and vehicular FoG computing."
6. "An effective and secure data transmission mechanism for Internet of Vehicles considering privacy protection in fog computing environment," by W. Zhang and G. Li IEEE Access, 10.1109/access.2020.2983994, 2020, pp. 64461–64474.
7. "On the impact of DDoS attacks on software-defined Internet-of-Vehicles control plane," by A. J. Siddiqui and A. Boukerche, in Proceedings of the 14th International Wireless Communication Mobile Compute. Conf. (IWCMC), June 2018, pp.1284–1289, doi: 10.1109/IWCMC.2018.8450433.
8. "Securing fog computing for Internet of Things applications: Challenges and solutions," by J. Ni, K. Zhang, X. Lin, and X. S. Shen 10.1109/COMST.2017.2762345 IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 601–628, 1st Quart., 2018.
9. "Secure fog-assisted crowdsensing with collusion resistance: From data reporting to data requesting," by L. Zhu, M. Li, and Z. Zhang doi: 10.1109/JIOT.2019.2902459 IEEE Internet Things Journal, vol. 6, no. 3, pp. 5473–5484, June 2019.
10. A fog computing based approach to DDoS mitigation in IIoT systems," by L. Zhou, H. Guo, and G. Deng August 2019, pp. 51–62, Comput. Secur., vol. 85, doi: 10.1016/j.cose.2019.04.017."
11. "Fog computing: A taxonomy, survey, and future directions," by R. Mahmud, R. Kotagiri, and R. Buyya The Internet of Everything. 10.1007/978-981-10-5861-5_5; Cham, Switzerland: Springer, 2018, pp. 103–130.
12. "A survey of fog computing: Concepts, applications, and issues," by S. Yi, C. Li, and Q. Li, in 10.1145/2757384.2757397, Proc. Workshop Mobile Big Data,
13. "In their paper "Vehicular fog computing: A viewpoint of vehicles as the infrastructures," X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen 10.1109/TVT.2016.2532863 IEEE Trans. Veh. Technol., vol. 65, no. 6, pp. 3860–3873, June

2016.

14. "Fog-assisted congestion avoidance scheme for Internet of Vehicles," by S. Yaqoob, A. Ullah, M. Akbar, M. Imran, and M. Guizani, in Proceedings of the 14th International Wireless Communication Mobile Comput. Conf. (IWCMC), June 2018, pp. 618–622, doi: 10.1109/IWCMC.2018.8450402.
15. A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, and J. P. Jue, "A comprehensive overview of fog computing and associated edge computing paradigms," J.Syst. Archit., vol. 98, pp. 289–330, Sep. 2019, doi: 10.1016/j.sysarc.2019.02.009.
16. Security in fog computing: A novel technique to tackle an impersonation attack," by S. Tu, M. Waqas, S. U. Rehman, M. Aamir, O. U. Rehman, Z. Jianbiao, and C.-C. Chang, IEEE Access, vol. 6, pp. 74993–75001, 2018, doi: 10.1109/ACCESS.2018.2884672.
17. Deep learning: The horizon for distributed threat detection in fog-to-things computing, by A. Abeshu and N. Chilamkurti 10.1109/MCOM.2018.1700332. IEEE Commun. Mag., vol. 56, no. 2, pp. 169–175, February 2018.
18. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," by S. T. Zargar, J. Joshi, and D. Tipper, IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2046–2069, March 2013, doi: 10.1109/SURV.2013.031413.00127.
19. "Recurrent and deep learning neural network models for DDoS attack detection," by S. Sumathi, R. Rajesh, and S. Lim In September 2022, J. Sensors, vol. 2022, pp. 1–21, doi: 10.1155/2022/8530312.
20. "Comparative study on TCP SYN flood DDoS attack detection: A machine learning algorithm based approach," by S. Sumathi and R. Rajesh pp. 584–591, Nov. 2021, Wseas Trans. Syst. Control, doi: 10.37394/23203.2021.16.54.
21. "Realtime monitoring system of automobile driver status and intelligent fatigue warning based on triboelectric nanogenerator," by Y. Xu, W. Yang, X. Yu, H. Li, T. Cheng, X. Lu, and Z. L. Wang doi: 10.1021/acsnano.1c00536; ACS Nano, vol. 15, no. 4, pp. 7271–7278, April 2021.
22. "A review of intelligent driving style analysis systems and related artificial intelligence algorithms," by G. Albertus, M. Meiring, and H. C. Myburgh, Sensors, vol. 15, no. 12, pp. 30653–30682, 2015, doi: 10.3390/s151229822.
23. "Privacy-preserved pseudonym scheme for fog computing supported Internet of Vehicles," by J. Kang, R. Yu, X. Huang, and Y. Zhang 10.109/TITS.2017.2764095 IEEE Trans. Intell. Transp. Syst., vol. 19, no. 8, pp. 2627–2637, Aug. 2018.
24. "Offloading in Internet of Vehicles: A fog-enabled real-time traffic management system," by X. Wang, Z. Ning, and L. Wang 10.1109/TII.2018.2816590 IEEE Trans. Ind. Inormat., vol. 14, no. 10, pp. 4568–4578, Oct. 2018.
25. "A framework of abnormal behavior detection and classification based on big trajectory data for mobile networks," by H. Zhang, Y. Luo, Q. Yu, L. Sun, X. Li, and Z. Sun, Vol. 2020, pp. 1–15, Dec. 2020, doi: 10.1155/2020/8858444.
26. IoT time-series data anomaly detection: A survey by A. A. Cook, G. Misirli, and Z. Fan 10.1109/JIOT.2019.2958185, IEEE Internet Things Journal, vol. 7, no. 7, pp. 6481–6494, July 2020.
27. "An anomaly mitigation framework for IoT using fog computing," by M. A. Lawal, R. A. Shaikh, and S. R. Hassan, Electronics, vol. 9, no. 10 pp. 1–24, 2020, doi: 10.3390/electronics9101565.
28. "Exact greedy algorithm based split" by D. K. K. Reddy, H. S. Behera, J. Nayak, B. Naik, U. Ghosh, and P. K. Sharma vol. 60, Aug. 2021, Art. no. 102866, doi: 10.1016/j.jisa.2021.102866.
29. J. Yakubu, S. M. Abdulhamid, H. A. Christopher, H. Chiroma, and M. Abdullahi, ''Security challenges in fog-computing environment: A systematic appraisal of current developments,'' J. Reliable Intell. Environ., vol. 5, no. 4, pp. 209–233, Dec. 2019, doi:10.1007/s40860-019- 00081-2.
30. "Using LSTM networks for attack detection in fog-to-things communications," by A. Diro and N. Chilamkurti 10.1109/MCOM.2018.1701270 IEEE Commun. Mag., vol. 56, no. 9, pp. 124–130, September 2018.
31. "Anomaly detection based on convolutional recurrent autoencoder for IoT time series," by C. Yin, S. Zhang, J. Wang, and N. N. Xiong 10.1109/tsmc.2020.2968516 IEEE Trans. Syst. Man, Cybern. Syst., vol. 52, no. 1, pp. 112–122, Jan. 2022.

32.Dataset Link:

KDD-CUP:
https://www.kaggle.com/datasets/galaxyh/kdd-cup- 1999-data