IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

DETECTING FOG-ASSISTED IOVS NETWORK ANOMALIES USING DEEP LEARNING

B AJITH KUMAR[1], ALLAGADDA LEELASAI[2], A DHANASEKHAR REDDY[3], G DAKSHAYANI[4]
[1]Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: ajithkumaryadav34@gmail.com
[2]P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: allagaddasai55@gmail.com
[3]Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: dhanasekhar918@gmail.com
[4]Assistant Professor, Department of CSE, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email:gdakshayani9@gmail.com

Abstract: Our review involves Deep Learning to detect anomalies in Fog-Assisted IoVs to further develop security. We recognized IoVs network attacks with 97% accuracy utilizing SVM, Random Forest, Decision Tree, Naive Bayes, DNN, and DNN Autoencoder. We added ensemble draws near, for example, the Voting Classifier, which accomplished 100 percent accuracy. This overhaul safeguards against validation breaks, information trustworthiness concerns, DDoS attacks, and malware dangers by further developing correspondence. Our work fortifies IoVs network security and addresses neighborhood haze hub weaknesses with Fog-Assisted layers to make trustworthy and safe wise transportation frameworks. Our endeavors lead to get information move, upgraded street wellbeing, and reliable astute transportation administrations for clients, IoV proprietors, and society. Our methodology underlines the significance of refined innovation in making transportation more secure and more effective by diminishing auto collisions and further developing correspondence.

Index Terms: Fog computing, smooth communication, Internet of Vehicles, anomaly detection, fogassisted IoVs.

1. INTRODUCTION

Internet of Vehicles (IoVs) developed from Vehicular Ad-Hoc Networks (VANETs) to suit the necessities of an inexorably mind boggling clever transportation framework (ITS) [1], [2]. This change introduces another period of traffic the board, effective observing, versatile detecting, and complex administrations like leaving alerts, sound/video web based in vehicles, and continuous mishap detailing [3]. The IoVs ecosystem connects vehicles (V2V), the grid (V2G), devices (V2D), infrastructure (V2I), as well as the other way around in metropolitan and country regions [2]. IoVs additionally give E-wellbeing applications and work as versatile medical clinics in crises [2].

IoVs total and examine information from incorporated internet based storehouses to further develop street security and transportation administrations inside Intelligent Transportation Systems (ITS) [3], [4]. IoVs additionally empower the smooth transmission, estimation, and capacity of gigantic volumes of information, fulfilling client and partner needs [5], [6]. Be that as it may, the remarkable development of the IoVs network has raised security concerns [3], [7].

The IoVs scene develops, uncovering security shortcomings that require proactive endeavors to moderate assaults. [3], [7]. Security breaks debilitate network availability and endanger information uprightness and secrecy [4], [8]. Message clog and security breaks during data scattering thwart IoVs network vehicle-to-vehicle (V2V) availability [4], [8]. Haze processing, a decentralized specialized strategy that lessens blockage and security chances, may settle these issues. [4], [9], [10].

Cisco's 2012 thought of haze figuring interfaces clients to the cloud by further developing information calculation, stockpiling, and systems administration at the organization's edge [12], [13]. Fog computing utilizes dispersed assets to answer rapidly and lessen inertness, not at all like cloud computing [14]. Fog computing keeps away from cloud computing's idleness, versatility, and information clog by handling information nearer to end-clients [14], [17].

Fog computing has many advantages, yet it likewise raises security concerns [12], [19], [20]. Fog computing opens neighborhood servers to account commandeering, DDoS attacks, information breaks, and information misfortune because of its decentralized nature [13], [14], [21], [22], [23], [24]. These weaknesses compromise IoV correspondence trustworthiness and security, imperiling public wellbeing.

To address these challenges, this study tends to fog computing's requirements and mitigates network-edge security dangers to further develop fog-assisted IoVs (Fa-IoVs) security. Fa-IoVs use fog computing to further develop correspondence and diminishing security attacks, empowering safe vehicle data transfer [6], [27], [28]. Fog nodes decisively conveyed along the IoVs organization can decrease blockage and security gambles, empowering intelligent transportation systems.[36]

2. LITERATURE SURVEY

In 2016, Kaiwartya et al. covered the Internet of Vehicles (IoVs)' reasoning, layered engineering, network model, issues, and future [1]. IoVs can modify transportation networks by empowering vehicle correspondence for better traffic signal and security, as indicated by the creators. They surveyed the layered design of IoVs, including V2V, V2G, V2D, and V2I correspondence, and noted security and versatility issues.

Xu et al. (2018) analyzed what the Internet of Vehicles means for information the executives and examination in the enormous information time [2]. The creators featured the capability of IoVs and huge information innovation to involve vehicle information for traffic arranging, prescient support, and customized administrations. To utilize IoVs to tackle transportation issues, they pushed data processing and examination.

Contreras-Castillo et al. (2018) analyzed the IoV's engineering, conventions, and security, uncovering its systems and issues [3]. IoVs have layered designs, thusly powerful correspondence conventions and security methodology are expected to safeguard information stream. For protected and reliable vehicle correspondence, they focused on the meaning of handling security shortcomings such message clog and security dangers.

ISSN 2347–3657

Volume 12, Issue 3, 2024

Yaqoob et al. (2019) proposed fog computing to forestall network blockage and further develop correspondence proficiency in the Internet of Vehicles [4]. The creators proposed fog computing for offloading process obligations and lessening data transmission latency in IoVs. They examined fog nodes at the network edge processing data locally to decrease clog and further develop framework execution. The recommended approach could further develop IoV correspondence versatility and dependability.

A productive and safe fog computing data transfer procedure for the IoV by Zhang and Li (2020) focused on protection [6]. IoV information transmission security and protection issues were tended to, strikingly in fog computing settings where information handling occurs at the network edge. A secure data transfer system with security saving methodologies was introduced to safeguard delicate information. The method guaranteed protected and confidential IoV information conveyance.

To further develop security and protection in the IoV, Tune et al. (2020) proposed mist based character confirmation [7]. In fog computing settings where information is handled locally, character distinguishing proof in IoVs presents security issues. They introduced a haze hub based vehicle confirmation method that safeguards security. Protected and confidential IoV validation was accomplished by the framework.

Yaqoob et al. (2018) fostered a fog-assisted blockage evasion system for the IoV to further develop correspondence and lessen network clog [18]. Fog nodes offload register jobs and improve information transmission in IoVs in the creators' conveyed blockage aversion approach. They proposed decisively putting Fog nodes to powerfully change traffic stream and diminish blockage. The method could further develop IoV correspondence versatility and dependability.[38]

Kang et al. (2018) planned to further develop haze processing upheld Web of Vehicles security with a pen name [27]. In haze figuring settings where information is handled locally, nom de plume in IoVs raises protection issues. They proposed utilizing haze hubs to create and oversee vehicle pen names safeguarding protection. It was effective in safeguarding IoV nom de plumes.

A Web of Vehicles haze empowered constant traffic the executives framework for offloading was proposed by Wang et al. (2018) to increment traffic the executives effectiveness [28]. A haze empowered design utilizes mist hubs to offload registering obligations and further develop IoV constant traffic the board. Traffic the board frameworks can be more responsive and versatile by conveying haze hubs at side of the road units (RSUs) to locally assemble and deal with traffic information. This innovation could upgrade IoV Traffic Stream and diminish clog.

In further developing correspondence proficiency, security, and protection for the Web of Vehicles, mist registering is pivotal. Scientists have created haze registering frameworks that enhance information handling, lessen network clog, and further develop IoV security. In any case, fog-assisted IoV examination can resolve new issues and upgrade the field.

3. METHODOLOGY

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

a) Proposed Work:

The proposed arrangement utilizes an Autoencoder Convolutional Neural Network (CNN)[48] to further develop security in fog-assisted Internet of Vehicles (IoVs) networks. CNN and autoencoder features are utilized to make a vigorous anomaly detection model that can distinguish IoVs network security concerns. This technique thinks about standard ML strategies including Decision Trees (DT), Random Forests (RF)[40], Support Vector Machines (SVM)[43], and Naive Bayes (NB) to find the ideal anomaly detection model. This similar examination will show how well the Autoencoder CNN approach recognizes anomalies and mitigates security worries in haze helped IoVs organizations.[40]

The proposed study presents a profound learning-based methodology that involves CNN and autoencoder calculations to tackle security issues in IoVs organizations. To secure fog-assisted IoVs networks, the best anomaly detection model should be tracked down through intensive testing and near investigation.

b) System Architecture:

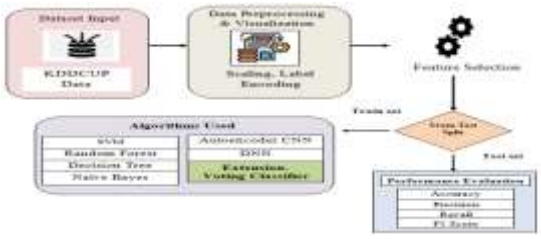

Fig 1 Proposed Architecture

The fog-assisted Internet of Vehicles (IoVs) anomaly detection system configuration has numerous fundamental stages. Beginning with the KDDCUP dataset, anomaly detection algorithms are prepared and tried. Data is then preprocessed and shown utilizing scaling and label encoding. Using feature selection systems to find the main properties smoothes out model training.

Then, the dataset is isolated into preparing and testing sets for model structure and appraisal. SVM, Random Forest, Decision Trees, Naive Bayes, AutoEncoder CNN, Deep Neural Networks (DNN), and Voting Classifier are used to detect abnormalities. Each algorithm's precision, F1 score, recall, and accuracy are assessed.

To choose the best anomaly detection technique for fog-assisted IoVs networks, every calculation is entirely assessed. This calculated plan thoroughly assesses anomaly detection techniques to pick the best organization security methodologies.

c) Dataset:

This study utilized the cybersecurity benchmark KDD Cup dataset for anomaly detection. Reproduction based network traffic information portrays invasion endeavors and destructive activities. It permits exhaustive examination with convention sorts, administration types, association spans, and IP addresses. Named models show common or strange activities, supporting directed learning. This dataset is much of the time used to test anomaly detection algorithms for network safety danger ID. Variety and marking make it ideal for method assessment and correlation. At last, the KDD Cup dataset further develops anomaly detection calculations, empowering solid cybersecurity arrangements.

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

Deep learning-based anomaly detection in fog-assisted IoVs networks utilizing the KDD dataset from KDD Cup 1999. This dataset of network traffic data covers different exercises and security concerns and is utilized in intrusion detection and network security. It gives a thorough network traffic portrayal for fog-assisted IoV anomaly detection including convention sorts, administration types, and association terms. In addition, named typical and strange conduct empower supervised learning. The dataset distinguishes examples and anomalies in IoVs network traffic. Because of its enormous marked dataset and reasonable organization traffic portrayal, the KDD dataset helps train and assess DL models for anomaly detection, upgrading fog-assisted IoVs network security.

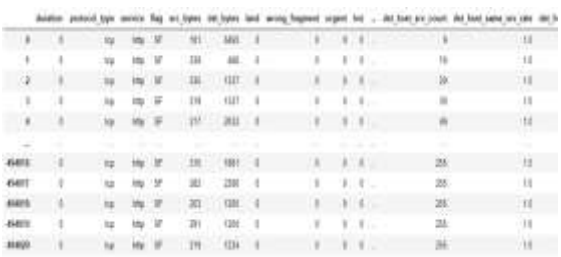

Fig 2 Dataset

d) Data processing:

To set up the dataset for model training, fog-assisted Internet of Vehicles (IoVs) anomaly detection data processing requires various cycles.

Loading the Dataset: Data is placed into a pandas dataframe, a well-known Python information control and examination bundle. This works on data control.

Keras Processing: The dataset is then handled utilizing Keras, a solid DL structure. Keras offers data arrangement and utilities for DL models.

Dropping Unwanted Columns: Non-anomaly-detecting columns are taken out from the dataset. Zeroing in on fundamental data diminishes clamor and works on model execution.

Data Normalization: Ceaseless dataset qualities are standardized to a standard scale to give impartial model training commitment. This stage keeps enormous scope qualities from dominating learning.

Encoding Categorical Variables: Encoding One-hot encoding is utilized to address straight out factors mathematically. This supports mathematical info DL models.

Splitting the Dataset: The processed dataset is isolated into training and testing sets. The anomaly detection model is trained on the training set and tried on the testing set.

After these cycles, the dataset is prepared for DL model training to detect fog-assisted IoVs network abnormalities.

e) Visualization:

Visualization is fundamental for understanding fog-assisted Internet of Vehicles (IoVs) network elements and evaluating anomaly detection procedures. Visualisation uncovers network traffic anomalies and deviations. Highlight circulation plots uncover network traffic qualities, recognizing anomalies and startling examples. Visualizing precision-recall curves and confusion matrices investigates model viability and mistake dissemination. These visualizations assist

ISSN 2347–3657

Volume 12, Issue 3, 2024

partners with picking models, improve, and secure organizations. Visualisation assists scholastics and experts with crossing fog-assisted IoVs networks by interfacing crude information to significant bits of knowledge.

f) Label Encoding:

Deep learning-based anomaly detection for fog-assisted IoVs networks requires label encoding. This strategy transforms straight out factors into numbers so ML calculations can deal with them. For interoperability with DL models like CNNs or RNNs, fog-assisted IoVs networks should encode unmitigated factors like vehicle classes, correspondence conventions, and occasion classifications mathematically. Label encoding assists the model with understanding the connections among classifications and organization traffic irregularities by giving interesting number marks to every variable class. Clear cut factors can be input highlights close by constant factors in the dataset in the wake of encoding, further developing anomaly detection algorithms. Label encoding is fundamental for getting ready unmitigated data for model training and involving it in fog-assisted IoVs anomaly detection operations.

g) Feature Selection:

Deep learning-based anomaly detection for fog-assisted Internet of Vehicles (IoVs) networks requires feature selection to find and pick the most significant dataset elements to increment model execution and productivity. Feature selection dimensionality, clamor, and works on the model's ability to detect abnormalities in fog-assisted IoVs organizations, where the dataset may contain many network traffic attributes. Correlation analysis, shared data, and tree-based include significance might assess every trademark and select the most prescient ones. Highlight determination improves on model preparation, diminishes processing intricacy, and lessens overfitting by picking significant elements and killing unessential ones. Feature selection likewise works on model interpretability by focusing on the main factors, assisting with fathoming fog-assisted IoVs network irregularities. Feature selection upgrades DL-based anomaly detection systems, making fog-assisted IoVs security more grounded.

h) Algorithms:

Support Vector Machine (SVM): A supervised learning approach for classification and regression is SVM. It boosts edge between classes by distinguishing the best hyperplane to isolate data of interest into classes. High-layered SVM [43] is compelling and strong to overfitting, making it fantastic for anomaly identification proof in muddled datasets.[42]

Random Forest: Random Forest is an ensemble learning approach that prepares a few decision trees and results their mode (classification) or mean prediction (regression). [40] Its commotion opposition, overfitting obstruction, and ability to deal with colossal datasets with high dimensionality make it ideal for anomaly identification.

Decision Tree: The supervised learning technique Decision Tree iteratively segments the dataset into subsets relying upon property estimations, creating a tree-like design of decision hubs. It's easy to utilize and can deal with mathematical and absolute data. Decision trees can overfit and not sum up to new information without regularization.

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

Naive Bayes: Naive Bayes is a Bayes' hypothesis based probabilistic classifier that expects feature independence. Regardless of its effortlessness, Naive Bayes characterizes well, particularly with enormous datasets. It is computationally productive, takes little training data, and functions admirably with insignificant qualities.

Deep Neural Network (DNN): DNN artificial neural networks incorporate various secret layers among input and output.[23] It is great for fog-assisted IoVs anomaly detection since it gains confounded designs from enormous volumes of information. DNN preparing requires a great deal of handling power and can cause overfitting or the vanishing gradient problem without regularization.

CNN Autoencoder: CNN Autoencoder neural networks use convolutional layers for feature extraction and reproduction. The calculation encodes approaching information into a lower-layered inactive space and recreates it. CNN Autoencoders catch spatial relationships and recognize oddities in light of reproduction blunders for unsupervised anomaly identification.

Voting Classifier: Ensemble learning procedure Voting Classifier joins fundamental classifier expectations to make last forecasts. It utilizes greater part or weighted voting join classifier results. Voting Classifier utilizes base model variety to build speculation and strength over individual classifiers.

4. EXPERIMENTAL RESULTS

Accuracy: A test's accuracy is its ability to recognize debilitated from sound cases. To quantify test accuracy, figure the small part of true positive and true negative in completely broke down cases. Numerically, this is:[44]

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

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

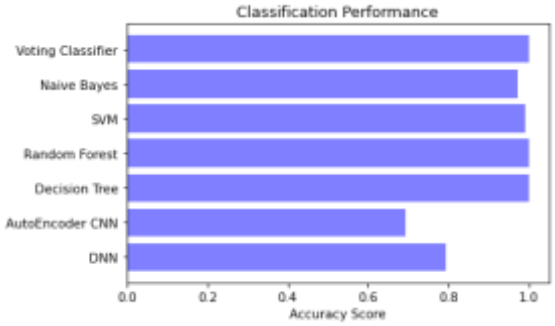

Fig 3 Accuracy Comparison Graph

F1-Score: Machine learning model accuracy is estimated by F1 score. Consolidating model precision and recall scores. The accuracy measurement estimates how frequently a model anticipated accurately all through the dataset.

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

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

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

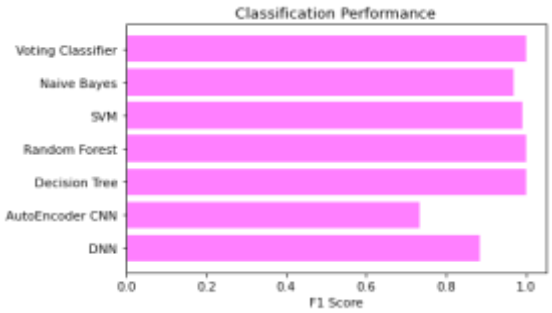

Fig 4 F1 Score Comparison Graph

Precision: Precision estimates the level of positive cases or tests precisely sorted. Precision is determined utilizing the recipe:

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

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

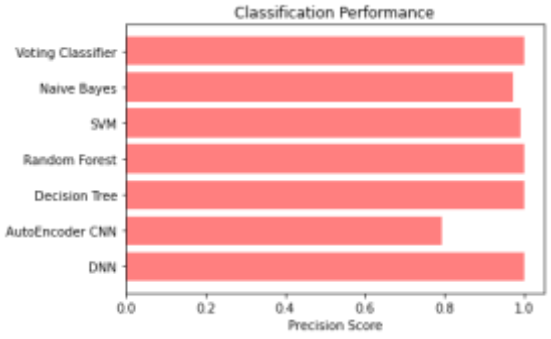

Fig 5 Precision Comparison Graph

Recall: Machine learning recall assesses a model's ability to perceive all significant examples of a class. It shows a model's culmination in catching occasions of a class by contrasting accurately anticipated positive perceptions with complete positives.

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

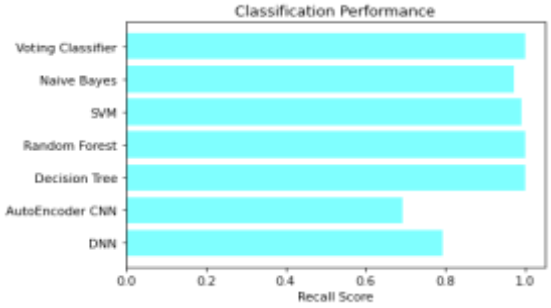

Fig 6 Recall Comparison Graph

Fig 7 Performance Evaluation Table

Fig 8 Home Page

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

Fig 9 Registration Page

Fig 10 Login Page

Fig 11 Upload Input Data

Fig 12 Predicted Results

5. CONCLUSION

Fog-assisted IoVs (Fa-IoVs) address clog and security issues by joining fog computing and IoVs. This paper presented CAadet, a DL-based anomaly detection algorithm for Fa-IoVs organizations, using the NSL-KDD dataset. We showed that CAadet is better at distinguishing abnormalities and further developing network security than different frameworks through exhaustive assessment. Coordinating a Voting Classifier into the undertaking upgraded precision by utilizing differed calculation qualities. A Flask-based front-end with SQLite verification makes Fa-IoVs anomaly detection secure and simple.

6. FUTURE SCOPE

Future innovative work in anomaly identification for Fog-assisted IoVs networks are conceivable. Future exploration could examine suggested courses in different IoT regions utilizing assorted datasets and DL models to further develop detection. Furthermore, anomaly detection models may be advanced, deceptions decreased, and continuous responsiveness moved along. Furthermore, coordinating current anomaly detection strategies with shrewd transportation frameworks might further develop vehicular organization security and effectiveness. High level anomaly detection strategies and their utilization in Haze helped IoVs organizations could further develop online protection and correspondence dependability in future astute transportation frameworks.

REFERENCES

[1] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. T. Lin, and X. Liu, ‘‘Internet of Vehicles: Motivation, layered architecture, network model, challenges, and future aspects,’’ IEEE Access,

vol. 4, pp. 5356–5373, 2016, doi: 10.1109/ACCESS.2016.2603219.

[2] W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, and X. Shen, ‘‘Internet of Vehicles in big data era,’’ IEEE/CAA J. Autom. Sinica, vol. 5, no. 1, pp. 19–35, Jan. 2018, doi: 10.1109/JAS.2017.7510736.

[3] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, ‘‘Internet of Vehicles: Architecture, protocols, and security,’’ IEEE Internet Things J., vol. 5, no. 5, pp. 3701–3709, Oct. 2018, doi: 10.1109/JIOT.2017.2690902.

[4] S. Yaqoob, A. Ullah, M. Akbar, M. Imran, and M. Shoaib, ‘‘Congestion avoidance through fog computing in Internet of Vehicles,’’ J. Ambient Intell. Humanized Comput., vol. 10, no. 10, pp. 3863–3877, Oct. 2019, doi: 10.1007/s12652-019-01253-x.

[5] A. Ullah, S. Yaqoob, M. Imran, and H. Ning, ‘‘Emergency message dissemination schemes based on congestion avoidance in VANET and vehicular FoG computing,’’ IEEE Access, vol. 7, pp. 1570–1585, 2019, doi: 10.1109/ACCESS.2018.2887075.

[6] W. Zhang and G. Li, ‘‘An efficient and secure data transmission mechanism for Internet of Vehicles considering privacy protection in fog computing environment,’’ IEEE Access, vol. 8, pp. 64461–64474, 2020, doi: 10.1109/access.2020.2983994.

[7] L. Song, G. Sun, H. Yu, X. Du, and M. Guizani, ‘‘FBIA: A fog-based identity authentication scheme for privacy preservation in Internet of Vehicles,’’ IEEE Trans. Veh. Technol., vol. 69, no. 5, pp. 5403–5415, Mar. 2020, doi: 10.1109/TVT.2020.2977829.

[8] A. J. Siddiqui and A. Boukerche, ‘‘On the impact of DDoS attacks on software-defined Internet-of-Vehicles control plane,’’ in Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), Jun. 2018, pp. 1284–1289, doi: 10.1109/IWCMC.2018.8450433.

[9] J. Ni, K. Zhang, X. Lin, and X. S. Shen, ‘‘Securing fog computing for Internet of Things applications: Challenges and solutions,’’ IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 601–628, 1st Quart., 2018, doi: 10.1109/COMST.2017.2762345.

[10] L. Zhu, M. Li, and Z. Zhang, ‘‘Secure fog-assisted crowdsensing with collusion resistance: From data reporting to data requesting,’’ IEEE Internet Things J., vol. 6, no. 3, pp. 5473–5484, Jun. 2019, doi: 10.1109/JIOT.2019.2902459.

[11] L. Zhou, H. Guo, and G. Deng, ‘‘A fog computing based approach to DDoS mitigation in IIoT systems,’’ Comput. Secur., vol. 85, pp. 51–62, Aug. 2019, doi: 10.1016/j.cose.2019.04.017.

[12] R. Mahmud, R. Kotagiri, and R. Buyya, ‘‘Fog computing: A taxonomy, survey and future directions,’’ Internet of Everything. Cham, Switzerland: Springer, 2018, pp. 103–130, doi: 10.1007/978-981-10-5861-5_5.

[13] S. Yi, C. Li, and Q. Li, ‘‘A survey of fog computing: Concepts, applications and issues,’’ in Proc. Workshop Mobile Big Data, Jun. 2015, pp. 37–42, doi: 10.1145/2757384.2757397.

[14] S. Khan, S. Parkinson, and Y. Qin, ‘‘Fog computing security: A review of current applications and security solutions,’’ J. Cloud Comput., vol. 6, no.

1, pp. 1–22, Dec. 2017, doi: 10.1186/s13677-017-0090-3.

[15] S. Yaqoob, A. Ullah, M. Awais, I. Katib, A. Albeshri, R. Mehmood, M. Raza, S. Ul Islam, and J. J. P. C. Rodrigues, ‘‘Novel congestion avoidance scheme for Internet of Drones,’’ Comput. Commun., vol. 169, pp. 202–210, Mar. 2021, doi: 10.1016/j.comcom.2021.01.008.

[16] L. M. Vaquero and L. Rodero-Merino, ‘‘Finding your way in the fog: Towards a comprehensive definition of fog computing,’’ ACM SIGCOMM Comput. Commun. Rev., vol. 44, no. 5, pp. 27–32, Oct. 2014, doi: 10.1145/2677046.2677052.

[17] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, ‘‘Vehicular fog computing: A viewpoint of vehicles as the infrastructures,’’ IEEE Trans. Veh. Technol., vol. 65, no. 6, pp. 3860–3873, Jun. 2016, doi: 10.1109/TVT.2016.2532863.

[18] S. Yaqoob, A. Ullah, M. Akbar, M. Imran, and M. Guizani, ‘‘Fog-assisted congestion avoidance scheme for Internet of Vehicles,’’ in Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), Jun. 2018, pp. 618–622, doi: 10.1109/IWCMC.2018.8450402.

[19] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, and J. P. Jue, ‘‘All one needs to know about fog computing and related edge computing paradigms: A complete survey,’’ J. Syst. Archit., vol. 98, pp. 289–330, Sep. 2019, doi: 10.1016/j.sysarc.2019.02.009.

[20] S. Tu, M. Waqas, S. U. Rehman, M. Aamir, O. U. Rehman, Z. Jianbiao, and C.-C. Chang, ‘‘Security in fog computing: A novel technique to tackle an impersonation attack,’’ IEEE Access, vol. 6, pp. 74993–75001, 2018, doi: 10.1109/ACCESS.2018.2884672.

[21] A. Abeshu and N. Chilamkurti, ‘‘Deep learning: The frontier for distributed attack detection in fog-to-things computing,’’ IEEE Commun. Mag., vol. 56, no. 2, pp. 169–175, Feb. 2018, doi: 10.1109/MCOM.2018.1700332.

[22] S. T. Zargar, J. Joshi, and D. Tipper, ‘‘A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks,’’ IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2046–2069, Mar. 2013, doi: 10.1109/SURV.2013.031413.00127.

[23] S. Sumathi, R. Rajesh, and S. Lim, ‘‘Recurrent and deep learning neural network models for DDoS attack detection,’’ J. Sensors, vol. 2022, pp. 1–21, Sep. 2022, doi: 10.1155/2022/8530312.

[24] S. Sumathi and R. Rajesh, ‘‘Comparative study on TCP SYN flood DDoS attack detection: A machine learning algorithm based approach,’’ Wseas Trans. Syst. Control, vol. 16, pp. 584–591, Nov. 2021, doi: 10.37394/23203.2021.16.54.

[25] Y. Xu, W. Yang, X. Yu, H. Li, T. Cheng, X. Lu, and Z. L. Wang, ‘‘Realtime monitoring system of automobile driver status and intelligent fatigue warning based on triboelectric nanogenerator,’’ ACS Nano, vol. 15, no. 4, pp. 7271–7278, Apr. 2021, doi: 10.1021/acsnano.1c00536.

[26] G. Albertus, M. Meiring, and H. C. Myburgh, ‘‘A review of intelligent driving style analysis systems and related artificial intelligence algorithms,’’ Sensors,

vol. 15, no. 12, pp. 30653–30682, 2015, doi: 10.3390/s151229822.

[27] J. Kang, R. Yu, X. Huang, and Y. Zhang, ‘‘Privacy-preserved pseudonym scheme for fog computing supported Internet of Vehicles,’’ IEEE Trans. Intell. Transp. Syst., vol. 19, no. 8, pp. 2627–2637, Aug. 2018, doi: 10.1109/TITS.2017.2764095.

[28] X. Wang, Z. Ning, and L. Wang, ‘‘Offloading in Internet of Vehicles: A fog-enabled real-time traffic management system,’’ IEEE Trans. Ind. Informat., vol. 14, no. 10, pp. 4568–4578, Oct. 2018, doi: 10.1109/TII.2018.2816590.

[29] H. Zhang, Y. Luo, Q. Yu, L. Sun, X. Li, and Z. Sun, ‘‘A framework of abnormal behavior detection and classification based on big trajectory data for mobile networks,’’ Secur. Commun. Netw., vol. 2020, pp. 1–15, Dec. 2020, doi: 10.1155/2020/8858444.

[30] A. A. Cook, G. Misirli, and Z. Fan, ‘‘Anomaly detection for IoT time-series data: A survey,’’ IEEE Internet Things J., vol. 7, no. 7, pp. 6481–6494, Jul. 2020, doi: 10.1109/JIOT.2019.2958185.

[31] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, ‘‘An anomaly mitigation framework for IoT using fog computing,’’ Electronics, vol. 9, no. 10, pp. 1–24, 2020, doi: 10.3390/electronics9101565.

[32] D. K. K. Reddy, H. S. Behera, J. Nayak, B. Naik, U. Ghosh, and P. K. Sharma, ‘‘Exact greedy algorithm based split finding approach for intrusion detection in fog-enabled IoT environment,’’ J. Inf. Secur. Appl., vol. 60, Aug. 2021, Art. no. 102866, doi: 10.1016/j.jisa.2021.102866.

[33] 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.

[34] A. Diro and N. Chilamkurti, ‘‘Leveraging LSTM networks for attack detection in fog-to-things communications,’’ IEEE Commun. Mag., vol. 56, no. 9, pp. 124–130, Sep. 2018, doi: 10.1109/MCOM.2018.1701270.

[35] C. Yin, S. Zhang, J. Wang, and N. N. Xiong, ‘‘Anomaly detection based on convolutional recurrent autoencoder for IoT time series,’’ IEEE Trans. Syst. Man, Cybern. Syst., vol. 52, no. 1, pp. 112–122, Jan. 2022, doi: 10.1109/tsmc.2020.2968516.

Dataset Link:

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

[36] G.Viswanath, “Hybrid encryption framework for securing big data storage in multi-cloud environment”, Evolutionary intelligence, vol.14, 2021, pp.691-698.

[37] Viswanath Gudditi, “Adaptive Light Weight Encryption Algorithm for Securing Multi-Cloud Storage”, Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol.12, 2021, pp.545-552.

[38] Viswanath Gudditi, “A Smart Recommendation System for Medicine using Intelligent NLP Techniques”, 2022 International Conference on

Automation, Computing and Renewable Systems (ICACRS), 2022, pp.1081-1084.

[39] G.Viswanath, "Enhancing power unbiased cooperative media access control protocol in manets", International Journal of Engineering Inventions, 2014, vol.4, pp.8-12.

[40] Viswanath G, "A Hybrid Particle Swarm Optimization and C4.5 for Network Intrusion Detection and Prevention System", 2024, International Journal of Computing, DOI: https://doi.org/10.47839/ijc.23.1.3442, vol.23, 2024, pp.109-115.

[41] G.Viswanath, "A Real Time online Food Ording application based DJANGO Restfull Framework", Juni Khyat, vol.13, 2023, pp.154-162.

[42] Gudditi Viswanath, "Distributed Utility-Based Energy Efficient Cooperative Medium Access Control in MANETS", 2014, International Journal of Engineering Inventions, vol.4, pp.08-12.

[43] G.Viswanath," A Real-Time Video Based Vehicle Classification, Detection And Counting System", 2023, Industrial Engineering Journal, vol.52, pp.474-480.

[44] G.Viswanath, "A Real- Time Case Scenario Based On Url Phishing Detection Through Login Urls ", 2023, Material Science Technology, vol.22, pp.103-108.

[45] Manmohan Singh,Susheel Kumar Tiwari, G. Swapna, Kirti Verma, Vikas Prasad, Vinod Patidar, Dharmendra Sharma and Hemant Mewada, "A Drug-Target Interaction Prediction Based on Supervised Probabilistic Classification" published in Journal of Computer Science, Available at: https://pdfs.semanticscholar.org/69ac/f07f2e756b79181e4f1e75f9e0f275a56b8e.pdf