ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

A NIDS-CNN LSTM MODEL FOR CLASSIFYING NETWORK INTRUSIONS BASED ON DEEP LEARNING

A DHANASEKHAR REDDY[1], B R TENDRAL[2], T ANIL KUMAR[3], P GOPICHAND[4]

[1]Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: dhanasekhar918@gmail.com

[2]P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: brtendral747@gmail.com

[3]Associate Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: anil.thumburu@gmail.com

[4]Assistant Professor, Department of CSE, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: pgopichand1@gmail.com

Abstract: Attack detection is the most important part of enterprise security, and deep learning-based attack detection algorithms are an important research topic. We develop a DL-based network attack detection classification model (NIDS-CNNLSTM) for remote detection situations in the Industrial Internet of Things (IIoT), to detect and distinguish network traffic data, and protect IIoT hardware and tasks. NIDS-CNNLSTM uses a long short-term memory neural network to prepare and characterize the features of convolutional neural networks for time series data, and demonstrates its importance using parallel and multi-stage situations. The model uses the sample data sets KDD CUP99, NSL_KDD, and UNSW_NB15. The validation accuracy and training loss of the three datasets are concentrated and comparable, and the traffic classification accuracy is excellent. The exhibition of NIDS-CNNLSTM is much better than prior models. The proficiency is shown by fantastic detection, classification, and low misleading problem rates in tests. It functions admirably for IIoT enormous scope and multi-situation network information.

Index Terms *- Network intrusion detection, deep learning, convolutional neural network, long short-term memory neural network.*

1. INTRODUCTION

IIoT has opened new entryways for worldwide turn of events. It will likewise present security dangers including modern center information spillage and unlawful terminal control. Hence, IIoT security is troublesome. IIoT security depends on dynamic latent safeguards such modern firewalls and intrusion detection. Firewalls can't impede infections or worms since they are inactive guards. Thusly, Intrusion detection technology is carried out to make up for firewall inadequacies. Customary static organization security is enhanced with intrusion detection advances. It safeguards against inward and outer Intrusions by constant organization checking. Proactive, constant, dynamic. Intrusion detection technology is a famous theme in IIoT security research as an organization security component. Late interruption discovery and arrangement calculation research has zeroed in on traditional ML and DL.[16]

This paper proposes and creates NIDS-CNNLSTM, a DL-based Network Intrusion Detection Classification Model. The review utilizes CNN and LSTM organizations to further develop intrusion detection accuracy and efficiency. The model's viability will be completely evaluated utilizing genuine network intrusion datasets to further develop ID approaches for safeguarding PC networks from arising digital dangers.

Customary Network Intrusion Detection battle to identify complicated and creating digital dangers. Numerous arrangements battle to recognize among standard and noxious organization action. This hole requires a more adaptable procedure. The proposed research presents NIDS-CNNLSTM, a deep learning classification model. This model purposes CNN and LSTM networks to perform more exact and dynamic ID than more established methods.

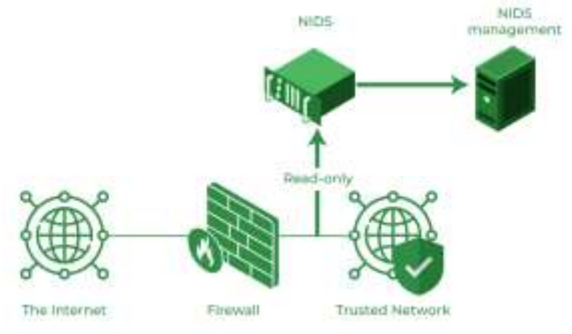


Fig 1 Intrusion Detection System

To eliminate the impedance of copy features, Xiao et al. [15] used an autoencoder (AE) to reduce the data aspect and a CNN to detect intrusion data. Staudemeyer [16] used a long short-term memory (LSTM) to identify intrusions and link the time-space of intrusion data to limit false positives. An intelligent lattice ID approach by Zhang et al. [17] uses GA and extreme learning machines. This model maintains the advantages of ELM and improves the bounds using GA. Vinayakumar et al. [18] combined CNN and LSTM. They used a sequential CNN-LSTM-IDS model to extract a low-level set of organizational traffic connectivity features into a high-level elemental representation. Yao et al. [19] proposed the AMI-ID model, which utilizes a combination of cross-layer features of CNN and LSTM to obtain complete elements with multi-domain features from the KDD Cup 99 and NSL_KDD datasets.

2. LITERATURE REVIEW

A straightforward decision tree can depict order rationale with noticeable principles. Assuming that rules incorporate delicate data, this construction might permit assailants to derive privileged intel. In this exploration, a tree pruning system in light of IP truncation anonymization is recommended to prune veritable IP addresses. Nonetheless, inappropriately arranged tree pruning might harm the first tree's presentation by precluding specific data for its thought. The proposed pruning methodology is tried on the 6-percent-GureKDDCup'99, full-variant GureKDDCup'99, UNSW-NB15, and CIDDS-001 datasets. To evaluate resilience and compromise, the outcomes are contrasted with the unpruned tree model. This study utilizes the C4.5 tree model. Our exact outcomes are promising and offer two principal benefits: delicate IP locations can be "pruned" (stowed away) during order to forestall client profiling, and the quantity of hubs in the tree is enormously diminished to make rule understanding conceivable while keeping up with classification accuracy.[18]

Standard PCs can't proficiently oversee gigantic information and recognize network traffic breaks, particularly huge information. Ordinary scientific strategies can't oversee delayed network traffic attacks and huge host log occasion information, bringing about numerous misleading up-sides and expanded preparing times. This study presents another technique for handling the essential large information difficulties of heterogeneous security information to further develop intrusion detection. To achieve the aforementioned goals, ensemble support vector machines (SVM) and chaos game optimization (CGO) are used. Our system improves the accuracy of intruder classification and identifies nine attack types in the UNSW-NB15 dataset. Factual analysis and execution metrics such as precision, recall, F1 score, accuracy, ROC curve, and misaligned grid are used to compare the proposed approach with standard models and evaluate its efficiency. The proposed approach has 96.29% precision contrasted with the chi-SVM (89.12%), a 6.47% increment. The proposed arrangement decreases misleading up-sides while overseeing security occasions in huge information frameworks because of its more prominent classification accuracy.[20]

Intrusion detection systems (IDS) report network traffic and framework activities to managers. ID may likewise disallow an unusual or noxious client or source address from entering the organization. Various kinds of IDS distinguish dubious traffic in various ways. Host and organization based IDS exist. As an antivirus and firewall, the IDS distinguishes known dangers by signature. Anomaly detection looks at traffic to pattern. In this exploration, fluffy and hereditary calculations are utilized to distinguish. Organizations, states, framework, and utility providers all rely upon PCs, PC organizations, and server farms for their activities. Assaults on PC framework are first come by network IDS. We make five ML classifiers for different attacks in this review. We used the CSE-CIC-IDS2018 dataset provided by the Security Facility and the Canadian Cyber Security Institute. This enormous network traffic follow assortment records many attacks and was as of late delivered. The 22-year-old KDD Cup'99 dataset was utilized to make network ID calculations before portable processing, Web 2.0/3.0, informal communication, web based video, and SSL. These significant Web peculiarities over the past twenty years require ID reexamination and improvement. Past AI classifier research using the CSE-CIC-IDS2018 dataset utilized a tremendous and complete arrangement of qualities, no less than one of which isn't dataset-invariant. Almost none have tried using all qualities with datasets of a couple hundred assault class models. This review's classifiers utilize a sensible measure of elements and are tried for security and speculation by giving both normal execution across 10 crease cross-approval and overlay variety.

The IoT gives shrewd, arranged contraptions and applications in a few fields to work on individuals' lives. Notwithstanding, IoT gadgets' greatest challenges are security gambles. The ongoing status of IoT apparatus security has multiple ways, yet more is required. ML can track down designs when traditional strategies fall flat. DL can further develop IoT security. This makes anomaly-based detection easy. This study proposes a CNN-based anomaly-based IDS that utilizes IoT's capacity to proficiently examine IoT traffic. The recommended model can recognize intrusions and distorted traffic. The model was built and evaluated based on the NID and BoT-IoT datasets with an accuracy of 99.51% and 92.85%, respectively.

3. METHODOLOGY

They propose a CNN-based network intrusion detection model in literature.To conquer the lopsided informational index issue, they use CNN to consequently extricate traffic qualities from crude informational collection and change each class' expense capability weight coefficient relying upon its numbers. This approach false alarm rate (FAR) and increments class accuracy with little numbers. The crude traffic vector design is switched over completely to picture arrangement to diminish estimation costs. The standard NSL-KDD informational collection is utilized to evaluate their CNN model.

Drawbacks:

1. The ongoing methodology chooses features from crude information utilizing Convolutional Neural Networks (CNNs). CNNs may consequently separate features, but they may not catch muddled fleeting conditions or undeniable level linkages, restricting their ability to decipher complex network traffic designs.

2. The unequal dataset issue is tended to by setting cost capability loads relying upon class numbers. This can decrease uneven class challenges, yet more complicated techniques that powerfully alter loads or produce manufactured information might find success.[22]

3. Current work lessens calculation costs by switching crude traffic vector information over completely to picture design. The transformation method might lose unobtrusive data in the first information, coming about in wrong or failure to distinguish explicit organization attack designs.

We propose a deep learning-based network intrusion detection classification model (NIDS-CNNLSTM) for the remote detecting situation of the IIoT to recognize and distinguish network traffic information and secure IIoT hardware and tasks. NIDS-CNNLSTM utilizes LSTM neural networks to prepare and group convolutional neural network features in time series information and demonstrates materialness utilizing paired and multi-arrangement situations. The model purposes KDD CUP99, NSL_KDD, and UNSW_NB15 exemplary datasets. We inspected the recommended model against past exploration.

Benefits:

1. LSTM neural networks are utilized in our review to catch fleeting connections in time series information. This technique might catch more complicated network traffic examples and linkages than CNNs alone.

2. While our strategy doesn't address uneven information, LSTM networks might be utilized to tackle class irregularity utilizing further developed procedures.

3. Our review consolidates CNNs and LSTMs to acquire a deeper information on network

traffic designs by using spatial and worldly features.

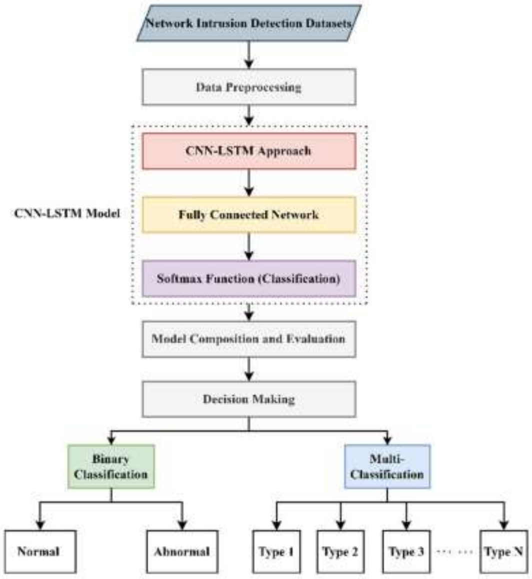


Fig 2 System Architecture

Modules:

- The data exploration module loads data into the system.
- The processing module reads the data for processing.
- Data will be separated into train and test using this module.
- To generate models, we used CNN, LSTM, CNN + LSTM, and CNN + BiLSTM. Algorithm accuracy calculated
- User signup and login: This module allows registration and login.
- User input: This module allows input for prediction.
- Final prediction: Displayed.

4. IMPLEMENTATION

CNN: Deep learning neural network architectures like CNNs are utilized in PC vision. A PC can investigate and decipher pictures and visual information utilizing computer vision.

LSTM: Long short-term memory networks are used in DL. A class of RNNs can learn long haul conditions, outstandingly for succession expectation.

CNN + LSTM: CNN-LSTM networks gain from preparing information utilizing convolutional and LSTM layers. The CNN-LSTM network is prepared utilizing hear-able based spectrograms removed from crude sound information.

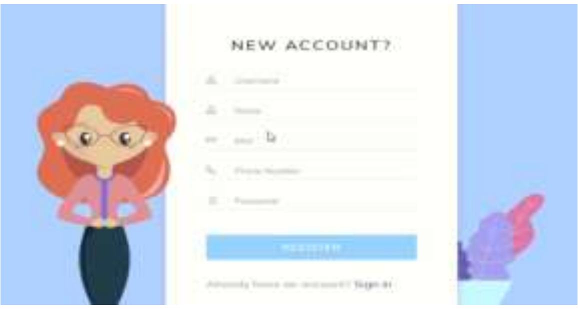
CNN + BiLSTM: A CNN+BilSTM CNN with bidirectional LSTM design architecture BiLSTM. The first named substance acknowledgment plan learns character-and word-level qualities. The CNN prompts character-level attributes. The model concentrates another feature vector from per-character feature vectors like person embedding and (alternatively) character type for each word utilizing convolution and a maximum pooling layer.[24]

5. EXPERIMENTAL RESULTS

Welcome
To Dashboard

NIDS-CNNLSTM: Network Intrusion Detection Classification Model Based on Deep Learning

Fig 3 Home page



NEW ACCOUNT?

Username

Name

Email

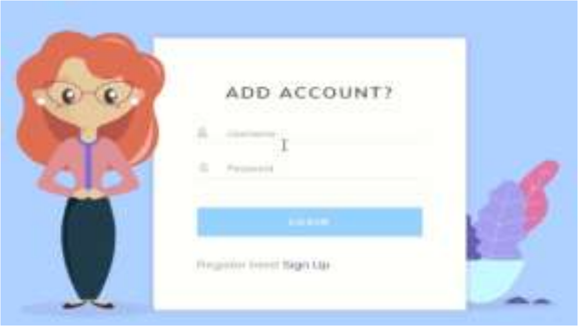
Phone Number

Password

REGISTER

Already have an account? Sign in

Fig 4 Registration page



ADD ACCOUNT?

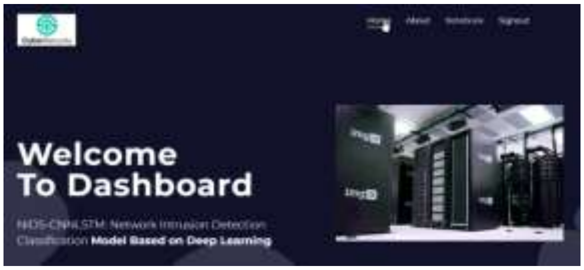
Username

Password

LOGIN

Register here! Sign Up

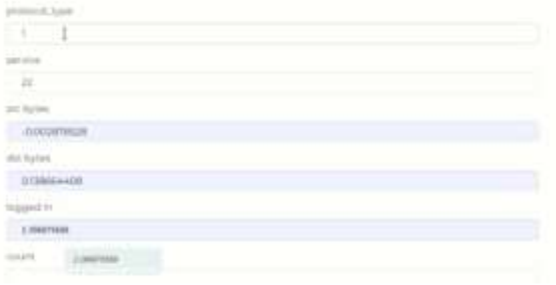
Fig 5 Login page



Welcome
To Dashboard

NIDS-CNNLSTM: Network Intrusion Detection Classification Model Based on Deep Learning

Fig 6 Main page



protocol_type

1

service

22

src bytes

[illegible]

dst bytes

[illegible]

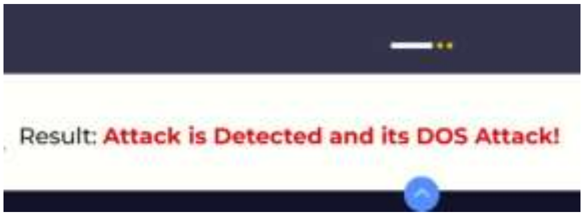
logged in

[illegible]

count

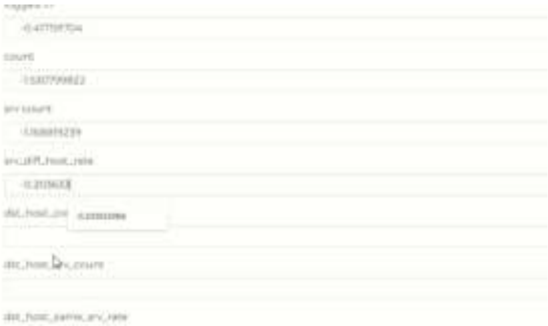
[illegible]

Fig 7 Upload input values



Result: Attack is Detected and its DOS Attack!

Fig 8 Prediction result



logged in

[illegible]

count

[illegible]

srv count

[illegible]

srv_diff_host_rate

[illegible]

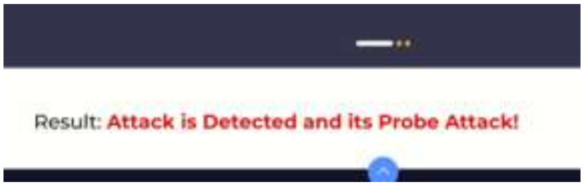
dst_host_co

[illegible]

dst_host_srv_count

dst_host_same_srv_rate

Fig 9 Upload another input values



Result: Attack is Detected and its Probe Attack!

Fig 10 Prediction Result

6. CONCLUSION

This paper offers NIDS-CNNLSTM to address the unfortunate discovery rate, grouping exactness, and bogus location pace of existing IIoT interruption identification models. NIDS-CNNLSTM improves and superimposes the two-layer CNN and unidirectional LSTM layers. CNN and LSTM extricate spatial and worldly attributes. The model's approval precision and preparing misfortune on the KDD CUP99, NSL_KDD, and UNSW_NB15 datasets exhibit high assembly and level. The model's relevance was tried utilizing paired and multi-characterization circumstances. It precisely orders traffic classifications and is sensible. NIDS-CNNLSTM beats prior models in characterization exactness, location rate, and misleading recognition rate. The interruption recognition arrangement model is superior to other people. We will expand the dataset awkwardness, little example traffic arrangement exactness, and model execution in future review.

REFERENCES

[1] S. J. Jian, Z. G. Lu, D. Du, B. Jiang, and B. X. Liu, ‘‘Overview of network intrusion detection technology,’’ J. Cyber Secur., vol. 5, no. 4, pp. 96–122, 2020.

[2] K. Wu, Z. Chen, and W. Li, ‘‘A novel intrusion detection model for a massive network using convolutional neural networks,’’ IEEE Access, vol. 6, pp. 50850–50859, 2018.

[3] T. Acharya, I. Khatri, A. Annamalai, and M. F. Chouikha, ‘‘Efficacy of heterogeneous ensemble assisted machine learning model for binary and multi-class network intrusion detection,’’ in Proc. IEEE Int. Conf. Autom. Control Intell. Syst. (I2CACIS), Jun. 2021, pp. 408–413.

[4] M. Injadat, F. Salo, A. B. Nassif, A. Essex, and A. Shami, ‘‘Bayesian optimization with machine learning algorithms towards anomaly detection,’’ in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2018, pp. 1–6.

[5] Y. J. Chew, S. Y. Ooi, K.-S. Wong, Y. H. Pang, and N. Lee, ‘‘Adoption of IP truncation in a privacy-based decision tree pruning design: A case study in network intrusion detection system,’’ Electronics, vol. 11, no. 5, p. 805, Mar. 2022.

[6] L. L. Ray, ‘‘Training and testing anomaly-based neural network intrusion detection systems,’’ Int. J. Inf. Secur. Sci., vol. 2, no. 2, pp. 57–63, 2013.

[7] A. Ponmalar and V. Dhanakoti, ‘‘An intrusion detection approach using ensemble support vector machine based chaos game optimization algorithm in big data platform,’’ Appl. Soft Comput., vol. 116, Feb. 2022, Art. no. 108295.

[8] M. Mehmood, T. Javed, J. Nebhen, S. Abbas, R. Abid, G. R. Bojja, and M. Rizwan, ‘‘A hybrid approach for network intrusion detection,’’ Comput., Materials Continua, vol. 70, no. 1, pp. 91–107, 2022.

[9] M. U. Ilyas and S. A. Alharbi, ‘‘Machine learning approaches to network intrusion detection for contemporary internet traffic,’’ Computing, vol. 104, no. 5, pp. 1061–1076, May 2022.

[10] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, ‘‘Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset,’’ IEEE Access, vol. 9, pp. 22351–22370, 2021.

[11] Z. Li, A. L. G. Rios, G. Xu, and L. Trajkovic, ‘‘Machine learning techniques for classifying network anomalies and intrusions,’’ in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), May 2019, pp. 1–5.

[12] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, ‘‘Anomaly-based intrusion detection system for IoT networks through deep learning

model,'' Comput. Electr. Eng., vol. 99, Apr. 2022, Art. no. 107810.

[13] Y. Fu, Y. Du, Z. Cao, Q. Li, and W. Xiang, ''A deep learning model for network intrusion detection with imbalanced data,'' Electronics, vol. 11, no. 6, p. 898, Mar. 2022.

[14] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, ''BAT: Deep learning methods on network intrusion detection using NSL-KDD dataset,'' IEEE Access, vol. 8, pp. 29575–29585, 2020.

[15] Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, ''An intrusion detection model based on feature reduction and convolutional neural networks,'' IEEE Access, vol. 7, pp. 42210–42219, 2019.

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

[17] 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.

[18] 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.

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

[20] 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.

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

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

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

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

[25] 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