International Journal of Computer and Engineering Optimization (IJCEO)
Volume 02, Issue 01, January– February (2024)

RESEARCH ARTICLE

AN OPTIMIZED DEEP LEARNING BASED INTRUSION DETECTION MODEL FOR NETWORK APPLICATION

D. Lavanya[1*] and Kannan Ramakrishnan[2]

[1]Department of Computer science and Engineering, Jawaharlal Nehru Technological University (JNTUA) in Anantapur, Andhra Pradesh 515002, India.
[2]Department of Electronics and Communication Engineering, Saveetha Engineering College, Kanchipuram - Chennai Rd, Chennai, Tamil Nadu 602105, India.

[*]*Corresponding e-mail: lavanyadoopati77@gmail.com*

Abstract – The deployment of advanced information technologies leads to wide data collection and processing in Internet of Things (IoT) systems. The wide usage of network and improved technologies increases the vulnerabilities and security issues. Thus, an Intrusion Detection System (IDS) was developed to predict and prevent the malicious activities in the network. However, the traditional IDS model failed to detect the malicious events accurately. Hence, a novel hybrid Antlion-based Radial Neural Network was designed to detect the attack data in the network. In this system, the dataset was pre-processed in the hidden layer to eliminate the noise or error data. Further, the important data features are tracked using the Antlion fitness for detection purposes. Finally, the malicious data are by contrasting the retrieved features with the learned features, objects can be recognized. Moreover, a user authentication module was designed to verify the users. The presented model was trained and tested with publically available IDS datasets namely: NSL-KDD and CICIDS. It is noted that the created framework managed to greater accuracy of 98.74%, and 98.96% for NSL-KDD and CICIDS datasets, respectively. Furthermore, the results are compared with the existing techniques for validation purposes.

Keywords *– Intrusion detection system, Radial Basis Neural network, Antlion optimization algorithm, User Authentication.*

1. INTRODUCTION

The IoT and digital information technologies are expanding at a never-before-seen pace these days. [1]. The large-scale usage of IoT systems increases the possibilities of attacks and security threats in the communication network [2]. In communication network, the data from the users are gathered and stored in cloud environment [3]. Hence, the IoT systems are widely used in communication networks for collecting, processing, and transmitting data [4]. The information collected using the IoT systems are very useful in providing intelligent services in various applications [5]. However, the gathered IoT data contains sensitive information. Thus, the privacy and security protection is important in the communication networks [6], [30]. To offer greater security in the distributed network, it is important to efficiently predict and stop network attacks [7]. This led to the development of a technology known as a network IDS (NIDS) to identify malevolent data in networks.

The traditional NIDS detects the malicious data effectively, but it lacks the ability to identify the unknown attacks present in the system [8]. This is mainly because not enough incursion data were available for the model training. to efficiently detect and stop network attacks [7]. Consequently, NIDS was created to find harmful data in the network. Thus, the deep learning (DL) and machine learning (ML) algorithmbased NIDS methods are developed to overcome these issues [9], [31]. In DL and ML-based intrusion model, the dataset was trained and tested separately [10]. Hence, the unknown attack identification is possible using this model. Support Vector Machine (SVM), Decision Tree (DT), and Random Forest (RF) are ML approaches algorithms are used to improve detection performances [14]. However, the ML-based IDS framework cannot handle the multi-domain intrusion detection [15], [32]. The comparison of ML and DL-based NIDS shows that the DL-based intrusion detection model performed better in terms of network security [16], [33].

The deep neural networks like graph neural system, CNN are effective in dealing with graph or network information [17], [34]. Moreover, they offer highest accuracy in detecting the known and unknown attacks [18]. However, the DL-based techniques require large-scale database to train the system for detection and classification purposes [18]. Moreover, the traditional DL algorithms like CNN [19], [35], multi-layer feedback neural system [19], etc., consumes more time in processing the dataset [20,36]. The existing techniques like IDS model based on deep learning theory [21], Autonomous IDS using deep convolutional neural system [22], anomaly identification framework based on convolutional neural system [23], [37], etc., are developed to identify the malevolent data in the network. In order to

safeguard network data from harmful occurrences, an optimal neural network was created.

The offered study work is organized into the sections below: Section 2 summarizes current research on the intrusion prevention model, Section 3 presents an illustration of the current system and its problem statement, Section 4 describes the design as well as workflow of the given intrusion prevention model, Section 5 presents an illustration of effectiveness and comparative analysis, and Section 6 is the conclusion.

2. RELATED WORK

Here is a description of a few recent related works

The security and confidentiality of unintentional users are put at risk since network data is used so frequently and is therefore open to assault by hackers and others. As a result, to detect security breaches Jing Yu et al. [21] presented an IDS method based on DL theory. This method deploys convolutional neural system to predict the security threats accurately. This developed model was test and validate with the public network datasets. Finally, the performances are compared with other techniques like recurrent neural network, and gradient boosting algorithm for validation. This method offers faster and accurate detection. Moreover, this model earned lower error rate of 4.67%. However, the prevention of security threats is not possible using this approach.

Qasem Abu Al-Haija and Ahmad Al Badawi [22] presented an autonomous IDS utilizing deep convolutional neural system to detect and prevent the security threats in Unmanned Aerial Vehicles (UAVs). Nowadays, the UAV communication systems are becoming popular and achieved remarkable growth. Thus, they are susceptible to attacks, and security threats. This developed scheme encoded Wi-Fi traffic logs of three common models of UAVs, namely the DBPower UDI, the Parrot Bebop, and the DJI Inspire and DJI Spark. This model achieved greater detection accuracy of 99.50% for publically avialble UAV communication dataset. Furthermore, the presented approach was verified by launching attacks in the system.

IoT was created to improve people's lives by enabling smart devices and apps to work together. One of the most serious concerns with IoT sector is the increasing privacy and security threats. Although various IDS models are designed to predict the security attacks, it faces several drawbacks. Therefore, Tanzila Saba et al. [23] suggested an anomaly identification framework based on convolutional neural system. This model examines the traffic, and analyses the IoT data to predict the security threats. Moreover, this method categorizes the traffic as normal and unusual traffic. The NID & BoT-IoT datasets were used to train and test this method. This technique obtained accuracy of 95.12% and 92.85% for NID and BoT-IoT datasets. However, the detection process consumes more time, and it is not efficient for large-scale datasets.

The ability to connect sensors and shooters directly is made possible by the integrating of ML and artificial intelligence into the cyberspace infrastructure without human control. The cyber data includes network data, military data, application data, etc. Hence, to protect these data from hackers, and attackers IDS methodology was designed. MarcChaléNathaniel D. Bastian et al [24] created an IDS framework based on Generative adversarial network and auto coders. This model helps in labelling the cyber data as benign or injected by processing the database. In this model, the database as collected and then it is analysed in the system with certain criteria for classification. However, training this model requires huge database.

One of the biggest challenges in communication networks is the timely and accurate identification of security attacks, and threats. Various techniques are already developed to detect the network vulnerabilities. However, they face issues in continuous monitoring and accurate detection. Hence, Emad-ul-HaqQazi et al. [25] created an efficient DL-based IDS methodology to identify the malicious data accurately. This model was validated with network benchmark datasets like KDD CUP'99. The accuracy achieved by this model is 97.14%. However, the classification of attacks is not possible in this method.

To protect the computer and communication networks from cyber-attacks, developing an effective IDS model is important. Recently, various IDS frameworks are developed based on ML algorithms to detect the cyber threats. However, they lack the standard feature set. To overcome this drawback, Mohanad Sarhan et al. [26] designed an IDS model based on Netflow meta-data collection protocol. The performances of this model are evaluated and verified with publically available datasets like CICIDS-2018, BoT-IoT, and ToN-IoT. Moreover, a tree classifier is incorporated in this protocol to classify the attack types. This model earned better results compared to traditional ML algorithms like SVM, DT, and RF. However, the timely detection is a challenging factor in this approach.

Vinayakumar Ravi et al. [27] designed an end-to-end security framework, which detects and classifies the network threats effectively. This framework deploys kernel-based principal component analysis, and recurrent neural system to extract the important features from the dataset. In addition, the dataset was pre-processed to filter the dataset in its initial stage. Additionally, this method uses an ensemble meta-classifier to classify the different kinds of attacks. The experimental results verify the accuracy, precision, & recall capabilities of the suggested approach. This model gained accuracy of 97.12%. However, the implementation of this model is highly complex.

Giovanni Apruzzese et al. [28] developed a network IDS model with supervised machine learning algorithm. This method integrates the machine learning features and cyber detection protocol attributes to detect the security threats. This model was tested with labelled dataset and the performances are estimated. Although this model provides timely attack detection in the network application, this method cannot identify unknown attacks. To identify unknown attacks, the system must be trained further using complex protocols. Thus, increases the system complexity, and computational time.

In recent times, IoT is emerging as the backbone of virtual applications. However, the advancements in IoT technologies increases the possibilities of data injection in the network. Hence, many researchers were conducted to resolve the security, and privacy issues. However, they face significant challenge in identifying the injected data from the dataset. Therefore, et al [29] created a cyber security method based on blockchain technology. The incorporation of blockchain in IoT network helps in processing the huge dataset with greater security. Moreover, the developed provides highest security against Denial of Service (DoS) attacks. Further, the presented scheme is evaluated with existing machine learning approaches like RF, XGBoost, etc for IoT-based datasets like BoT-IoT, CICIDS, etc.

The major contribution of the presented IDS framework is listed below,

- Initially, the publically available network intrusion datasets (NSLKDD and CICIDS) are gathered and imported into the python system.
- Then a hybrid optimized deep learning technique (AbRNN) was developed in the system with security parameters.
- The raw dataset was filtered in the hidden layer of RNN to eliminate the null values and error data.
- Further, the antlion optimal fitness is integrated to track the important data features and then; to detect the injected data, the retrieved features are cross-checked with learned features.
- Moreover, a user authentication module was created with login strategy to improve the network security.
- Finally, the performances are evaluated and verified with existing approaches in terms of accuracy, precision, recall, and f1-score.

3. SYSTEM MODEL AND PROBLEM STATEMENT

Various ID techniques have been used in the past with improved results for incursion forecasting. The intrusion's harmfulness, however, was the fundamental reason why the prevention technique was constrained. However, the network application avoidance system is the module that is most appreciated for protecting user data privacy. On the basis of the cryptosystems, some preventative measures have been developed for network applications. Therefore, if an attack breaks the algorithm, the raw data is collapsed and compromised by malevolent events. Therefore, the purpose of the current paper is to provide a mechanism for protecting network users against damaging DDoS attacks. Additionally, constant tracking of internet users is not possible with the current intrusion model. The only detection offered by this architecture is for assault nodes. But the current intrusion strategy does not allow for the removal of attack nodes from network applications. In order to ignore the assault nodes and enable ongoing network monitoring, a novel penetration model is created. As a result, a cutting-edge Buffalo-based Elman Neural Model (BENM) was created to constantly check login circumstances and block rogue users from the network.

4. PROPOSED ABRNN IDS FRAMEWORK

A novel Antlion-based Radial Neural Network (AbRNN) framework was developed in this article to identify network data security threats. The presented method combines the attributes of antlion optimization and radial basis neural function to track and detect the injected data. Moreover, a user verification module was created with certain login criteria to validate the original user. In the presented framework, initially the network is intrusion datasets CICIDS and NSLKDD was collected from Kaggle site. AbRNN Framework is shown in Figure 1.

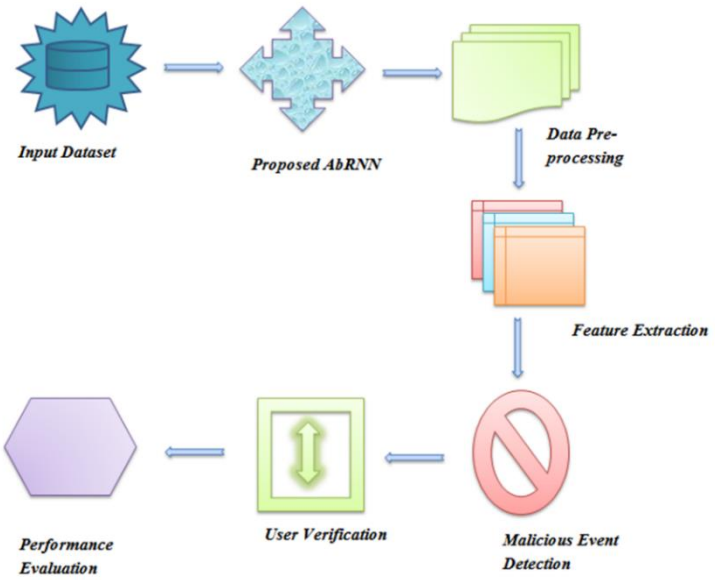

Figure 1. AbRNN Framework

These input datasets are then filtered making use of the RBNN hidden layer's pre-processing function. Further, an antlion optimal fitness solution was in integrated in the classification layer to track and select the important data features. These tracked data features are compared with trained data features to classify the normal and injected data.

The introduced framework is illustrated in Figure 1. The developed scheme was trained and tested in the python software and the outcomes are compared with the existing techniques.

4.1. AbRNN Layers

The AbRNN scheme consists of five different layers namely, input layer, hidden layer (HL), classification layer (CL), optimization layer, and output layer. In the first layer the system is initialized with the acquired intrusion dataset. In the second layer, the pre-processing function is embedded to clear the error or null features provide in the dataset. In the third layer, the meaningful and meaningless features are classified and the meaningless features are neglected from the system. Layers of AbRNN is shown in Figure 2.

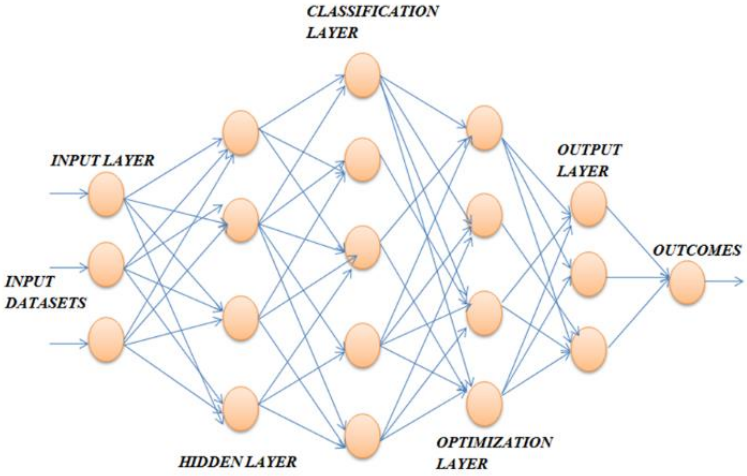

Figure 2. Layers of AbRNN

In the fourth layer, the ant lion fitness solution is integrated to detect and neglect the malicious events present in the dataset. In the final layer, the outcomes of the provided scheme are estimated in terms of accuracy, precision, recall, and f-measure. The layer of the AbRNN model is displayed in Figure 2.

4.1.1. Dataset Pre-processing

To initialize the detection of intrusions process, the intrusion detection datasets namely, NSLKDD and CICIDS are collected from the site (Kaggle). Then, the collected dataset is imported into the python system and initialized for further processing. The dataset initialization is represented in Eqn. (1).

$$Fi_{IDS} = [N_{i1}, N_{i2}, N_{i3}, N_{i4}, \ldots, N_{ik}] \quad (1)$$

Where, Fi_{IDS}refers to the intrusion detection function, $N_i$indicates the data provide in the dataset, and $m$denotes the total data count in the dataset. The imported dataset contains error or null features in it. Hence, after initialization the dataset is pre-processed to eliminate the error features. The pre-processing of the dataset increases the system accuracy, and lowers the network complexity. Here, the pre-processing function is applied to the AbRNN HL to reduce the complexity. The pre-processing function is expressed in Eqn. (2).

$$K_s(iIDS) = \sum_{i=0}^{k}\left(-N_i^{''} + N_i\right) + \alpha(iIDS) \quad (2)$$

Where, K_s indicates the filtering function,N_i''represents the noise data, and αrefers to the filtering variable. However, for identifying the malicious events extracting the dataset features is important. The pre-processed dataset contains both meaningful and meaningless features in it. Hence, the feature extraction module is designed in the developed model to classify the meaningful and meaningless separately.

4.1.2. Feature Extraction

In the proposed scheme, the feature extraction function is integrated into the classification layer. Once, the dataset enters into the CL the feature extraction function starts to separate the meaningless and meaningful features. After classification, the meaningless features are removed from the system to minimize the time consumption, and resource usage. The feature extraction function is formulated in Eqn. (3).

$$Y_{ex} = \frac{(mf, m''f) \times iIDS}{\beta(pf - m''f)} \quad (3)$$

Here, Y_{ex} refers to the feature extraction function, mf denotes the meaningful features, $m''f$ indicates the meaningless features, pf represents the present features and β refers to the feature tracking variable. The extracted features contain both malevolent and benign features. Thus, to detect the malicious events provide in the dataset the optimization layer is developed in the proposed system. This layer is interconnected with the classification layer to effectively detect the malicious events. In the optimization layer, the ant lion fitness solution is incorporated to increase the detection accuracy. The malicious event classification is expressed in Eqn. (4).

$$C_F(iIDS) = \begin{cases} if\left(E_f^{'} = t_f\right); Benign \\ else; Malicious \end{cases} \quad (4)$$

Where, C_F represents the event classification function, $iIDS$ defines the intrusion dataset, t_f indicates the trained features, and $E_f^{'}$ refers to the extracted features. If the trained features match with the extracted features, it is represented

as “Benign” or it is represented as “Malicious features”. After malicious event classification, the proposed model neglects it from the system.

4.1.3. Verification Module

To authenticate the network users, the verification module was developed in the system. This module consists of user login conditions namely, user-id, and passwordEvery user on the network has a different password and user ID. The user's password and user ID must be entered correctly in order to access the file or data. If the user-id and password match the system permits the user to access file. On the other hand, if the login conditions not match then the system denies the user’s request.

$$V_{us} = match \begin{cases} if\,(U_{L(id,pw)} = 1); AccessFile \\ if\,(U_{L(id,pw)} \neq 1); AccessDenied \end{cases} \quad (5)$$

Where, V_{us} refers to the user verification function, U_L indicates the user login conditions, id denotes the user-id, and pw denotes the password. It is set that if the login conditions are equal to one, then the user-id, and password entered by the user is correct. On the other hand, if the login conditions are not equal to one, then the user-id, and password entered by the user is not correct. Hence, the system displays as “Access Denied”. Flowchart of AbRNN is shown in Figure 3.

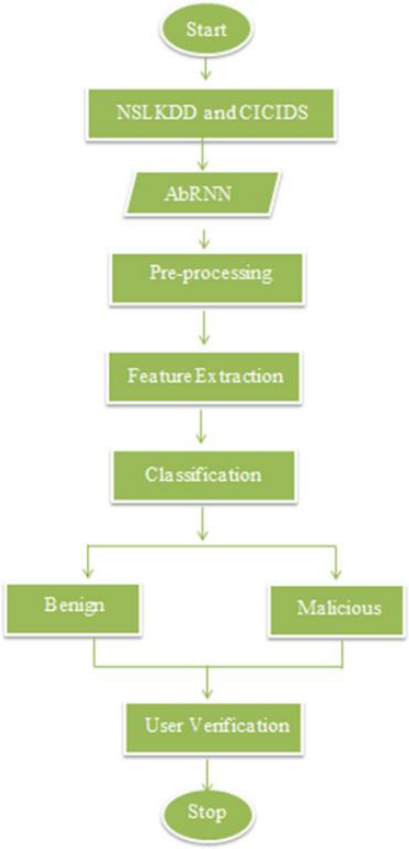

Figure 3. Flowchart of AbRNN

Pseudo code
Step 1: Import and initialize the input dataset (NSLKDD and CICIDS) into the system.
Step 2: Train and pre-process the dataset utilizing the AbRNN method to remove the error or null features.
Step 3: Extract the features present in the dataset in feature extraction module.
Step 4: Train the extracted features to detect and neglect the malicious features.
Step 5: Create the user verification module with login strategy.
Step 6: Match the user login parameters (user-id, and password) to identify the authenticated users.
Step 7: If parameters matches “File Access”, else “Access denied”.
Step 8: Terminate the process.

The flowchart of the suggested technique is displayed in Figure 3. Moreover, the step-by-step working procedure is illustrated in pseudo code format.

5. RESULT AND DISCUSSION

In this paper, an optimized neural system-based IDS framework was proposed to predict the malicious events in the network. To validate the presented approach, the IDS dataset was collected and initialized in the system. Further, the dataset was filtered and the important features are tracked and extracted for prediction purposes. In addition, a user verification module was designed to provide continuous

monitoring in the network. Parameter Specification is shown in Table 1.

Table 1. Parameter Specification

Tool	Specification
Platform	Python
Version	3.12
OS	Windows 10
Datasets	NSL-KDD and CICIDS
Application	Network

The suggested framework was implemented in the python software version 3.12 and the results are evaluated separately for both datasets (NSL_KDD and CICIDS). The parameter description is tabulated in Table 1. Moreover, a comparative assessment was performed to validate the performances of the presented method.

5.1. Performance Assessment

In performance evaluation, the outcomes of the presented system such as precision, accuracy, recall, and f-measure are determined by executing it in the python software. Moreover, to manifest the efficacy of the presented algorithm the results are compared with some existing techniques like K-Nearest Neighbour_ Double Exponentially Weighted Moving Average (KNN_DEWMA) [32], Hybrid Trust Management Scheme (HTMS) [33], Real-Time Security System using Convolutional Neural Network (RTSS_CNN) [34], and Detection of Malicious Events using Learning Automata (DMELA) [35].

5.1.1. Accuracy

Accuracy is a performance metrics, which indicates how exactly the presented approach identifies the malicious events in the network. It is determined by dividing the positive prediction by total predictions. The accuracy calculation is formulated in Eqn. (6)..

$$P_{ac} = \frac{m^{+}+m^{-}}{m^{+}+m^{-}+n^{+}+n^{-}} \quad (6)$$

Where,P_{ac}represents the detection accuracy, m^{+} ,m^{-}, $n^{+}$and n^{-}denotes the true-positive (TP), true-negative (TN), false-positive (FP), and false-negative (FN), respectively. Accuracy Validation is shown in Figure 4.

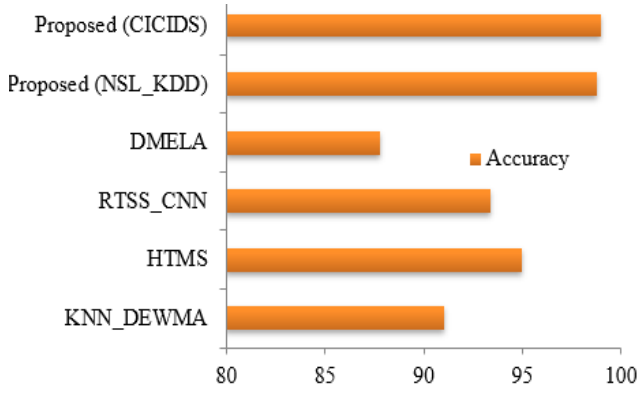

Figure 4. Accuracy Validation

The accuracy of the suggested model was validated by comparing it with the traditional techniques like KNN_DEWMA, HTMS, RTSS_CNN, and DMELA. The accuracy validation is displayed in Fig 4. Here, the same NSL_KDD and CICIDS dataset are considered to determine the accuracy of the existing approaches. The accuracy obtained by the traditional scheme for the network dataset is 91%, 95%, 93.4%, and 87.8%, respectively. But, the suggested scheme attained higher accuracy of 98.5% and 98.96% for NSLKDD and CICIDS datasets. This comparative assessment verifies that the presented method accurately detects the malicious event in the network.

5.1.2. Recall

In network security model, recall is an important performance parameter that represents the relevant instances among the total retrieved instances. It is determined as the ratio of TP to the FN, and TP. The recall formula is expressed in Eqn. (7).

$$Rl_{c} = \frac{m^{+}}{m^{+}+n^{-}} \quad (7)$$

Here, Rl_{c}refers to the system recall percentage. Recall Comparison is shown in Figure 5.

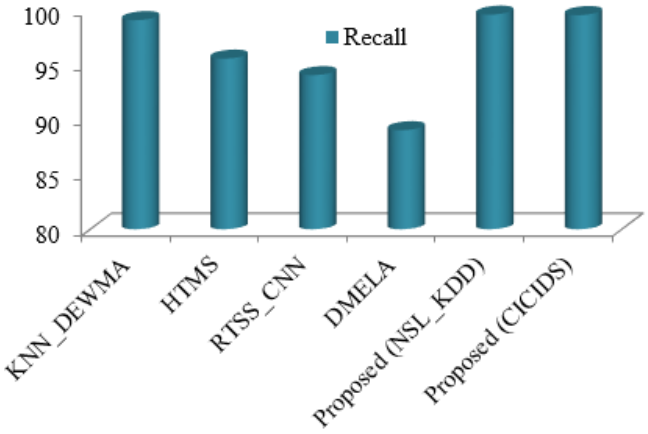

Figure 5. Recall Comparison

The evaluation of system recalls in relation to current methods sis shown in Figure 5. Recall is the metric, which represents the relevant total positive attack detection out of the positive and negative predictions of the system. From the comparative recall performance, it is observed that the suggested approach earned greater recall of 99.75% which is very high compared to the recall attained by existing approaches like KNN_DEWMA, HTMS, RTSS_CNN, and DMELA. The recall achieved by the traditional event detection is 97%, 95.5%, 94%, and 89%.

5.1.3. Precision

Precision refers to the Out of all the good outcomes, correct forecasts made up a majority. The true-positive number is divided by the TP and FP to determine how accurate the network method is. It is seen in Eqn. (8).

$$Pi_{cs} = \frac{m^{+}}{m^{+}+n^{+}} \quad (8)$$

Where,Pi_{cs} indicates the precision percentage. Precision Comparison is shown in Figure 6.

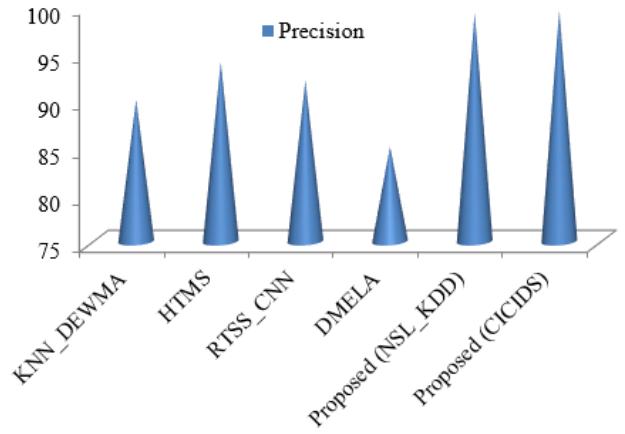

Figure 6. Precision Comparison

The validation of system's precision with different methods is illustrated in Figure 6. The precision percentage obtained by the recent approaches like KNN_DEWMA, HTMS, RTSS_CNN, and DMELA is 90%, 94%, 92%, and 85%, respectively. But the provided approach achieved greater precision of 99.10% and 99.43%, for NSL_KDD and CICIDS datasets, respectively. The higher precision indicates that the developed model detects the malicious data accurately.

5.1.4. F-measure

F-measure indicates the performance of recall and precision. It combines combining the recall & precision numbers into one. By dividing the sum of recall and precision, it is calculated value by their sum. The f-measure is formulated in Eqn. (9

$$F_{ms} = 2\frac{Pi_{cs} \times Rl_c}{Pi_{cs} + Rl_c} \quad (9)$$

Where, F_{ms} represent the f-measure. F-measure Comparison is shown in Figure 7.

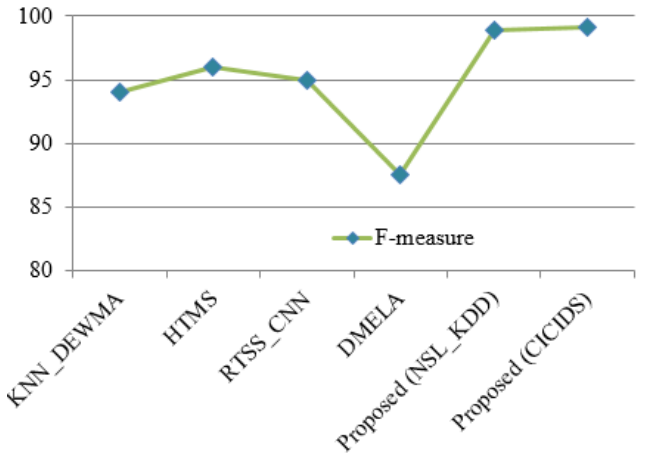

Figure 7. F-measure Comparison

The resulting model's f-measure is verified using various known techniques in Figure 7. Here, the existing techniques like KNN_DEWMA, HTMS, RTSS_CNN, and DMELA are implemented and tested with the same network datasets. The f-measure obtained by the traditional algorithms is 94%, 96%, 95%, and 87.5%, respectively. But the presented model earned higher f-measure of 98.78% and 99.07% for NSLKDD and CICIDS datasets. This shows that the recall and precision performance of the presented model is high compared to other techniques.

5.2. Discussion

A hybrid intrusion detection model was designed in this article to find harmful activities in a network dataset. The method being used was validated with the network datasets like NSLKDD and CICIDS. In the proposed technique, the input datasets are filtered and then the features are tracked to identify the malevolent events. In addition, to enhance the network security user verification module was developed in this approach. Comparative Assessment is shown in Table 2.

Table 2. Comparative Assessment

Techniques	***Accuracy***	***Precision***	***Recall***	***F-measure***
KNN_DEWMA	91	90	97	94
HTMS	95	94	95.5	96
RTSS_CNN	93.4	92	94	95
DMELA	87.8	85	89	87.5
Proposed (NSLKDD)	98.5	99.1	99.75	98.78
Proposed (CICIDS)	98.96	99.43	99.46	99.06

Finally, the presented model performances are measured for precision, recall, f-measure, and accuracy. A comparison analysis was also carried out for validation purposes. Table 2 lists the overall comparative analysis.

6. CONCLUSION

Recently, the combination of advanced information and digital technologies in IOT systems increased the security concerns in network applications. Hence, an optimized deep network-based IDS model was developed in this article. This model integrates the attributes of Antlion optimization, and RBNN to predict the attack data effectively. Moreover, a user authentication module was incorporated to provide continuous monitoring in the network. This module permits only authenticated user to access the data/file in the network application. The developed framework was executed and tested with two IDS datasets namely: NSL-KDD, and CICIDS. Finally, the results are evaluated and compared with the traditional IDS schemes for validation purposes. In addition, the performance enhancement score is also determined from the comparative assessment. It is observed that in the suggested approach, the performances like precision, accuracy, f-measure, and recall are improved by 5.43%, 5.56%, 4.04%, and 4.06%, respectively. This shows

that the proposed scheme accurately detects the malicious data in the network application.

CONFLICTS OF INTEREST

This paper has no conflict of interest for publishing.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat, M. Alazab, and T. R. Gadekallu, "Federated learning for intrusion detection system: Concepts, challenges and future directions," *Computer Communications*, vol. 195, pp. 346-361, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] A. Thakkar, and R. Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," *Artificial Intelligence Review*, vol.55, no. 1, pp. 453-563, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] W. Lo, H. Alqahtani, K. Thakur, A. Almadhor, S. Chander, and G. Kumar, "A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic," *Vehicular Communications*, vol. 35, pp. 100471, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] W. Lo, W. Layeghy, S. Sarhan, M. Gallagher, M., and M. Portmann, "E-graphsage: A graph neural networkbased intrusion detection system for iot," In *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, pp. 1-9, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] N. Gupta, V. Jindal, and P. Bedi, "CSE-IDS: Using cost-sensitive deep learning and ensemble algorithms to handle class imbalance in network-based intrusion detection systems," *Computers and Security*, vol. 112, pp. 102499, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. A. Khan, "Performance analysis of machine learning algorithms in intrusion detection system: A review," *Procedia Computer Science*, vol. 171, pp. 1251-1260, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory*, vol. 101, pp. 102031, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] A. Drewek-Ossowicka, M. Pietrołaj, and J. Rumiński, "A survey of neural networks usage for intrusion detection systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 497-514, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu, I. Kevin, and K. Wang, "Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9310-9319, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] M. T. Nguyen, and K. Kim, "Genetic convolutional neural network for intrusion detection systems," *Future Generation Computer Systems*, vol. 113, pp. 418-427, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, "Intrusion detection system for healthcare systems using medical and network data: A comparison study," *IEEE Access*, vol. 8, pp.106576-106584, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] R. V. Mendonça, A. A. Teodoro, R. L. Rosa, M. Saadi, D. C. Melgarejo, P. H. Nardelli, and D. Z. Rodríguez, "Intrusion detection system based on fast hierarchical deep convolutional neural network," *IEEE Access*, vol. 9, pp. 61024-61034, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] L. Ashiku, and C. Dagli, "Network intrusion detection system using deep learning," *Procedia Computer Science*, vol. 185, pp. 239-247, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] H. Choi, M. Kim, G. Lee, and W. Kim, "Unsupervised learning approach for network intrusion detection system using autoencoders," *The Journal of Supercomputing*, vol. 75, pp. 5597-5621, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] A. R. Gad, A. A. Nashat, and T. M. Barkat, "Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset," *IEEE Access*, vol. 9, pp. 142206-142217, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, "Netflow datasets for machine learning-based network intrusion detection systems," *In Big Data Technologies and Applications: 10th EAI International Conference, BDTA 2020, and 13th EAI International Conference on Wireless Internet, WiCON 2020, Virtual Event, December 11, 2020, Proceedings* vol. 10, pp. 117-135, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] G. D. C. Bertoli, L. A. P. Júnior, O. Saotome, A. L. Dos Santos, F. A. N. Verri, C. A. C. Marcondes, and J. M. P. De Oliveira, "An end-to-end framework for machine learning-based network intrusion detection system," *IEEE Access*, vol. 9, pp. 106790-106805, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] P. Devan, and N. Khare, "An efficient XGBoost–DNN-based classification model for network intrusion detection system," *Neural Computing and Applications*, vol. 32, no. 16, pp. 12499-12514, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] A. Yang, Y. Zhuansun, C. Liu, J. Li, and C. Zhang, "Design of intrusion detection system for internet of things based on improved BP neural network," *IEEE ACCESS*, vol. 7, pp. 106043-106052, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[20] S. Huang, and K. Lei, "IGAN-IDS: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks," *Ad Hoc Networks*, vol. 105, pp. 102177, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] J. Yu, X. Ye, and H. Li, "A high precision intrusion detection system for network security communication based on multi-scale convolutional neural network," *Future Generation*

Computer Systems, vol. 129, pp. 399-406, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Q. Abu Al-Haija, and A. Al Badawi, "High-performance intrusion detection system for networked UAVs via deep learning," *Neural Computing and Applications*, vol. 34, no. 13, pp.10885-10900, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Computers and Electrical Engineering*, vol. 99, pp. 107810, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] M. Chalé, and N. D. Bastian, "Generating realistic cyber data for training and evaluating machine learning classifiers for network intrusion detection systems," *Expert Systems with Applications*, vol. 207, pp. 117936, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] M. Imran, N. Haider, M. Shoaib, and I. Razzak, "An intelligent and efficient network intrusion detection system using deep learning," *Computers and Electrical Engineering*, vol. 99, pp. 107764, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] M. Sarhan, S. Layeghy, and M. Portmann, "Towards a standard feature set for network intrusion detection system datasets," *Mobile networks and applications*, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] V. Ravi, R. Chaganti, and M. Alazab, "Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system," *Computers and Electrical Engineering*, vol. 102, pp. 108156, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[28] G. Apruzzese, L. Pajola, and M. Conti, "The cross-evaluation of machine learning-based network intrusion detection systems," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 5152-5169, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[29] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, "A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 55-68, 2022.[CrossRef] [Google Scholar] [Publisher Link]

[30] Y. Deng, X. Zhou, J. Shen, G. Xiao, H. Hong, H. Lin, and B. Q. Liao, "New methods based on back propagation (BP) and radial basis function (RBF) artificial neural networks (ANNs) for predicting the occurrence of haloketones in tap water," *Science of The Total Environment*, vol. 772, pp. 145534, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[31] L. Abualigah, and D. Ali "A novel hybrid antlion optimization algorithm for multi-objective task scheduling problems in cloud computing environments," *Cluster Computing*, vol. 24 pp. 205-223, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[32] F. Harrou, M. M. Hittawe, Y. Sun, and O. Beya, Malicious attacks detection in crowded areas using deep learning-based approach," *IEEE Instrumentation and Measurement Magazine*, vol. 23, no. 5, pp. 57-62, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[33] F. Ahmad, F. Kurugollu, C. A. Kerrache, S. Sezer, and L. Liu, "Notrino: A novel hybrid trust management scheme for internet-of-vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 9244-9257, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[34] M. V. de Assis, L. F. Carvalho, J. J. Rodrigues, J. Lloret, and M. L. Proença Jr, "Near real-time security system applied to SDN environments in IoT networks using convolutional neural network," *Computers and Electrical Engineering*, vol. 86, pp. 106738, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[35] R. R. Rout, G. Lingam, and D. V. Somayajulu, Detection of malicious social bots using learning automata with url features in twitter network," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 4, pp. 1004-1018, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[36] S. Gokul Pran, S. Raja, "An efficient feature selection and classification approach for an intrusion detection system using Optimal Neural Network," *Journal of Intelligent and Fuzzy Systems*, vol. 44, no. 5, pp. 8561-712023. [CrossRef] [Google Scholar] [Publisher Link]

[37] S. G. Pran, S. Raja, S. Jeyasudha "Intrusion detection system based on the beetle swarm optimization and K-RMS clustering algorithm," *International Journal of Adaptive Control and Signal Processing*, vol. 38, no. 5, pp. 1675-89, 2024. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

D. Lavanya, is a computer science and engineering working at Golden Valley College in Madanapalle, affiliated with Jawaharlal Nehru Technological University (JNTUA) in Anantapur, Andhra Pradesh, where she is passionate about technology and innovation.

Kannan Ramakrishnan received the M.E. degrees in the Department of Electronics and Communication Engineering from Anna University Chennai in 2010. In Jan 2022 – till now: Assistant Professor, Saveetha Engineering College. Dec 2020 – Jan 2022: Assistant professor, Sri Venkateswara College of Engineering and Technology, Chitoor. Apr 2018 –Apr 2020: Assistant professor, Saveetha School of engineering, SIMATS. Area of interest VLSI, Digital electronics CMOS integrated circuits, Embedded systems.

Arrived: 30.01.2024
Accepted: 26.02.2024