



ISSN: 2321-2152

**IJMECE**

*International Journal of modern  
electronics and communication engineering*

E-Mail

[editor.ijmece@gmail.com](mailto:editor.ijmece@gmail.com)

[editor@ijmece.com](mailto:editor@ijmece.com)

[www.ijmece.com](http://www.ijmece.com)

# IOT-ENABLED CYBERSECURITY INFRASTRUCTURES DETECT REAL-TIME MALICIOUS INTRUSIONS AND ATTACKS

K YATHEENDRA<sup>1</sup>, SEMBEDI THULASI PRASANNA<sup>2</sup>, T ANIL KUMAR<sup>3</sup>, K KAVITHA<sup>4</sup>

<sup>1</sup>Associate Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur,  
Email: k.yatheendra84@gmail.com

<sup>2</sup>P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email:  
thulasitharu31@gmail.com

<sup>3</sup>Associate Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur,  
Email: [anil.thumburu@gmail.com](mailto:anil.thumburu@gmail.com)

<sup>4</sup>Assistant Professor, Department of MCA, Madanapalli Institute of Technology and Science,  
Email: kavithagoud32@gmail.com

**Abstract:** The undertaking underscores intrusion detection as a proactive insurance against PC infections, malware, and threatening assaults on PC organizations. The task utilizes DL out how to find and relieve cybersecurity weaknesses and breaks in IoT-driven digital actual frameworks to further develop security. By further developing accuracy, detection efficacy, and false positives, the drive expects to further develop ID. This features network safety advancement. A state of the art DL approach, generative adversarial networks, are utilized to meet task objectives. It likewise differentiates unsupervised and deep learning-based discriminative calculations, showing a total and effective network protection philosophy. Our concentrate successfully coordinated various models into a ensemble method to further develop forecasting accuracy. CNN+LSTM, a hybrid architecture, is eminent. This hybrid model has almost 100% accuracy on the KDD-Cup dataset, demonstrating our ensemble technique for intrusion detection in IoT-based cybersecurity systems.

**Index terms** - Cybersecurity, Internet of Things, intrusion detection system (IDS), anomaly detection, security attacks, deep learning.

## 1. INTRODUCTION

Deep learning (DL) approaches benefit many cycles, including artificial neural networks, by utilizing different administrators. It has information, yield, and secret layers [2], [3]. Notwithstanding, DL layers are nonlinear and answer approaching information. DL techniques have been used to track down realistic, picture, sign, and discourse and sound acknowledgment as of late. Clinical hereditary qualities and disease treatment utilize DL learning techniques broadly [4]. Picture, text, and numeric ordered progressions are utilized in the DL procedures to show how to oversee immense information with forward and backpropagation strategies. How gadgets change values and hyperparameters with aspects to process test size delivering the various layers is another point. Effective procedures scarcely change among testing and preparing show and portrayal. A slight variety from the family's quality and primary

preparation strategies causes out of date shrewdness [5]. Protection and security are significant since numerous spaces have accepted and embraced DL draws near. Information travel between encoded structures in training, testing, and connection point modules is crucial to DL draws near. All models' training DL depends on monstrous, classified, and delicate client information, generally training information [6].

The following layer of guard is intrusion detection systems (IDS). [7]. IDS screens dubious movement and tells while found, working with verification, security frameworks, and encryption to safeguard against cyberattacks. IDS recognizes pernicious from non-malevolent action utilizing harmless traffic/ordinary stream designs and definite assault explicit measures [8]. Information mining depicts and sends IDSs with tough way of behaving and more noteworthy accuracy than standard IDSs that might impact current, modern cyberattacks. [9]. Organizations are anxious about protecting critical infrastructure (CI), strikingly Internet Industrial Control Systems (IICs), as IIoT gadgets increment [4]. Industrial Control Systems (ICS) oversee fundamental control works and muddled undertakings utilizing equipment, programming, administrators, and correspondences. Online IICs network attacks have been identified by various intrusion detection systems (IDS) in the writing. Most contemporary IDSs have difficult issues in their procedures and evaluation measures. This study utilizes deep-autoencoder-based LSTM model/technique to make a compelling IDS for IIoT-fueled IICs with low detection rate and high FPR.[42]

Secret or basic data should not be uncovered by means of DL procedures. An ID gadget is normally programming or an actual gadget that screens showing up and leaving local area guests for malignant exercises or security breaks. IDS and IDS arrangements educate overseers regarding any activity that could hurt information or organization foundations, similar to gatecrasher cautions. IDS innovations break down your local area's bundles and organization guest types for odd way of behaving or indications of a capacity split the difference. ID structures are generally inactive, albeit some can mediate when they recognize unsafe way of behaving. They're generally for constant perceivability during limit local area splits the difference. Numerous IDS items act distinctively founded on the ID gear utilized. A network intrusion detection system (NIDS) [10] cautiously puts sensors across the network. These sensors will screen local area visits without influencing execution or deterrents. Host-based comprehensive intrusion detection systems (HIDS) follow visits to specific gadgets and servers [7].

## 2. LITERATURE SURVEY

The ImageNet LSVRC-2010 challenge's 1.2 million high-goal photographs were characterized into 1000 classes utilizing an immense, deep convolutional neural network. We accomplished top-1 and top-5 blunder paces of 37.5% and 17.0% on test information, obviously better than the earlier cutting edge. [2] The 60 million-boundary brain network involves 650,000 neurons, five convolutional layers, some maximum pooling layers, and three completely associated layers with a 1000-way softmax. We utilized non-soaking neurons and a GPU-effective convolution execution to accelerate preparing. An as of late found regularization

approach named "dropout" decreased overfitting in completely associated layers very well. In the ILSVRC-2012 contest, we entered a variation of this model and won top-5 test blunder rate with 15.3%, contrasted with 26.2% for the second-best passage.

Skin cancer is strange tissue improvement that can kill. It has become quite possibly of the most risky danger in the body. Patient perseverance can be worked on by early identification. Detecting skin disease is testing. Clinical picture conclusion currently profits by PC vision. Innovation and PC accessibility have prompted the advancement of ML methods and DL models for clinical picture examination, outstandingly skin injury pictures. In this article [3], we present a DL model with picture pre-handling stages that characterizes skin sores better than past models. Pre-handling stages recognize harmless and dangerous HAM10000 disease sores utilizing standardization, information decrease, and information expansion. The trial result showed 96.10% preparation precision and 90.93% testing exactness for the recommended model. This model runs rapidly and pleasantly.[44]

IDS are fundamental for network security. It is a second insurance against many attacks [31, 32, 33, 40]. Powerlessness to distinguish new dangers with high recognition rate and low deception rate is the primary constraint of existing IDSs. In [4], we present an IDS in light of classifier tree likelihood forecasts. Our model has 2 layers. Initial, a classifier tree. A classifier joins tree likelihood forecasts in the subsequent layer. Every hub in the 4-level tree addresses a classifier. The initial hub groups associations into Forswearing of Administration assaults and Bunch 2. The subsequent hub characterizes Bunch 2 and Group 3 testing assaults associations. In Remote-to-Neighborhood assaults and

Bunch 4, the third hub recognizes Group 3 associations. Group 4's Client to-Root and Ordinary associations are arranged by the last hub. The last classifier in the subsequent layer consolidates the principal layer's likelihood forecasts and makes the last judgment. Our model has the most minimal deception rate and greatest recognition rate in KDD'99 and NSL-KDD preliminaries. Our model is more precise than past IDS models, with 96.27% for KDD'99 and 89.75% for NSL-KDD 33], [34], [35], [36], [37], [38], [39], [40].

This review offers a novel IDS that coordinates REP Tree, JRip calculation, and Forest PA classifiers in light of decision trees and rules [5]. The first and second strategies order network traffic as Assault/Harmless utilizing informational collection credits. The third classifier inputs the first and second classifier results and beginning informational collection qualities. The proposed IDS beats cutting edge frameworks in exactness, recognition rate, deception rate, and time above, as per CICIDS2017 dataset examination.

Innovation's quick development and extended interconnectedness present new network safety issues. Industry experts and the scholarly world are cooperating to develop IDS with high accuracy, negligible intricacy, and quick reaction to this rising pattern in PC assaults. [6] This article depicts current Interruption Identification Frameworks (IDS) and its key standards [7]. This paper likewise talks about whether information mining and information disclosure might be utilized to make information mining-based IDSs that are more accurate at detecting novel intrusions and stronger than conventional IDSs [6, 7].





The exploration looks at intrusion detection system training and assessment datasets here. Investigate KDDCUP99, NSL KDD, and UNSW-NB15 datasets to grasp their items, attributes, and construction. This stage gives information bits of knowledge.

duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	rst	...	dst_host_srv_count
0	0	tcp	SYN	181	5430	0	0	0	0	...	0
1	0	tcp	SYN	230	440	0	0	0	0	...	10
2	0	tcp	SYN	245	1307	0	0	0	0	...	20
3	0	tcp	SYN	219	1307	0	0	0	0	...	30
4	0	tcp	SYN	217	2032	0	0	0	0	...	40
...	...	...	...	...	...	...	...	...	...	...	...
#44016	0	tcp	SYN	210	1001	0	0	0	0	...	200
#44017	0	tcp	SYN	202	2080	0	0	0	0	...	200
#44018	0	tcp	SYN	203	1001	0	0	0	0	...	400
#44019	0	tcp	SYN	201	1300	0	0	0	0	...	200
#44020	0	tcp	SYN	219	1234	0	0	0	0	...	200

Fig 2 KDDCUP dataset

Scholastic analysts utilize KDDCup99, NSL-KDD, and UNSW-NB15 to dissect destructive activities and identify changed dangers. The NSL-KDD dataset broadens KDD99 and eliminates unnecessary information from training and testing and determines how much keeps in each group. The dataset contains 42 qualities in three classes: traffic, endlessly satisfied. The KDDCup 99 dataset is famous in IoT online protection [33], [34], [35], [36], [37], [38], [39], [40]. From the evaluation program DARPA98 IDS, this dataset contains named and unlabeled training and testing information for seven and fourteen days [33]. To deliver reasonably forceful ways of behaving and assaults, perfectStorm (IXIA) and the UNSW Digital Reach Lab produced the UNSW-NB15 dataset. Each dataset record contains 47 properties, isolated into 10 classifications: Secondary passages, DoS, Examination, Exploits, Conventional, Surveillance, Fuzzers for Strange Movement, Shellcode, and Worms.[48]

#### iv) Data Processing:

ata processing transforms raw information into business-helpful data. Information researchers accumulate, sort out, clean, check, break down, and orchestrate information into diagrams or papers. Data can be handled physically, precisely, or electronically. Data ought to be more significant and decision-production simpler. Organizations might upgrade activities and settle on basic decisions quicker. PC programming improvement and other mechanized information handling innovations add to this. Big data can be transformed into significant bits of knowledge for quality administration and independent direction.

#### v) Feature selection:

Feature selection chooses the steadiest, non-repetitive, and pertinent elements for model turn of events. As data sets extend in amount and assortment, purposefully bringing down their size is significant. The fundamental reason for feature selection is to increment prescient model execution and limit processing cost.

One of the vital pieces of feature engineering is picking the main attributes for machine learning algorithms. To diminish input factors, feature selection methodologies take out copy or superfluous elements and limit the assortment to those generally critical to the ML model. Rather than permitting the ML model pick the main qualities, feature selection ahead of time enjoys a few benefits.

#### vi) Algorithms:

CNNs are planned explicitly to decipher information that looks like a lattice, similar to photos. They naturally and adaptively extricate a spatial order of qualities from the info information utilizing

convolutional layers. In assignments including picture and video acknowledgment, CNNs are habitually used.

```
verbose, epoch, batch_size = 1, 100, 4
activationFunction='relu'

def CNN():

    cnnmodel = Sequential()
    cnnmodel.add(Conv2D(filters=128, kernel_size=2, activation='relu', input_shape=(28, 28, 3)))
    cnnmodel.add(MaxPooling2D(pool_size=2))
    cnnmodel.add(Dropout(rate=0.2))
    cnnmodel.add(Flatten())
    cnnmodel.add(Dense(5, activation='softmax'))
    cnnmodel.compile(optimizer='adam', loss='categorical_crossentropy', metrics=['accuracy'])
    cnnmodel.summary()
    return cnnmodel

cnnmodel = CNN()
```

Fig 3 CNN

RNNs are made to handle successive contribution by keeping a memory or inner state. They handle approaching information in a circling way that empowers the organization to consider earlier setting. They are thusly proper for occupations including time-series information or groupings.

```
def create_model(input_shape):
    # Create model
    model = Sequential()
    model.add(LSTM(128, input_shape=input_shape, activation='relu', return_sequences=True))
    model.add(Dropout(0.2))
    model.add(LSTM(128, input_shape=input_shape, activation='relu', return_sequences=True))
    model.add(Dropout(0.2))
    model.add(LSTM(128, input_shape=input_shape, activation='relu', return_sequences=True))
    model.add(Dropout(0.2))
    model.add(LSTM(128, input_shape=input_shape, activation='relu', return_sequences=True))
    model.add(Dropout(0.2))
    model.add(Dense(10, kernel_initializer='uniform', activation='softmax'))
    model.add(Dense(1, kernel_initializer='uniform', activation='linear'))
    # compile model
    adam = tf.keras.optimizers.Adam(learning_rate=0.001, decay=0.00001)
    model.compile(loss='mse', optimizer=adam, metrics=['accuracy'])
    model.compile(loss='categorical_crossentropy', optimizer=adam, metrics=['accuracy'])
    return model

model = create_model(input_shape=(18, 1))
print(model.summary())
```

Fig 4 RNN

Consolidating **CNN with LSTM** utilizes LSTM's understanding and maintenance of fleeting connections as well as CNN's ability to separate spatial data from information (like pictures). For issues

requiring successive and geological information, this mixture strategy functions admirably [2], [11], [12], [13], [14], [15], [16], and [17].

```
import tensorflow as tf
tf.keras.backend.clear_session()

model = tf.keras.models.Sequential([tf.keras.layers.Conv2D(filters=64, kernel_size=3, strides=1, padding='valid'),
tf.keras.layers.MaxPooling2D(pool_size=2, strides=1, padding='valid'),
tf.keras.layers.Conv2D(filters=32, kernel_size=3, strides=1, padding='valid', activation='relu'),
tf.keras.layers.MaxPooling2D(pool_size=2, strides=1, padding='valid'),
tf.keras.layers.Flatten(),
tf.keras.layers.Dense(128, activation='relu'),
tf.keras.layers.Dropout(0.5),
tf.keras.layers.Dense(10, activation='softmax'),
tf.keras.layers.Dropout(0.5),
tf.keras.layers.Dense(1)

lr_schedule = tf.keras.optimizers.schedules.ExponentialDecay(
    decay_steps=10000,
    decay_rate=0.1,
    staircase=False)

model.compile(loss=tf.keras.losses.MeanSquaredError(),
optimizer=tf.keras.optimizers.Adam(learning_rate=lr_schedule, momentum=0.1),
metrics=['acc'])
model.summary()
```

Fig 5 CNN + LSTM

For unsupervised learning, **RBM** is a generative stochastic artificial neural network. Consolidating CNN and BiGRU proposes applying a blend of bidirectional gated recurrent layers (BiGRU) to record consecutive examples and convolutional layers for feature extraction (CNN), perhaps for unpredictable example recognition applications.

```
import tensorflow as tf
tf.keras.backend.clear_session()

model = tf.keras.models.Sequential([tf.keras.layers.Conv2D(filters=64, kernel_size=3, strides=1, padding='valid'),
tf.keras.layers.MaxPooling2D(pool_size=2, strides=1, padding='valid'),
tf.keras.layers.Conv2D(filters=32, kernel_size=3, strides=1, padding='valid', activation='relu'),
tf.keras.layers.MaxPooling2D(pool_size=2, strides=1, padding='valid'),
tf.keras.layers.Flatten(),
tf.keras.layers.Dense(128, activation='relu'),
tf.keras.layers.Dropout(0.5),
tf.keras.layers.Dense(10, activation='softmax'),
tf.keras.layers.Dropout(0.5),
tf.keras.layers.Dense(1)

lr_schedule = tf.keras.optimizers.schedules.ExponentialDecay(
    decay_steps=10000,
    decay_rate=0.1,
    staircase=False)

model.compile(loss=tf.keras.losses.MeanSquaredError(),
optimizer=tf.keras.optimizers.Adam(learning_rate=lr_schedule, momentum=0.1),
metrics=['acc'])
model.summary()
```

Fig 6 RBM

DNNs are highly viable in separating complex examples and qualities from the information since they are made out of a few layers of interconnected hubs

organized in a multi-facet perceptron design. They are widely used for regression and classification in an assortment of ML issues.

```
# encode the train data
x_train_encode = encoder.predict(X_train)
# encode the test data
x_test_encode = encoder.predict(X_test)
## So effectively, its like dimensionality reduction or feature extraction

# define the model
from sklearn.neural_network import MLPClassifier
model = MLPClassifier(random_state=1, max_iter=300)
## specifying max_iter = 200, to avoid the CONVERGENCE WARNING
## why do we get CONVERGENCE WARNING?
## because the model has converged already, but our loop is still training over many epochs.
## Reduce the epochs

# fit the model on the training set
model.fit(x_train_encode, y_train)

# make predictions on the test set
yhat = model.predict(x_test_encode)

# calculate classification accuracy
acc = accuracy_score(y_test, yhat)
```

Fig 7 DNN with MLP

#### 4. EXPERIMENTAL RESULTS

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

$$\text{Precision} = \frac{\text{True positives}}{(\text{True positives} + \text{False positives})} = \frac{TP}{TP + FP}$$

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

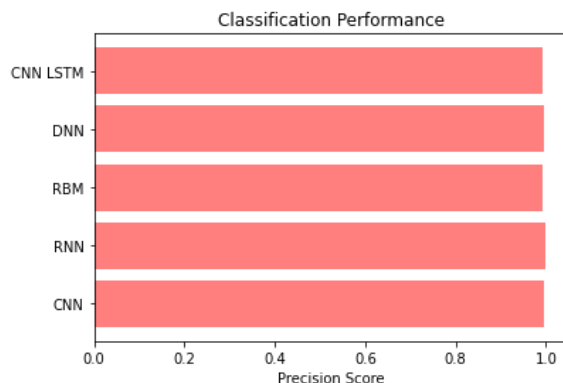


Fig 8 Precision comparison graph

**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.[50]

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

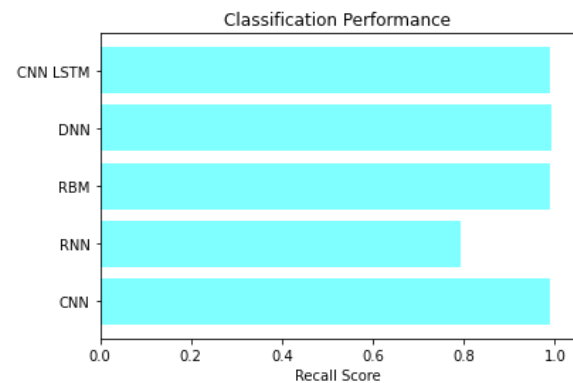


Fig 9 Recall comparison graph

**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:

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

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



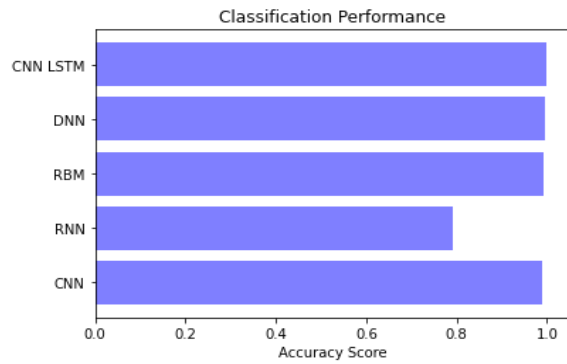


Fig 10 Accuracy graph

**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.

$$F1 \text{ Score} = 2 * \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} * 100$$

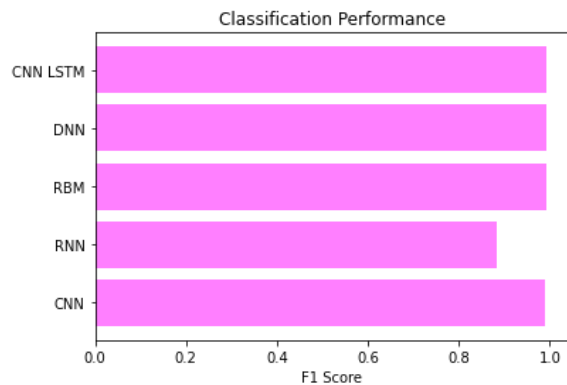


Fig 11 F1Score


Algorithms used	Accuracy	Precision	Recall	F1-score
CNN	0.989	0.994	0.989	0.991
RNN	0.793	1.000	0.793	0.885
RBM	0.991	0.993	0.991	0.992
DNN	0.994	0.994	0.994	0.994
Extension CNN+LSTM	1.000	0.993	0.990	0.992


Fig 12 Performance Evaluation





Fig 13 Home page


## NEW ACCOUNT?

 Username

 Name

 Mail

 Phone Number

 Password

REGISTER

Already have an account? [Sign in](#)

dst\_host\_count

dst\_host\_srv\_count

dst\_host\_same\_srv\_rate

dst\_host\_diff\_srv\_rate


dst\_host\_same\_src\_port\_rate

dst\_host\_srv\_diff\_host\_rate

Fig 14 Sign in page

## ADD ACCOUNT?

 admin

 .....

LOGIN

Register here! [Sign Up](#)

Fig 15 Login page

Predict

Fig 16 User input

Result: **There is No Attack Detected and Its Normal!**

Fig 17 Predict result for given input

## 5. CONCLUSION

Deep learning methods like Recurrent Neural Networks (RNN), Convolutional Neural Networks (CNN) [2], [11], [12], [13], [14], [15], [16], [17], and Deep Neural Networks (DNN) are exceptionally esteemed for early cyber-attack detection and malware identification. The examination shows how DL might further develop cybersecurity by proactively perceiving and decreasing dangers. The drawn out CNN + LSTM ensemble model accomplishes close to 100% accuracy, making it stick out. This unprecedented result shows the ensemble model's continuous strength and adaptability. The mix of CNN and LSTM networks accomplishes extraordinary cyber-attack detection accuracy, showing ensemble approaches' handiness. The Flask reconciliation makes sending simple and useful for online security. The Flask structure works on network safety framework arrangement and cooperation with its straightforward connection point. This ease of use works on the framework's convenience and guarantees its certifiable organization. The review recommends further learning coordination and the need for better Intrusion Detection Systems (IDS). Continuous location and order of unfriendly activities exhibit the task's ground breaking approach, laying the way for proceeding with cybersecurity advancement through clever innovation.

## 6. FUTURE SCOPE

High level DL and transfer learning techniques might be investigated from here on out. This could prompt further developed models, boosting the framework's confounded cyber threat detection. The recommended technique is adaptable and material since it very well might be utilized in many firms, including

multinationals. This could further develop cybersecurity for organizations, defending their valuable resources from cyberattacks. Edge computing will further develop ongoing danger discovery by handling and investigating information nearer to IoT gadgets [23]. This strategy limits inactivity, further develops responsiveness, and upgrades network assets, further developing constant digital danger recognition and alleviation. Future use of federated learning could change model training. Permitting cooperative training without revealing crude information safeguards information protection while helping worldwide model rightness and flexibility. This cooperative technique can upset IoT cybersecurity.

## REFERENCES

- [1] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.
- [2] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 2, pp. 84–90, Jun. 2017.
- [3] M. K. Islam, M. S. Ali, M. M. Ali, M. F. Haque, A. A. Das, M. M. Hossain, D. S. Duranta, and M. A. Rahman, "Melanoma skin lesions classification using deep convolutional neural network with transfer learning," in *Proc. 1st Int. Conf. Artif. Intell. Data Analytics (CAIDA)*, Apr. 2021.
- [4] A. Ahmim, M. Derdour, and M. A. Ferrag, "An intrusion detection system based on combining probability predictions of a tree of classifiers," *Int. J. Commun. Syst.*, vol. 31, no. 9, p. e3547, Jun. 2018.

- [5] A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, "A novel hierarchical intrusion detection system based on decision tree and rules-based models," in Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS), May 2019, pp. 228–233.
- [6] Z. Dewa and L. A. Maglaras, "Data mining and intrusion detection systems," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 1, pp. 1–10, 2016.
- [7] B. Stewart, L. Rosa, L. A. Maglaras, T. J. Cruz, M. A. Ferrag, P. Simoes, and H. Janicke, "A novel intrusion detection mechanism for SCADA systems which automatically adapts to network topology changes," *EAI Endorsed Trans. Ind. Netw. Intell. Syst.*, vol. 4, no. 10, p. e4, 2017.
- [8] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102419.
- [9] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, "A bidirectional LSTM deep learning approach for intrusion detection," *Expert Syst. Appl.*, vol. 185, Dec. 2021, Art. no. 115524.
- [10] A. A. Salih, S. Y. Ameen, S. R. Zeebaree, M. A. Sadeeq, S. F. Kak, N. Omar, I. M. Ibrahim, H. M. Yasin, Z. N. Rashid, and Z. S. Ageed, "Deep learning approaches for intrusion detection," *Asian J. Res. Comput. Sci.*, vol. 9, no. 4, pp. 50–64, 2021.
- [11] J. Azevedo and F. Portela, "Convolutional neural network—A practical case study," in Proc. Int. Conf. Inf. Technol. Appl. Singapore: Springer, 2022, pp. 307–318.
- [12] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2016, pp. 770–778.
- [13] J. Yosinski, J. Clune, Y. Bengio, and H. Lipson, "How transferable are features in deep neural networks?" in Proc. Adv. Neural Inf. Process. Syst., vol. 27, 2014, pp. 1–9.
- [14] G. Awad, C. G. Snoek, A. F. Smeaton, and G. Quénot, "Trecvid semantic indexing of video: A 6-year retrospective," *ITE Trans. Media Technol. Appl.*, vol. 4, no. 3, pp. 187–208, 2016.
- [15] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2016, pp. 2818–2826.
- [16] M. Uddin, R. Alsaqour, and M. Abdelhaq, "Intrusion detection system to detect DDoS attack in Gnutella hybrid P2P network," *Indian J. Sci. Technol.*, vol. 6, no. 2, pp. 71–83, 2013.
- [17] R. L. Haupt and S. E. Haupt, *Practical Genetic Algorithms*. Wiley, 2004, doi: 10.1002/0471671746.
- [18] D. Hossain, G. Capi, and J. M., "Optimizing deep learning parameters using genetic algorithm for object recognition and robot grasping," *J. Electron. Sci. Technol.*, vol. 16, no. 1, pp. 11–15, 2018.
- [19] O. E. David and I. Greental, "Genetic algorithms for evolving deep neural networks," in Proc.

Companion Publication Annu. Conf. Genetic Evol. Comput., Jul. 2014, pp. 1451–1452.

[20] J. Gu and S. Lu, “An effective intrusion detection approach using SVM with Naïve Bayes feature embedding,” *Comput. Secur.*, vol. 103, Apr. 2021, Art. no. 102158.

[21] E. Gyamfi and A. Jurcut, “Intrusion detection in Internet of Things systems: A review on design approaches leveraging multi-access edge computing, machine learning, and datasets,” *Sensors*, vol. 22, no. 10, p. 3744, May 2022.

[22] A. K. Balyan, S. Ahuja, U. K. Lilhore, S. K. Sharma, P. Manoharan, A. D. Algarni, H. Elmannai, and K. Raahemifar, “A hybrid intrusion detection model using EGA-PSO and improved random forest method,” *Sensors*, vol. 22, no. 16, p. 5986, Aug. 2022.

[23] X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu, and K. I.-K. Wang, “Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system,” *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9310–9319, Jun. 2021.

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

[25] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, “Machine learning and deep learning methods for cybersecurity,” *IEEE Access*, vol. 6, pp. 35365–35381, 2018.

[26] A. S. Dina and D. Manivannan, “Intrusion detection based on machine learning techniques in computer networks,” *Internet Things*, vol. 16, Dec. 2021, Art. no. 100462.

[27] H. Zhang, J. L. Li, and X. M. Liu, C Dong, “Multi-dimensional feature fusion and stacking ensemble mechanism for network intrusion detection,” *Future Gener. Comput. Syst.*, vol. 122, pp. 130–143, Sep. 2021.

[28] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, “Internet of Things: A survey on machine learning-based intrusion detection approaches,” *Comput. Netw.*, vol. 151, pp. 147–157, Mar. 2019.

[29] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, “Network intrusion detection for IoT security based on learning techniques,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2671–2701, Jan. 2019.

[30] J. Toldinas, A. Venčkauskas, R. Damaševičius, Š. Grigaliunas, N. Morkevičius, and E. Baranauskas, “A novel approach for network intrusion detection using multistage deep learning image recognition,” *Electronics*, vol. 10, no. 15, p. 1854, Aug. 2021.

[31] G. Andresini, A. Appice, and D. Malerba, “Autoencoder-based deep metric learning for network intrusion detection,” *Inf. Sci.*, vol. 569, pp. 706–727, Aug. 2021.

[32] K. Gupta, D. K. Sharma, K. Datta Gupta, and A. Kumar, “A tree classifier based network intrusion detection model for Internet of Medical Things,”



Comput. Electr. Eng., vol. 102, Sep. 2022, Art. no. 108158.

[33] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, “Deep learning approach for network intrusion detection in software defined networking,” in Proc. Int. Conf. Wireless Netw. Mobile Commun. (WINCOM), Oct. 2016, pp. 258–263.

[34] F. Jiang, Y. Fu, B. B. Gupta, Y. Liang, S. Rho, F. Lou, F. Meng, and Z. Tian, “Deep learning based multi-channel intelligent attack detection for data security,” IEEE Trans. Sustain. Comput., vol. 5, no. 2, pp. 204–212, Apr. 2018.

[35] M. A. Ferrag and L. Maglaras, “DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids,” IEEE Trans. Eng. Manage., vol. 67, no. 4, pp. 1285–1297, Nov. 2019.

[36] S. Basumallik, R. Ma, and S. Eftekharij, “Packet-data anomaly detection in PMU-based state estimator using convolutional neural network,” Int. J. Electr. Power Energy Syst., vol. 107, pp. 690–702, May 2019.

[37] M. Uddin, A. A. Rahman, A. Alarifi, M. Talha, A. Shah, M. Iftikhar, and A. Zomaya, “Improving performance of mobile ad hoc networks using efficient tactical on demand distance vector (TAODV) routing algorithm,” Int. J. Innov. Comput., Inf. Control, vol. 8, no. 6, pp. 4375–4389, 2012.

[38] A. A. Khan, A. A. Laghari, T. R. Gadekallu, Z. A. Shaikh, A. R. Javed, M. Rashid, V. V. Estrela, and A. Mikhaylov, “A drone-based data management and

optimization using Metaheuristic algorithms and blockchain smart contracts in a secure fog environment,” Comput. Electr. Eng., vol. 102, Sep. 2022, Art. no. 108234.

[39] F. Feng, X. Liu, B. Yong, R. Zhou, and Q. Zhou, “Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device,” Ad Hoc Netw., vol. 84, pp. 82–89, Mar. 2019.

[40] M. A. Salama, H. F. Eid, R. A. Ramadan, A. Darwish, and A. E. Hassanien, “Hybrid intelligent intrusion detection scheme,” in Soft Computing in Industrial Applications. Berlin, Germany: Springer, 2011, pp. 293–303.

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

[42] 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.

[43] 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.

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

[45] 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.

[46] G.Viswanath, “A Real Time online Food Ordering application based DJANGO Restfull Framework”, Juni Khyat, vol.13, 2023, pp.154-162.

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

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

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

[50] 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>