



A Smart Intrusion Detection Networked System Against Cyber Attacks Based on Intelligent Algorithms

Dalia Kefah Neamet¹ • Mahmood Zaki Abdullah^{*2}

¹Computer networks, College of Information Engineering,
Al-Nahrain University, Baghdad, Iraq.

²Computer Engineering Department,
Mustansiriyah University, Baghdad, Iraq.

Received: 20 02 2025; Accepted: 17 08 2025

Available: 31 08 2026

Abstract: The Internet of Things (IoT) faces growing security challenges, with escalating threats targeting devices, necessitating the development of efficient, secure intrusion detection systems (IDS). Deep learning (DL) and machine learning (ML) offer promising solutions to enhance detection accuracy and network security in IoT environments. In this paper, we propose a hybrid deep learning classification model (DNN-LSTM), applied to the Multi-Step Cyber-Attack Dataset (MSCAD), which consists of 66 features. We apply the DNN (deep neural network), LSTM (long short-term memory), and hybrid model (DNN-LSTM) to the dataset to evaluate their performance. The experimental findings showcase that our proposed model surpasses the accuracies achieved by DNN, LSTM models, and hybrid models, with scores of 99.72%, 99.76%, and 99.78%, respectively. It demonstrates their exceptional ability to produce the most accurate predictions. The results highlight the superiority of the DNN-LSTM hybrid model in identifying multi-step cyber-attacks, reducing false positives, and enhancing the overall efficiency of intrusion detection in IoT systems. Our work presents a promising approach to strengthening security in IoT networks

*Corresponding author.

E-mail address: drmzaali@uomustansiriyah.edu.iq (A.A.J. Al Noor).

Peer Review under the responsibility of Universidad Nacional Autónoma de México.

and contributes to the advancement of intrusion detection systems through the use of advanced deep learning techniques. These findings indicate that hybrid models like DNN-LSTM can play a critical role in addressing the evolving security challenges of IoT.

Keywords: Long short-term memory, deep neural network, multi-step cyber-attack, IDS.

1. Introduction

The Internet of Things (IoT) is a rapidly growing technology that enables physical devices and everyday objects to connect to the Internet, facilitating the transmission and reception of data (Rasheed et al, 2023). IoT devices encompass a wide range of items, including smartphones, smart homes, wearable, and even industrial machines (Khanna & Kaur, 2020). The ultimate goal of IoT is to enhance the efficiency, convenience, and precision of both personal and business operations. However, with the rapid expansion of IoT, the associated challenges have become increasingly prominent (Mohanta et al, 2020). One of the most critical challenges is the escalating security threats that target IoT devices. The proliferation of various types of attacks poses a significant risk to the integrity and privacy of IoT systems. Consequently, there is an urgent need to develop highly secure and efficient systems capable of safeguarding IoT environments from these threats (Abdullah & Al Ashoor, 2022). IoT systems have static defense mechanisms in the form of firewalls, anti-viruses software, or software patches, which have become a constraint for device manufacturers due to the heterogeneity of such devices (Kaur et al, 2023). Furthermore, the multi-functionality factor has also posed the challenge of developing and deploying a security mechanism capable of detecting attacks over a wide range of devices. This has resulted in the infeasibility of robust security measures (Yang et al, 2022). The widespread deployment of IoT applications means their security has become vital for secure communications (Aversano et al, 2021). Therefore, installing intrusion detection systems (IDSs) to identify malicious actors and maintain the availability and safety of IoT networks is crucial. An intrusion detection system monitors a network's health and activity. An alert is issued to the network administrator once an intrusion is discovered (Zhong et al, 2020). An IDS is crucial for protecting IoT networks Rule-based IDS methods have traditionally been used, but the complexity and

diversity of IoT networks have rendered them inefficient. Several modern techniques based on machine learning and specifically artificial intelligence (AI) have been developed. They can be used for the detection of threats, and uncovering network vulnerabilities. In addition, they can automate many tasks involved in cybersecurity such as intrusion detection and malware analysis (Admass et al, 2024). Deep learning is one approach that could be used to improve the efficiency and precision of IDS for IoT devices. To maximize the use of IDSs in the IoT using deep learning and machine learning and further identify the flaws and strengths of these systems (Choudhary et al, 2023).

In recent years, numerous researchers have been working on designing and implementing effective malware classification systems.

Venkatesan (2023), utilized the ability of an integrated autoencoder for features extraction, which made good classifiers. They used the maximum capabilities of Soft-Max to improve the classification procedure, they also produced a suitable accuracy in the dataset NS - KDD.

Aldhaheri, et al, (2024) improved an attacker detection system that using a hybrid deep learning method. They used a statistical method to search for network characteristics, tested a special encoder to realize a network threat, and further improved the accuracy. Their high-efficiency detection algorithm gives a good performance.

Mohammad and Alsmadi (2021) introduced a machine learning model using good feature selection method which is called Highest Wins, for establishing an accurate IDS. The Highest Wins method is tested on large-scale datasets and established methods like chi-square and information gain in terms of performance and feature reduction. It is also applied to the NS-KDD dataset with more convenient results and reduced the time of building the model.

Ferrag et al, (2020) introduced many methods based on using machine learning to carry out a reliable intrusion detection system. Most of the research works including SVM, random forests, and decision trees, to enhance the attack detection accuracy using selected features from the NSL-KDD dataset.

Abdullah et al, (2024) introduced machine learning algorithms like Adaptive Boosting-Deep Learning (Ada-Boost-Deep Learning) or (ABDL), Multi- Layer Perceptron (MLP), Bayesian Networks Model (BNM), and random forest (RF). It is also applied to the NS-KDD dataset with more convenient results and reduced the time of building the model. This paper's contributions introduced a novel architecture that combines a deep neural network (DNN) and LSTM networks and it used (DNN-LSTM) model to develop a hybrid model capable of detecting intrusions in IoT networks using the Multi-Step Cyber- Attack Dataset. The remainder of this paper is organized as follows: Section

2 provides a methodology. The results of the algorithm, tested against a commonly used reference, along with comparative analysis, are presented in Section 3. Finally, Section 4 presents the conclusions that can be drawn.

2. Methodology

The proposed method would include many procedural stages like data preparation, splitting dataset, building the model and performance evaluation, and setting up an overall strategy to heading the research problem, Figure 1 illustrates the procedural steps of the proposed research. while Figure 2 shows the architecture of hybrid DNN-LSTM model.

2.1 Preparation of dataset

Within the period of this work, the Multi-Step Cyber-Attack (MSCAD) Dataset was among the best and latest datasets in the field of IDS (Muna et al., 2018). The dataset

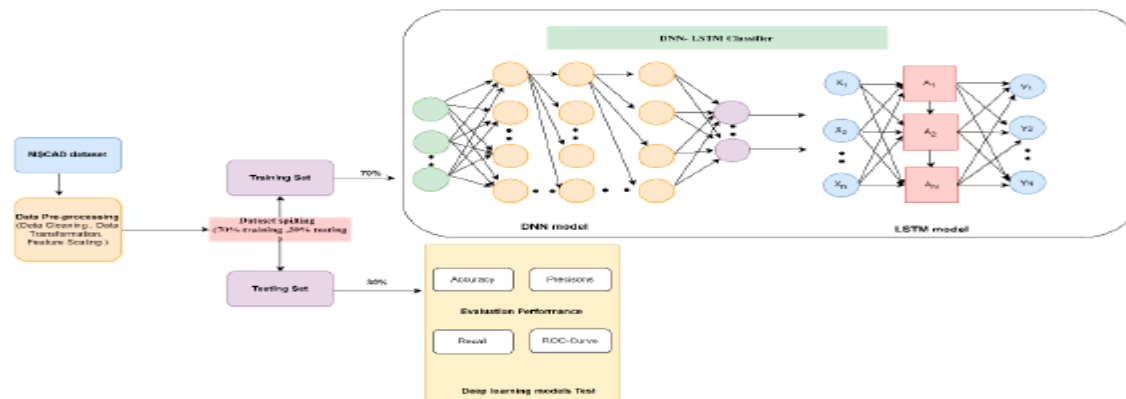


Figure 1. Proposed model.

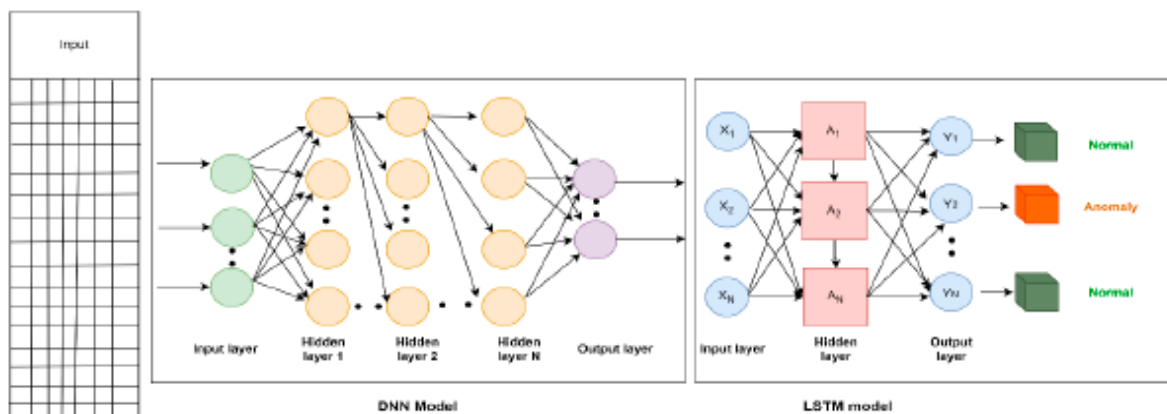


Figure 2. The architecture of hybrid DNN-LSTM model.

was preprocessed before feeding into the model. The accuracy of the model is potentially greatly improved with proper data preprocessing. In this step, the data was inspected for missing values and outliers, and further data was transformed into relevant features by employing feature scaling and categorical variables. At the end of this step, the dataset had 66 features.

2.2 Data splitting

In this step, the data is split. Data splitting involves dividing a dataset into subparts to facilitate the model's training, the prime objective of the data splitting is to assess the effectiveness of the model on unseen data. Here, the data is split into two sets 70% which includes the training set and 30 % which includes the test set. After the split, the training data consist of 60825 records and the testing data of 26069 records.

2.3 Build the model

In this step, we build and implement the model using DNN (deep neural network), LSTM (long short-term memory), and the hybrid (DNN-LSTM) model using the MSCAD dataset.

2.3.1 DNN model

As shown in Figure 3, the DNN part of our model consists of dense, activation, and hidden layers. Dense layers are commonly used to turn input training data into a high dimensional feature space, which helps in the effective learning of complex features (Sze et al, 2017). At first the DNN model, using the input layer and three hidden layers with 128, 64, and 32 neurons, respectively are used, each followed by a dropout layer to prevent overfitting.

2.3.2 LSTM model

It is a type of improved vision of RNN (recurrent neural network) which is designed to solve long dependency issues. LSTM's main learning mechanism is called 'gate' which allows the network to identify the part having less/more information. It acts accordingly to ignore and pay more attention to that specific part of sequential data in textual sequences. Thus, LSTM can learn and capture the dependency within sequence better and provide higher-performance sequential data (Khan et al, 2023), It has added and deleted the data, which has an incoming gate, outgoing gate, and hidden gate (Li et al, 2020). The incoming gate decides whether the new incoming data or information should be stored. The outgoing gate decides which data are used to evaluate the yield of LSTM. The

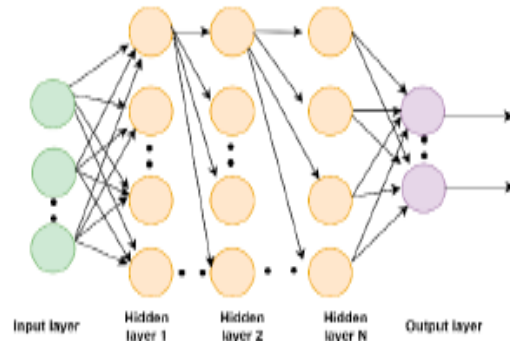


Figure 3. DNN structure.

hidden gate determines which data is irrelevant to forgotten and deleted data (Slevi & Visalakshi., 2021). The model has three LSTM layers, an input layer, a hidden layer and an output layer. We use the LSTM model with three layers employed, each with a different number of neurons 128, 64, and 32.

2.3.3 Hybrid DNN-LSTM model

It leverages the strength of both models to achieve enhanced performance of the model. The DNN part of the proposed model consists of dense, activation, and hidden layers. Dense layers are commonly used to turn input training data into a high-dimensional feature space. It helps in the effective learning of complex features. the LSTM takes the output of the DNN model as input to process sequential dependencies. The architecture has three dense layers, 128, 64, and 32 nodes, followed by three-layer LSTM neurons with 128, 64, and 32. Figure 3 shows the architecture of the hybrid DNN-LSTM deep learning model.

2.4 Evaluations of the proposed model

The model was evaluated using the predicated classes of the confusion matrix shown in Table 1. Equations 1 to 4 were applied to calculate all metrics (Khan et al, 2023).

Accuracy: it represents the proportions of the correct sample occurrence among all samples as shown in Equation (1).

$$ac = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Precision: It represents the correct computation of the proportion of estimated positive samples to all positive expected instances as shown in Equation (2).

$$Pr = \frac{TP}{TP+FP} \quad (2)$$

Sensitivity: also known as a recall, it calculates the capability of the method to differentiate all relevant instances from real positive samples, as shown in Equation (3).

$$Se = \frac{TP}{TP+FN} \quad (3)$$

F-measure: represents the integration of sensitivity and precision into one item as shown in Equation (4).

$$F - \text{measure} = \frac{2 \times \text{Se} \times \text{Pr}}{\text{Se} + \text{Pr}} \quad (4)$$

Table 1. Predicated classes.

Predicated class		
Actual class	TP	FN
	FP	TN

Where:

TP (True Positive): Represents the number of samples that are correctly estimated as positive.

FP (False Positive): Represents the no. of samples that are incorrectly estimated as positive.

FN (false negative): Represents the no. of samples that are incorrectly estimated as negative.

TN (Ture Negative): Represents the no. of samples that are correctly estimated as negative (Slevi & Visalakshi., 2021).

3. Performance Evaluations

For experiment purposes, we use the Keras deep learning library with TensorFlow. A model's evaluation provides crucial insight into its ability to generalize and make predicates based on previously unknown data. The effectiveness of the DNN-LSTM was evaluated on the MSCAD dataset. Accuracy, precision, recall, F1 score, and ROC curve have been used as evaluation measures to analyze the model's performance.

3.1 DNN model

During the experiments, the output of different models was recorded to make improvements. We trained the model for 100 epochs with a batch size 32, we achieved an accuracy of 99.72%. Figure 4 shows the confusion matrix using the DNN model, which is used to evaluate the performance of a classification model. It shows how well



Figure 4. Confusion matrix using DNN model.

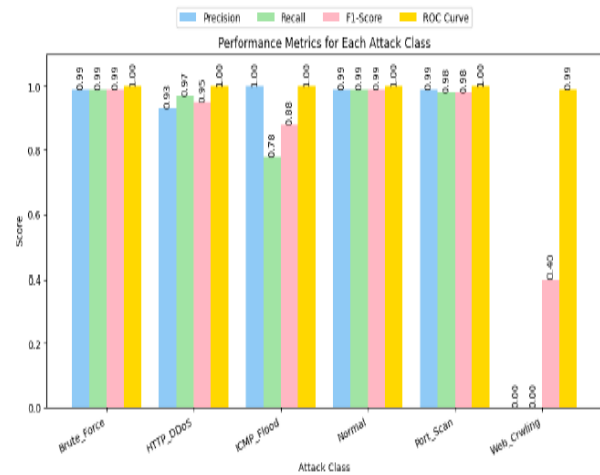


Figure 5. Performance metrics using DNN model.

the model predicted different attack classes compared to their actual labels.

The results shown in Figure 5 shows the model's classified performance for all classes, with near-perfect AUC scores (mostly 1.00), indicating high accuracy in distinguishing between them.

3.2 LSTM model

The LSTM model with three layers is achieved employed, and the model was trained for 100 epochs with batch size 32. The obtained results achieved an accuracy of 99.76%. The results in Figure 6 show the confusion matrix using the LSTM model, which is used to evaluate the performance of a classification model. Metrics include precision, recall, F1-score, and ROC curve,

3.3 DNN-LSTM model

The combined DNN model with the LSTM model is achieved. The architecture has three dense layers with



Figure 6. Confusion matrix using LSTM model.

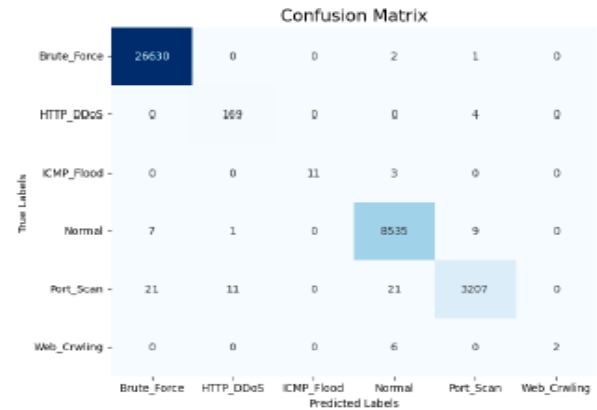


Figure 7. Confusion matrix of DNN-LSTM.

128, 64, and 32 nodes, followed by three-layer LSTM neurons with 128, 64, and 32. Then the model was trained for 100 epochs with a batch size 32. We achieved an accuracy of 99.78%. The results in Figure 7 show how well the model predicted different attack classes as compared to their actual labels.

The result in Figure 8 shows the performance metrics using the LSTM model for different attack classes as compared to their actual labels, while Figure 9 shows the performance Metrics using the DNN-LSTM model.

Table 2 shows the summary of DNN, LSTM, and hybrid DNN-LSTM models. It shows that the hybrid DNN-LSTM model achieves accuracy and good choice for identifying attacks.

Table 2. Comparison of performance evaluation of three models.

Model	Accuracy %	RMSE	Precision	Recall	F1-score
DNN	99.72	0.0224	0.82	0.79	0.80
LSTM	99.76	0.0129	0.99	0.83	0.87
DNN-LSTM	99.78	0.0125	0.99	0.38	0.87

Table 3. Summary of algorithm classification used in research studies. The proposed models compare with reference (Abdullah et al., 2024) that uses of ADBL (Adaptive Boosting-Deep learning) with the use of the MSCAD dataset. The proposed algorithm, when applied to the MSCAD dataset, demonstrates its impact as it produced high accuracy.

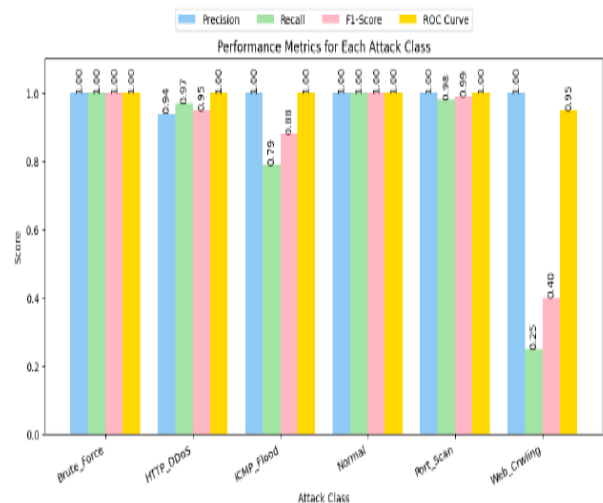


Figure 8. Performance metrics using the LSTM model.

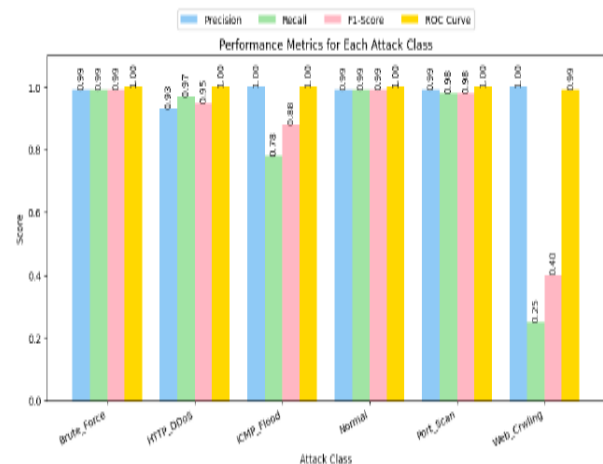


Figure 9. Performance Metrics using the DNN-LSTM.

Table 3. Summary of algorithm classification used in research studies.

Ref.	Algorithm of Classification	Dataset	Analyses Measurements
(Khan et al., 2019)	SoftMax	An UNSWNB15, And NSLKDD,	A good accuracy obtained in NSLKDD is 98.6%, and UNSWNB15, accuracy was 92.4%
(Zhong et al., 2020)	HELAD	MATlab	Better accuracy 95.6%
(Mohammad & Alsmadi, 2021)	Naive Bayes and decision tree	NS-KDD	99.56% with decision tree
(Choudhary et al., 2023)	SVM, random forests, and decision trees	NS-KDD	99% using decision tree
(Abdullah et al., 2024)	AB, MLP, BNM, and FR algorithms	MSCAD	99.7076% using ABDT with Rank ≥ 0.2
Proposed algorithms	DNN, LSTM and hybrid DNN-LSTM model	MSCAD	99.78%

Conclusions

Using the MSCAD dataset, we created the DNN, LSTM, and hybrid DNN-LSTM model for intrusion detection. We achieved promising outcomes with our hybrid model after thorough training and evaluation. The model displayed high accuracy when compared with the DNN and LSTM models. The models used appropriate evaluation metrics such as accuracy, precision, recall, F1-score, and ROC curve. The hybrid approach effectively combined the strengths of both DNN and LSTM, enabling it to capture both spatial and temporal patterns in network traffic data, thus providing an enhanced ability to detect intrusions. These promising results suggest that the hybrid DNN-LSTM model is a viable solution for intrusion detection systems, with significant potential for further improvements and real-world applications in cybersecurity. Future work could explore optimizing the model for larger datasets and integrating additional features to further enhance its detection capabilities.

Acknowledgements

The author would like to thank the reviewers and professors of Mustansiriyah and Al-Nahrain University for their valuable contribution to the publication of this research.

Funding

None of the authors received any sponsorship to produce the research reported in this article.

Conflict of Interest

For this article the authors do not have any type of conflict of interest to declare.

References

- Abdullah, M. Z., Jassim, A. K., Hummadi, F. N., & Al Khalidy, M. M. M. (2024). New strategies for improving network security against cyber attack based on intelligent algorithms. *Journal of Engineering and Sustainable Development*, 28(3), 342-354.
<https://doi.org/10.31272/jeasd.28.3.4>
- Abdullah, S. A., & Al Ashoor, A. A. (2022). Ipv6 security issues: A systematic review following prisma guidelines. *Baghdad Science Journal*, 19(6), 39.
<https://doi.org/10.21123/bsj.2022.7312>
- Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2, 100031.
<https://doi.org/10.1016/j.csa.2023.100031>
- Aldhaheeri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2024). Deep learning for cyber threat detection in IoT networks: A review. *Internet of Things and cyber-physical systems*, 4, 110-128.
<https://doi.org/10.1016/j.iotcps.2023.09.00>
- Aversano, L., Bernardi, M. L., Cimitile, M., & Pecori, R. (2021). A systematic review on Deep Learning approaches for IoT security. *Computer Science Review*, 40, 100389.
<https://doi.org/10.1016/j.cosrev.2021.100389>

- Choudhary, V., Tanwar, S., & Choudhury, T. (2023). A Hybrid Deep Learning Model for Intrusion Detection System in the Internet of Things Environment. In *2023 4th International Conference on Data Analytics for Business and Industry (ICDABI)* (pp. 682-689). IEEE.
<https://doi.org/10.1109/ICDABI60145.2023.10629562>
- Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, 102419.
<https://doi.org/10.1016/j.jisa.2019.102419>
- Kaur, B., Dadkhah, S., Shoeleh, F., Neto, E. C. P., Xiong, P., Iqbal, S., ... & Ghorbani, A. A. (2023). Internet of Things (IoT) security dataset evolution: Challenges and future directions. *Internet of Things*, 22, 100780.
<https://doi.org/10.1016/j.iot.2023.100780>
- Khan, F. A., Gumaei, A., Derhab, A., & Hussain, A. (2019). A novel two-stage deep learning model for efficient network intrusion detection. *Ieee Access*, 7, 30373-30385.
<https://doi.org/10.1109/ACCESS.2019.2899721>
- Khan, I. U., Ayub, M. Y., Abdollahi, A., & Dutta, A. (2023). A hybrid deep learning model-based intrusion detection system for emergency planning using IoT-network. In *2023 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)* (pp. 1-5). IEEE.
<https://doi.org/10.1109/ICT-DM58371.2023.10286954>
- Khanna A., and S. Kaur, (2020). "Internet of things (IoT), applications and challenges: A comprehensive review," *Wirel. Pers. Commun.*, vol. 114, no. 2, pp. 1687-1762.
<https://doi.org/10.1007/s11277-020-07446-4>
- Li, Y., Ghosh, S., Joshi, J., & Oviatt, S. (2020, November). Lstm-dnn based approach for pain intensity and protective behaviour prediction. In *2020 15th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2020)* (pp. 819-823). IEEE.
<https://doi.org/10.1109/FG47880.2020.00061>
- Mohammad, R. M. A., & Alsmadi, M. K. (2021). Intrusion detection using Highest Wins feature selection algorithm. *Neural Computing and Applications*, 33(16), 9805-9816.
<https://doi.org/10.1007/s00521-021-05745-w>
- Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of things*, 11, 100227.
<https://doi.org/10.1016/j.iot.2020.100227>
- Muna, A. H., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. *Journal of information security and applications*, 41, 1-11.
<https://doi.org/10.1016/j.jisa.2018.05.002>
- Rasheed, A. F., Zarkoosh, M., & Al-Azzawi, S. S. (2023). The impact of feature selection on malware classification using chi-square and machine learning. In *2023 9th International Conference on Computer and Communication Engineering (IC-CCE)* (pp. 211-216). IEEE.
<https://doi.org/10.1109/ICCCE58854.2023.10246084>
- Slevi, S. T., & Visalakshi, P. (2021). A survey on deep learning based intrusion detection systems on Internet of Things. In *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 1488-1496). IEEE.
<https://doi.org/10.1109/I-SMAC52330.2021.9641050>
- Sze, V., Chen, Y. H., Yang, T. J., & Emer, J. S. (2017). Efficient processing of deep neural networks: A tutorial and survey. *Proceedings of the IEEE*, 105(12), 2295-2329.
<https://doi.org/10.1109/JPROC.2017.2761740>
- Venkatesan, S. (2023). Design an intrusion detection system based on feature selection using ML algorithms. *Mathematical Statistician and Engineering Applications*, 72(1), 702-710.
<https://www.philstat.org/index.php/MSEA/article/view/2000>
- Yang, X., Shu, L., Liu, Y., Hancke, G. P., Ferrag, M. A., & Huang, K. (2022). Physical security and safety of IoT equipment: A survey of recent advances and opportunities. *IEEE Transactions on Industrial Informatics*, 18(7), 4319-4330.
<https://doi.org/10.1109/TII.2022.3141408>
- Zhong, Y., Chen, W., Wang, Z., Chen, Y., Wang, K., Li, Y., ... & Li, K. (2020). HELAD: A novel network anomaly detection model based on heterogeneous ensemble learning. *Computer Networks*, 169, 107049.
<https://doi.org/10.1016/j.comnet.2019.107049>