International Journal of Computer and Engineering Optimization (IJCEO)
Volume 3, Issue 1, January– February (2025)

RESEARCH ARTICLE

ADAPTIVE AUTOENCODER BASED DEEP LEARNING FRAMEWORK FOR INTRUSION DETECTION IN IOT

Mudassir Khan [1, *] and P. William [2]

[1] Department of Computer Science, College of Computer Science, Applied College Tanumah, King Khalid University, Abha, Saudi Arabia
[2] School of Engineering and Technology, Sanjivani University, Kopargaon, Maharashtra, India
[*]*Corresponding e-mail: mkmiyob@kku.edu.sa*

Abstract – Internet of Things (IoT) is a new paradigm that integrates physical items from a variety of domains, such as human health, industrial processes, environmental monitoring and home automation with the Internet. In addition to many advantages, It creates security issues and expands the number of gadgets we use on a daily basis. The proposed deep learning-based intrusion detection methods test against a range of threats to determine their efficacy and offer suggestions for how well they perform in IoT intrusion detection. However, it is difficult to apply traditional Intrusion Detection system techniques to the Internet of Things due to its unique characteristics, including devices, specific protocol stacks, standards and limited resources. A new variational Autoencoder based Deep learning framework for Intrusion Detection (AUTODEEP-ID) has been proposed to address this problem and detect attacks in an Internet of Things environment. The suggested approach makes use of a BIGRU to categorize data into attacks and a Variational Autoencoder to extract pertinent features. The efficiency of the suggested approach is evaluated by recall, precision and accuracy. The observational findings shows that the AUTODEEP-ID detects DDOS and U2R as 0.3% and 0.2 % respectively.

Keywords *– Internet of Things, Intrusion Detection System, deep learning, network security, DDoS attack, U2R attack.*

1. INTRODUCTION

The Internet-of-things (IoT) links various physical devices through the Internet and has a wide range of applications, including in the transportation, agriculture, military, and healthcare Increasing automation and providing timely insights and supporting informed decision-making through data analysis are core goals of IoT by making it possible for devices and systems to communicate with one another without requiring human intervention. However, the use of transmission and communication protocols in IoT devices raises serious security issues.

Understanding traffic patterns and spotting possible threats are essential for maintaining strong network security in the Internet of Things (IoT). Consequently, intrusion detection systems (IDSs) are now necessary to guarantee optimal network performance. These systems are made to identify and react to security risks that affect infrastructure, computer networks, systems, and other online spaces. Intrusion detection and prevention systems reduce risks and improve overall security by automatically recognizing and controlling threat events.

To identify trends in network traffic and identify possible threats, a variety of deep learning (DL) techniques are used. In this procedure, features are extracted from input datasets using a CNN-based method, and the most pertinent features are chosen using TSODE. However, there are issues with the system, such as a high rate of false positives and trouble adjusting to attacks that haven't been discovered yet.

In order to address this problem, AUTODEEP-ID, a system that makes use of the most recent developments in deep learning (DL). It applies a bidirectional gated recurrent unit (BIGRU) to identify and categorize possible attacks and uses a variational autoencoder to extract features from input datasets. The system is designed to detect intrusion attempts by analyzing incoming network data. The following are this work's main contributions:

- This study's primary goal is to create a practical strategy for guaranteeing network security in an Internet of Things (IoT).
- Provide a successful IDS plan that utilizes the advantages of deep learning to accurately classify and detect attacks in an IOT environment.
- A specially created variational autoencoder was used to extract pertinent features from the input data.
- The suggested BiGRU model is used to generate alerts and classify intrusions.

The rest of this paper is structured as follows: A thorough literature review is provided in Section II. The deep learning-based intrusion detection methodology is described

in Section III. The experimental findings and important observations are covered in Section IV. The study is finally concluded and future research directions are outlined in Section V.

2. LITERATURE REVIEW

In 2024 Afridi et al[14] suggested a novel distributed hybrid intrusion detection technique for the Internet of Vehicles (IoV) that is based on deep learning. To efficiently detect network intrusions, their model combines a convolutional neural network (CNN) with an enhanced long short-term memory (LSTM) network. According to experimental results, the algorithm has a strong detection performance, a 99.7% accuracy rate, and a rapid detection rate, reaching its target in as few as 20 iterations.

In 2023 Bhavsar et al [15] suggested an intrusion detection system (IDS) was proposed using the Pearson Correlation Coefficient–Convolutional Neural Network (PCC-CNN) deep learning model. The system performs binary classification to identify abnormal behaviour. With misclassification rates of 0.02, 0.02, and 0.01, the integrated model shows strong potential for accurate intrusion detection to detect anomalies in network traffic

In 2024 Hazman et al [16] suggested IDS-SIODL is a new intrusion detection system (IDS) for IoT-enabled smart cities that combines a long short-term memory (LSTM) model with feature engineering. With a recording accuracy of roughly 0.9990 and processing times of about 600 ms for training and 6 ms for classification, the system exhibits good performance. The model's efficacy in identifying intrusions is demonstrated by evaluation metrics like accuracy, recall, and precision.

In 2023 Chen et al[17] suggested a IG-Chi, a hybrid feature selection model, was created To improve classification accuracy and decrease feature dimensionality. To find the most pertinent features, this method combines information gain with the chi-square test. According to experimental results, the DF model uses less than 10% of CPU resources, while other models use more than 15%. Nevertheless, increased computational efficiency (CE) comes at the expense of decreased security performance robustness.

In 2023 Gaber et al [18], an Industrial Internet of Things (IIoT) framework was put forth suggested to do away with the need to link Industrial Automation and Control Systems (IACS) to traditional ICT platforms. The Random Forest (RF) and Binary Analysis (BA) classifiers performed better than other recent state-of-the-art machine learning and multi-objective algorithms, according to experimental results. However, the system's complexity makes real-time implementation difficult.

In 2023 Shahriar et al [19] suggested CAN Shield is a signal-level intrusion detection framework for the CAN bus that is based on deep learning. Compared to the traditional mean average method, the overall AUROC is 6.40% higher in this result. It does, however, demand more processing power.

In 2024, Almutairi et al [20] suggested an Intrusion Detection Method Based on Ensemble Deep Learning and Quantum Dwarf Mongoose Optimization in the CPS Environment. By using feature selection, the QDMO-EDLID technique detects the existence of intrusions. The results demonstrate improved performance with a 99.51% maximum accuracy.

3. PROPOSED METHODOLOGY

In this section a novel AUTODEEP-ID has been suggested for IOT attack detection. IOT devices are the source of the data in this case. Following collection, the data was preprocessed using methods like data cleansing and normalization. BI-GRU is used for classification, and variational auto encoders are used for feature extraction to extract pertinent data. in order to identify IOT attacks. This method is used in the Internet of Things (IoT) context to better balance exploration and exploitation, allowing for the selection of an ideal subset of features to increase the precision of intrusion detection predictions. Fig. 1 displays the workflow for the AUTODEEP-ID in network security

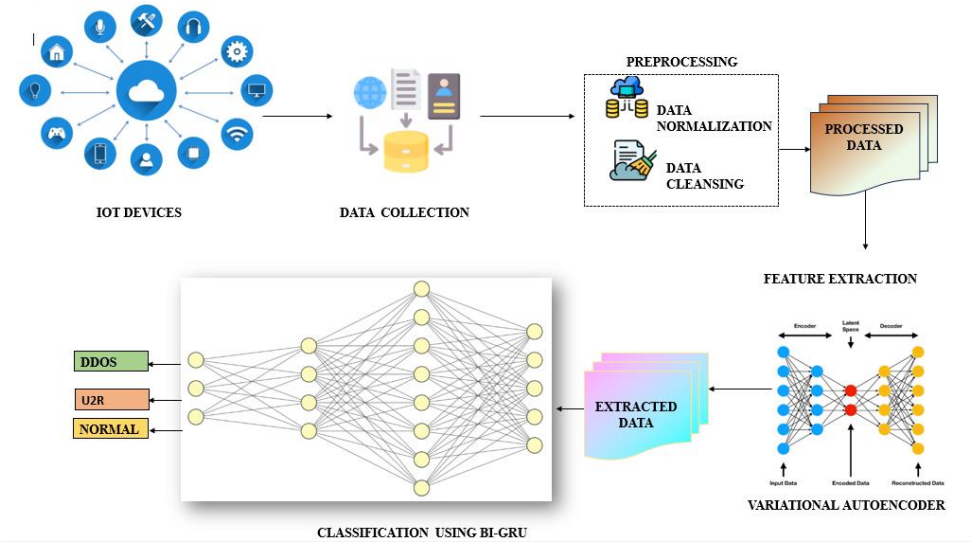

Figure 1. Framework of the AUTODEEP-ID in network security

3.1 Data Collection

IOT devices that have sensors installed are the source of data collection. The fundamental representation of IoT traffic data is used as input in this section.

3.2 Preprocessing

The raw data obtained from sensors is prepared for analysis during preprocessing. Data normalization and data cleansing are two preprocessing techniques**.**

3.2.1 Data cleansing

The process of starting with raw data from one or more sources and preserving its dependability is known as data cleansing

3.2.2 Data normalization

A crucial preprocessing step in getting data ready for artificial neural network training is data normalization. It shortens the total training time and aids in accelerating model convergence. Data can be standardized using a variety of methods, including min-max scaling, mean normalization, and standard scaling

$$X' = \frac{X-min(X)}{max(X)-min(X)} \quad (1)$$

3.3 Feature Extraction

As potent deep generative models that can capture complex, high-dimensional data in an unsupervised, low-dimensional latent space, variational autoencoders (VAEs) are used for feature extraction. Autoencoders (AEs), which are trained to reconstruct their input data, serve as the foundation for VAEs. Nevertheless, new samples cannot be produced by conventional autoencoders. In order to overcome this restriction, VAEs impose a variational constraint by requiring that the latent variable z have a normal distribution. In order to generate new data points and improve the model's generative capabilities, the decoder then takes samples from this distribution.

$$M(y,\widehat{y}) = \|x-\hat{x}\| \quad (2)$$

$$log\ p_\theta(y) = \sum_{j=1}^{m} log\ p_\theta(y^i) \quad (3)$$

$$log\ p_\theta(y^i) = DF(w(x|y^{(i)},\emptyset),Z(x|y^{(i)},\emptyset)) + M(\theta,\emptyset;y^i) \quad (4)$$

where the distance between two distributions is determined using the DF divergence function.

$$M(\theta,\emptyset;y^{(i)}) = - DF(w(x|y^{(n)},\emptyset),v(y,\theta)) + R_{w(n|m^{(i)},\emptyset}[log(x^{(n)}|z,\theta)] \quad (5)$$

The KL function's non-negativity allows equation (3) to be rewritten as:

$$\log p_\theta(y^i) \geq - DF(w(x|y^{(n)},\emptyset),v(y,\theta)) + R_{w(n|m^{(i)},\emptyset}[log(x^{(1)}|z,\theta)] \quad (6)$$

$$z = \mu + \sigma s \quad (7)$$

where the mean and latent variable are indicated by μ and σ.

$$M_{VAE} = \sum_{j=l}^{n}(\frac{1}{L}\sum_{m=1}^{m} logp(y^i w^{(m,n)},\theta) - DF(w(x|y^{(i)},\emptyset),N(0,1) \quad (8)$$

Equation (7) uses the jth jth sample $F(n)$ F(n), which is taken from a standard normal distribution and corresponds to the ith ith data instance, to compute $w(m,n)$ w (m,n). The datasets are then subjected to variational autoencoders in order to extract significant features

3.4 Classification

BiGRU, a simplified version of the long short-term memory (LSTM) network, is used for classification. With fewer training iterations, fewer parameters, and a more straightforward gating mechanism that lessens the chance of overfitting, GRU provides performance that is on par with or better than LSTM. This enables GRU to simplify the network architecture while preserving the efficacy of LSTM. These benefits have led to the widespread adoption of GRU. The update gate and the reset gate, which control the retention and deletion of data throughout the learning process, are its two primary components.

$$F_t = \sigma(T_F[R_n - 1, Y_n]) \quad (9)$$

$$S_t = \sigma(T_S[R_n - 1, Y_n]) \quad (10)$$

$$\widetilde{M_n} = \text{tanm}(T_m[S_t \odot M_n\text{-}1, Y_n]) \quad (11)$$

$$M_n = (1\text{-}F_t)\odot M_n\text{-}1 + F_t \odot \widetilde{M_n} \quad (12)$$

$$H_t = \vec{L} : \overleftarrow{L} \quad (13)$$

where \vec{L} represents the forward gated recurrent unit state and L represents the backward gated recurrent unit state. Lastly, the BIGRU model accurately and with a low error rate divides the data into DDOS, U2R, and normal.

4. RESULT AND DISCUSSION

A computer running an Intel CoreTM i5-8250U CPU at 1.8 GHz, 12 GB of RAM, and 64-bit Windows 10 Professional was used for the experiments. Python 3 was used to implement the suggested models

4.1 Dataset Description

The 1998 DARPA Intrusion Detection Evaluation Program, carried out by MIT Lincoln Laboratory, provided the dataset used in this investigation. Network traffic data from about 100 users on 1,000 UNIX-based systems was collected over a 10-week period. The KDDCup 1999 dataset was produced by processing this data after it was recorded using the tcpdump format. The KDDCup-99 dataset classifies attacks into five primary categories and comprises 41 features. These features fall into three categories: time-based traffic features calculated with a 2-second sliding window, content features that contain comprehensive TCP/IP payload information, and basic features taken from packet capture (Pcap) files

4.2 Performance Metrics

This section explains the measures that were used to evaluate the AUTODEEP-ID. The effectiveness of the

recommended strategy has been evaluated using the Recall, F1-Score, Accuracy and Precision measures.

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

$$PR = \frac{TP}{TP+FP}$$

$$F1-score = \frac{2*(PR*Recall)}{(PR+Recall)}$$

$$Recall = TP/(TP+FN)$$

4.3 Performance Analysis

According to the experimental results, the proposed technique has been compared with current techniques for detecting attacks.

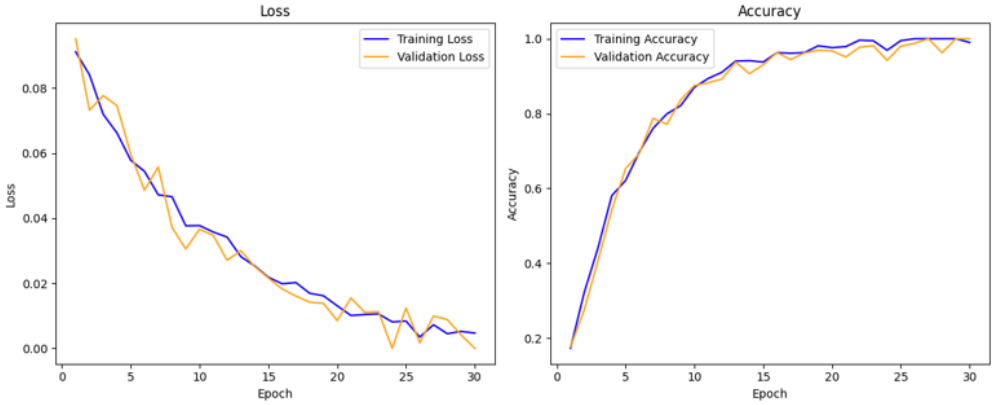

Figure 2. Accuracy vs Loss

The accuracy and loss values of the KDDCup99 dataset at various iteration stages are shown in Figure 2. The graph illustrates how accuracy and loss change with the number of training iterations for the BiGRU-based intrusion detection model

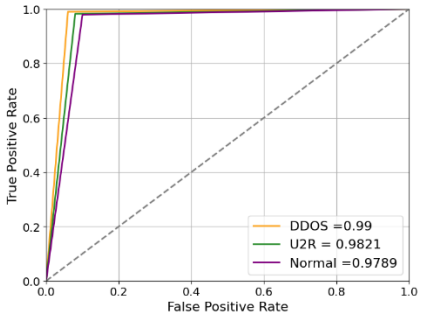

Figure 3. Roc Analysis dataset

The ROC of intrusion detection outcomes using the BIGRU is shown in Figure 3. In comparison to the dataset, parameters produced a comparatively high AUC of 0.99 for DDOS 0.9821 for U2R and 0.9789 for normal.

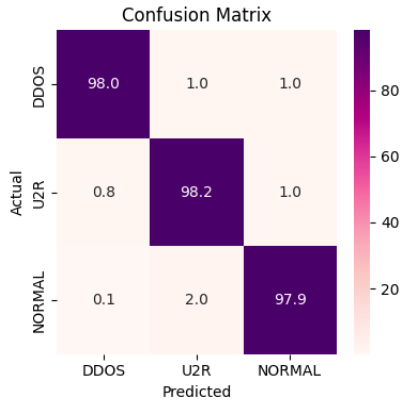

Figure 4. Confusion Matrix

For classification tasks, Figure 4 shows confusion matrices with performance predicted labels on DDOS, UR2, and Normal 98.45% of labels are identified, with 1.08% being classified as normal and 1.20% as somewhat elevated. The classifier performs well across all datasets, especially when it comes to detection

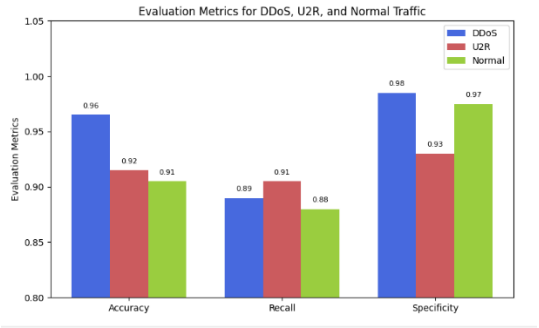

Figure 5. Performance analysis

The performance study of categorization classes using the KDDcup99 dataset is shown in Figure 5. the recommended method accuracy, recall, and specificity are 98.01, 98.21, 97.89 respectively.

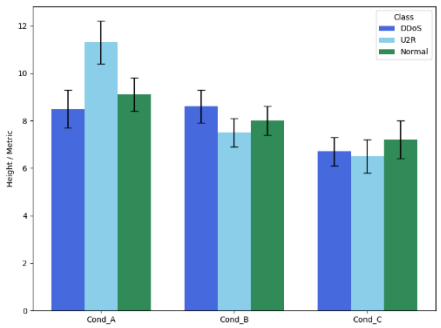

Figure 6. Error score

Figure 6 shows how the model can identify and categorize DDoS, U2R, and normal network traffic types under varied circumstances. Each bar's height represents the average detection performance, and error bars show variations between test runs or conditions

5. CONCLUSION

This study suggests a AUTODEEP-ID methodology to classify and detect attacks in IOT environment. To effectively capture features and raise the accuracy of the classification model, the variational autoencoder is used for feature extraction. The network is able to categorize attacks into DDOS and U2R Normal by feeding these extracted features into the BIGRU model. f1 score, recall, precision, and accuracy are used to assess the suggested approach. The suggested attack classes for the dataset are DDOS, U2R, and Normal, which are 98.01, 98.21, and 97.89, respectively. Our suggested methodology has a higher accuracy rate. The system can be enhanced by combining it with artificial intelligence to produce an intelligent system that can identify attacks by analyzing data patterns from system device readings.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors

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] 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 of Things Journal, vol. 9, no. 12, pp. 9310–9319, 2021[CrossRef] [Google Scholar] [Publisher Link]

[2] D. Javeed, T. Gao, M. S. Saeed, and P. Kumar, "An intrusion detection system for edge-envisioned smart agriculture in extreme environment," IEEE Internet of Things Journal, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] S. Li, G. Chai, Y. Wang, G. Zhou, Z. Li, D. Yu, and R. Gao, "CRSF: An intrusion detection framework for industrial internet of things based on pretrained CNN2D-RNN and SVM," IEEE Access, vol. 11, pp. 92041–92054, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T. H. Kim, "Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey," IEEE Access, vol. 10, pp. 121173–121192, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] A. Raghuvanshi, U. K. Singh, G. S. Sajja, H. Pallathadka, E. Asenso, M. Kamal, A. Singh, and K. Phasinam, "Intrusion detection using machine learning for risk mitigation in IoT-enabled smart irrigation in smart farming," Journal of Food Quality, vol. 2022, no. 1, p. 3955514, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] 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]

[8] M. Esmaeili, S. H. Goki, B. H. K. Masjidi, M. Sameh, H. Gharagozlou, and A. S. Mohammed, "ML-DDoSnet: IoT intrusion detection based on denial-of-service attacks using machine learning methods and NSL-KDD," Wireless Communications and Mobile Computing, vol. 2022, no. 1, p. 8481452, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] T. Gaber, J. B. Awotunde, S. O. Folorunso, S. A. Ajagbe, and E. Eldesouky, "Industrial internet of things intrusion detection method using machine learning and optimization techniques," Wireless Communications and Mobile Computing, vol. 2023, no. 1, p. 3939895, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] H. Liao, M. Z. Murah, M. K. Hasan, A. H. M. Aman, J. Fang, X. Hu, and A. U. R. Khan, "A survey of deep learning technologies for intrusion detection in Internet of Things," IEEE Access, vol. 12, pp. 4745–4761, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] S. Tharewal, M. W. Ashfaque, S. S. Banu, P. Uma, S. M. Hassen, and M. Shabaz, "Intrusion detection system for industrial Internet of Things based on deep reinforcement learning," Wireless Communications and Mobile Computing, vol. 2022, no. 1, p. 9023719, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] J. B. Awotunde, C. Chakraborty, and A. E. Adeniyi, "Intrusion detection in industrial internet of things network based on deep learning model with rule-based feature selection," Wireless Communications and Mobile Computing, vol. 2021, no. 1, p. 7154587, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] J. Li, M. S. Othman, H. Chen, and L. M. Yusuf, "Optimizing IoT intrusion detection system: Feature selection versus feature extraction in machine learning," Journal of Big Data, vol. 11, no. 1, p. 36, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Z. Abou El Houda, B. Brik, and L. Khoukhi, "Why should I trust your IDS?: An explainable deep learning framework for intrusion detection systems in Internet of Things networks," IEEE Open Journal of the Communications Society, vol. 3, pp. 1164–1176, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] A. Alferaidi, K. Yadav, Y. Alharbi, N. Razmjooy, W. Viriyasitavat, K. Gulati, S. Kautish, and G. Dhiman, "Distributed deep CNN-LSTM model for intrusion detection method in IoT-based vehicles," Mathematical Problems in Engineering, vol. 2022, no. 1, p. 3424819, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] M. Bhavsar, K. Roy, J. Kelly, and O. Olusola, "Anomaly-based intrusion detection system for IoT application," Discover Internet of Things, vol. 3, no. 1, p. 5, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "Enhanced IDS with deep learning for IoT-based smart cities security," Tsinghua Science and Technology, vol. 29, no. 4, pp. 929–947, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] X. Chen, P. Wang, Y. Yang, and M. Liu, "Resource-constraint deep forest based intrusion detection method in Internet of Things for consumer electronics," IEEE Transactions on Consumer Electronics, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] T. Gaber, J. B. Awotunde, S. O. Folorunso, S. A. Ajagbe, and E. Eldesouky, "Industrial internet of things intrusion detection method using machine learning and optimization techniques," Wireless Communications and Mobile Computing, vol. 2023, no. 1, p. 3939895, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] M. H. Shahriar, Y. Xiao, P. Moriano, W. Lou, and Y. T. Hou, "CANShield: Deep-learning-based intrusion detection framework for controller area networks at the signal level," IEEE Internet of Things Journal, vol. 10, no. 24, pp. 22111–22127, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] L. Almutairi, R. Daniel, S. Khasimbee, E. L. Lydia, S. Acharya, and H. I. Kim, "Quantum dwarf mongoose optimization with ensemble deep learning based intrusion detection in cyber-physical systems," IEEE Access, vol. 11, pp. 66828–66837, 2023. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

Mudassir Khan is an accomplished academic, researcher, author, and consultant with expertise in computer science and data analytics. He holds an MCA and a Ph.D. in Big Data Analytics using Deep Learning. Currently, he is pursuing a postdoctoral fellowship at Multimedia University, Malaysia, and is a Co-Supervisor for Postgraduate Studies at Lincoln University College, Malaysia. With over 14 years of teaching and research experience, Dr. Khan has contributed significantly to the field as an Assistant Professor at King Khalid University. His expertise includes Big Data, Deep Learning, Machine Learning, Data Science, IoT, and AI, with a focus on medical imaging in healthcare. Dr. Khan has published over 95+ research articles in prestigious journals and presented his work at international conferences.

P. William is working as Director (Research) at Sanjivani University , Kopargaon. He is the Post Doctoral Fellow from Amity University Dubai, UAE and Adjunct faculty of Victorian Institute of Technology, Australia. He is recognized in World Top 2% Scientist list by Stanford University and Elsevier. He is a member of IEEE, QCFI, ISTE and various other professional bodies. His research includes innovation and development of cutting edge solutions in the fields of natural language processing, artificial intelligence, deep learning, machine learning, soft computing, cybersecurity, and cloud computing. He has published 225+ papers in Scopus indexed journals and Conferences. He has 30+ patents published with grants in his credit. He has authored and edited 20+ books with renowned publishers of global recognition. He has been associated with numerous Multi-National Companies and various Educational Groups for his expertise in research, corporate training and consulting where he has contributed to the advancement of knowledge and practice in his domain. A focused professional with experience of consulting in Research, Innovation and Development. He served as a Chairperson and Auditor in multiple committees of national recognition. Delivered Keynote speeches and chaired many sessions in International Conferences. He was appointed as Series Editor, Guest Editor and Reviewer in Scopus/ Web of Science indexed journals.

Arrived: 16.01.2025
Accepted: 21.02.2025