International Journal of Computer and Engineering Optimization (IJCEO)
Volume 02, Issue 04, July – August (2024)

RESEARCH ARTICLE

CODE-IDS: CONVOLUTIONAL NEURAL NETWORK BASED INTRUSION DETECTION SYSTEM USING DEEP LEARNING

Ramakrishna Hegde [1, *] and S M Soumyasri [2]

[1] Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, India.
[2] Associate Professor, Department of Computer Appliications, Vidya Vikas Institute of Engineering and Technology, Mysore.
[*]*Corresponding e-mail: ramhegde111@gmail.com*

Abstract – The Internet of things is a network of interconnected devices that exchange data and communicate with the cloud and other IoT devices. IoT devices, which may include consumer electronics as well as mechanical and digital equipment, are typically equipped with sensors and software. But conventional IDS frameworks frequently have trouble correctly distinguishing intricate attack patterns from typical activity, which leads to a high false-positive rate and little flexibility to changing threats. This paper proposes a novel CODE-IDS framework using deep learning Network to improve network security by precise cyber threat identification and mitigation. While allowing secure access to attacker, the system records the actions of possible attackers. The technique successfully differentiates between typical, DDoS, MiTM, and probe attack traffic by using Deep learning. PCA is used for feature extraction and the Adaptive Weighted Particle Swarm Optimization is applied to retain the most important classification for feature selection. The parameters, enhancing its accuracy and performance the overall accuracy of the suggested model is 98.78% and methods achieving a low accuracy of 93.85% 96.8% and 96.8% respectively.

Keywords *– Intrusion Detection, Adaptive Weighted Particle Swarm Optimization, Deep Learning, Convolutional Neural Network, Principal component analysis.*

1. INTRODUCTION

IOT devices has developed into a game-changing concept that is transforming our interactions with technology and our environment. It represents a vast network of interrelated systems, sensors devices that able to collect, exchange, process data instantly. If an IoT system complies with all applicable security standards, it is theoretically completely safe; but, in reality, this is not always the case [1]. An increasing number of devices are being connected every day as Internet of Things grows quickly. Devices with limited resources and diversified and wide networking make them susceptible to a range of cyberattacks [2]. Various techniques have been used to identify security breaches; however, they are frequently computationally efficient and inappropriate for situations when resources are limited. The development of effective security measures against a variety of assaults is therefore necessary. The development of efficient attack detection techniques has been made possible by recent developments in deep learning (DL) models [3].

IoT expands the Internet's capabilities beyond computers to encompass a wide range of settings and procedures. End users connect everything that can be seen to the network in order to collect data, transmit it back, or do both. [4]. IoT devices have limited computational and storage capability, sophisticated security measures requiring a lot of memory or data are inapplicable. IoT devices are more susceptible as a result of the weak or nonexistent security software [5]. It is crucial to swiftly implement intelligent solutions in IoT-based applications in order to defend against complex cyberattacks. As a result, the SDN-like framework must be recognized for a number of attack issues [6].

IoT systems frequently have less processing power. In order to solve this, developing a lightweight attack detection model in a resource-constrained context requires lowering the number of characteristics. Additionally, efficiently identifying irregularities from the enormous volumes of high-dimensional data in IoT is still a difficult undertaking [7]. The cloud computing environment, which has more sophisticated CPUs and sufficient memory resources, is where the data gathered from the Internet of Things system is kept [8]. Because IoT devices are utilized in smart city applications, cyberattacks have the ability to modify devices to an insecure setting or obtain information about citizens' daily activities without the user or administrator's knowledge [9]. The goal is to shift the DL implementation from edge layer sensors to the closest location of data sources, where data analysis will be completed quickly. Traditional cloud-based services are extended by fog computing to the network edge, where data is generated [10].

1.1. Objective

The main objective of this study to detect possible security breaches and unauthorized access attempts with high accuracy and minimize false positives, to improve and

develop methods or algorithms that efficiently identify and analyze malicious activity within a network by looking at network traffic patterns. The objective of this study:

- To develop a hybrid optimization model to identify IoT network intrusions and extract optimal features from traffic data, which should lower the deep learning model's computational cost.
- To develop deep learning algorithm that minimizes data loss and monitors and detects assaults with high accuracy.
- To develop model for cyber-attack that looks for recognized attacks as well as suspicious or malevolent activity in order to spot threats early on and take action before they cause harm.
- To develop an IDS that can effectively grow with the number of IoT devices, preserving functionality while guaranteeing minimal resource usage.
- To create a collaborative intrusion detection system that effectively tracks and identifies cyberattacks on dispersed Internet of Things devices.

1.2. Contribution

Following are the main contributions the research work presented in this study:

- For the purpose of safe, and secure method has been suggested to improve network performance.
- created an advanced intrusion detection system that accurately detects cyberthreats by utilizing deep learning, particularly the LSTM network.
- Proposed adaptive deep learning model is appropriate for real-world applications since it can react to changing cyberthreats.
- Optimized IDS framework for resource-constrained IoT environments such as smart homes, healthcare, and industrial IoT.
- Enhancing security through effective classification using deep learning and fuzzy rules.

The remainder of this study is organized as follows: Section 2 precise with the related works. The developed methodology is included in section 3. Section 4 includes the experimental results and discussion. Section 5 includes the conclusion and future work.

2. LITERATURE REVIEW

In 2024, Jhansi Bharathi Madavarapu, [11] suggested framework can identify a variety of cyberattacks with a 99.97% detection rate, 99.96% detection accuracy in binary classification, 99.65% detection accuracy in classification. It is also efficient as to response time and detection accuracy. Because of its dispersed nature, high computing capability, close proximity to edge devices, the suggested method deploys an attack detector on fog nodes. To determine which of the six DL models performs the best, they are compared. Five distinct datasets with a range of assaults are used to assess each DL model. According to experiments, the long short-term memory model works better than the other five DL models.

In 2024, Vishnu Karthik Ravindran, [12] suggested IoT-IDCS-CNN utilizes parallel processing with fast I9-core-based Intel CPUs and high-performance computing with the reliable CUDA based Nvidia GPUs (Graphical Processing Units). Specifically, the suggested system is made up of three subsystems: one for traffic classification, one for feature engineering, and one for feature learning. In this study, every subsystem was created, checked, combined, and validated. The solution was evaluated using the NSL-KDD dataset, which covers all of the major IoT computing attacks.

In 2024, T. Maris Murugan and A Jeyam [13] developed IoT systems are becoming more vulnerable to cyberattacks due to advancements in the IoT environment, which may result in malevolent incursions. These incursions may result in both financial and physical harm. The IoT system/framework, the IoT, learning-based approaches, and the challenges faced by IoT devices or systems following an attack are the main topics of this article. A variety of cyberattacks, including DDoS, probing, U2, R2L, botnet assault, spoofing, MITM attacks, are used to evaluate learning-based techniques.

In 2024, K. Paul Joshua and A. Jenice Prabhu, [14] structure that uses Transfer Learning (TL) to get beyond these obstacles. In particular, a new collaborative learning methodology that allows a source network with a large amount of labeled data to efficiently and rapidly teach "knowledge" to a target network with unlabeled data. The productivity, adaptability, and scalability of intrusion detection systems are limited by requirement that the networks' data sets used in state-of-the-art research have the same characteristics.

In 2024, M. Devaki, Jeyaraman Sathiamoorthy and M. Usha, [15] suggests enhancing network intrusion detection systems with a deep hybrid learning model. In order to achieve this, the data set is first preprocessed and standardized. Then, to successfully identify anomalies in traffic data from industrial internet of things (IoT) devices, deep hybrid learning models that ALSTM and FCN with Gradient XGBoost and AdaBoost are built.

In 2024, Bakhsh, S.A. et al., [16] suggested better performance utilizing the CIC-IoT22 dataset in comparison to the state-of-the-art DL-IDS. Furthermore, by producing quick fixes for security issues in IoT networks, the models may improve intrusion detection in these networks. Furthermore, by producing quick fixes for security issues in IoT networks, the models may improve intrusion detection in these networks.

In 2024, Souri, A. et al., [17] suggested model is compared to a number of alternative baseline DL models. The model's performance was evaluated using three important datasets UNSW-NB15, and CICIoT 2023 that included a variety of attack scenarios. With less resource usage, the suggested model outperforms the current model in terms of accuracy and detection time and use a correlation coefficient as a fitness function in Genetic Algorithms (GA) to pick features. Furthermore, feature ranking uses mutual

information (MI) to gauge how dependent each feature is on the target variable.

3. PROPOSED METHODOLOGY

In this research the proposed DL model design for cybersecurity in smart healthcare, smart home, smart city environment. This study begins with pre-processing standaization and data cleaning to remove the noise from the data. PCA is use for feature extraction to identify the revelent features. Then the feature selection is applied by using Adaptive Weighted Particle Swarm Optimization. To classify detection of cyberattack as Normal, DDoS, MiTM, Probe, ConvBi-LSTM Network is used. The model framework obtains various smart system the role of the attacker attempts to take advantage of fault, highlighting how important need cybersecurity measures. Figure1 represent the suggested CODE-IDS method to improve threat detection and reduce cyber risks.

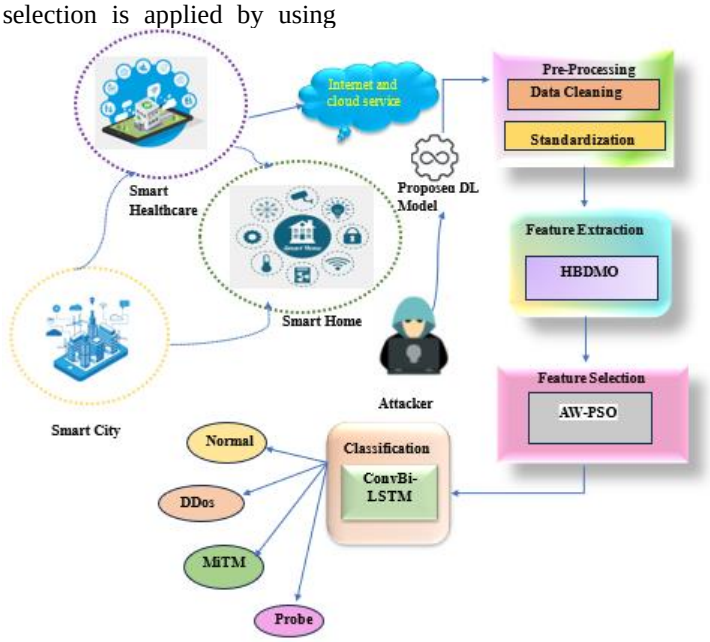

Figure 1. Proposed framework of cyber-attack detection model

3.1. Data pre-processing

The framework's initial phase is shown in this section, the DL models, the data is pre-processed. In addition to preventing overfitting issues, proper pre-processing of network traffic enables DL models. The two phases of pre-processing are data processing and feature selection. Due to the enormous volume of the dataset, three distinct datasets that can accurately represent the whole dataset for training and testing procedures were created by randomly selecting data from both regular traffic and all attack kinds. In order to remove imbalances from the data set, log standaization procedures were used.

3.2. PCA based on feature extraction

Principal component analysis represents vector as the sum of its basis vectors, PCA recognition from a mathematical perspective involves three fundamental processes. The covariance matrix is first created using training data. Next, associated eigenvalues and eigenvectors are computed. Third, by projecting the test data into the subset domain and contrasting them with the data from the training subspace domain, the test data are detected. The following steps compose the PCA algorithm:

Let F (x, y) be a m x n two-dimensional array of intensity values in the input data. The training set's average image is ascertained via,

$$\bar{x} = \frac{1}{L}\sum_{i=1}^{L} x_i \quad (1)$$

The dispersion of each feature vector with regard to the mean vector may be represented by computing the covariance matrix. As defined by, the covariance matrix C

$$C_{xx} = \frac{1}{L}\sum_{i=1}^{L}(x_i - \bar{x})(x_i - \bar{x})^T \quad (2)$$

It is possible to calculate the eigenvectors and associated eigenvalues using,

$$CV = \lambda V \quad (3)$$

where V denotes the collection of eigenvectors connected to eigenvalue. Using eigenspace, this displayed image and the training data will be compared. Similarity metrics will be used to compare the data. For recognition, the training data with the greatest similarity to the test data will be utilized.

3.3. Adaptive Whale -Particle Swarm Optimization based on feature selection

Adaptive Whale-Particle Swarm Optimization, a novel hybrid algorithm, is developed for feature selection. It integrates strategies from whale optimization and adaptive swarm optimization. A randomly selected solution is the first step in the AW-PSO algorithm. On the other hand, search agents react differently to different actions. Equation (4) and (5) describes the objective function F_{obj}, which is employed in each iteration.

$$H_{obj} = E * (1 + \beta)/XF \quad (4)$$

$$XF = m/s \quad (5)$$

Where m is the number of elements sampled, S is the lack of a population, E is the population error, and b is a constant with a value of 0.5. The hunter assists in the hunting process, the task of finding the prey and surrounding it as effectively as possible falls to the hunter.

Algorithm 1: AW-PSO

Begin with initializing the population of humpback whales as $Y_i = (1, 2, \ldots, n)$, where initially $i = 1$.

For each Y_i, determine the fitness function F_{obj}.

While (i < maximum number of iterations)

For each search agent

Update b, P, L, and m

Modify the position of the current search agent

else if $(|P| > 1)$

Select Y_{rand}, the agent for random searches.

The current search agent's position can be modified

The global best position can be found by searching for the lowest individual best position.

end if

else if $(m > 0.5)$

Upgrade the position of the current search agent

Replace the global best position with the new position

end if

end for

Update $Y^*(i)$ if a better solution is found.

$i = i + 1$

End while

3.4. ConvBi-LSTM Network based on classification

Convolutional features are present both input-to-state and state-to-state transitions of ConvLSTM, a form of recurrent neural network for spatiotemporal prediction. Based on inputs and previous states, the ConvLSTM predicts the future state of a specific grid cell. Using a convolution operator in input-to-state and state-to-state transitions makes this simple. The convolution operator and Hadamard product are shown by the following key equations for ConvLSTM:

$$x_t = \sigma(Y_{xi} * X_t + Y_{si} * H_{t-1} + Y_{ci} \odot C_{t-1} + b_i \quad (6)$$

$$r_t = \sigma(Y_{xr} * X_t + Y_{sr} * H_{t-1} + Y_{cr} \odot C_{t-1} + b_r \quad (7)$$

$$c_t = r_t \odot C_{t-1} + x_t \odot tanh(Y_{xc} * X_t + Y_{sc} * H_{t-1} + b_c \quad (8)$$

$$o_t = \sigma(Y_{xo} * X_t + Y_{so} * H_{t-1} + Y_{co} \odot C_t + b_o \quad (9)$$

$$H_t = o_t \odot tanhn(C_t) \quad (10)$$

A ConvLSTM with larger transitional kernel must be able to catch rapid movement, while one with a smaller kernel should be able to capture slower motions, if we consider to be the hidden representations of moving objects.

4. RESULTS AND DISCUSSIONS

4.1. Dataset Description

The performance of suggested model was evaluated using well-known datasets: UNSW-NB-15. The research community is aware that these databases contain a wide range of network threats. In our tests, we examined the complete datasets without separating out certain attack types to assess the efficacy of suggested model in identifying a wide variety of cyberattacks.

4.2. Performance Evaluation

Accuracy, recall, F1-score, precision, and Matthews Correlation Coefficient are among the metrics used to assess the detection model's performance. Higher accuracy values signify greater performance on a given job, which is how these models are measured. False Positive, True Negative, True Positive, and False Negative all contribute to the confusion matrix. Figure 3 represent the performance evaluation of classification model quality. TP, TN, FP, and FN are all taken into account to create a balanced categorization performance measure. Performance Evaluation of proposed model is shown in Figure 3

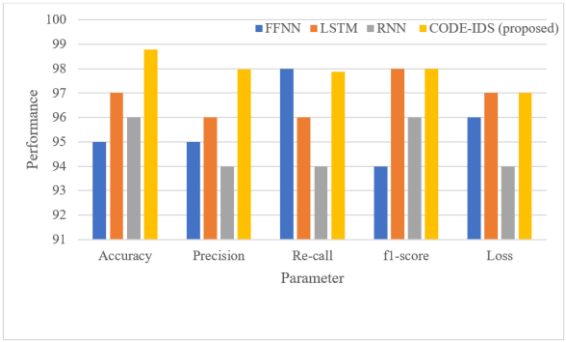

Figure 2. Performance Evaluation of proposed model

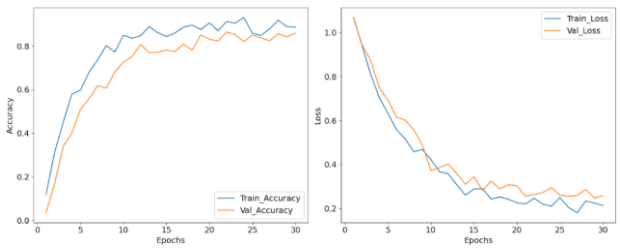

Figure 3. Accuracy and loss curve of the Proposed Method

The suggested CODE-IDS framework has attained an overall accuracy of 99.01% DS method. The classification of the validation and testing is illustrated through accuracy and loss plots of the proposed intrusion detection methods shown in Figures 3(a) and 3(b) These plots illustrate the model's performance highlighting its effectiveness in detecting intrusions. The low loss values also reflect successful learning with minimal overfitting during the training process.

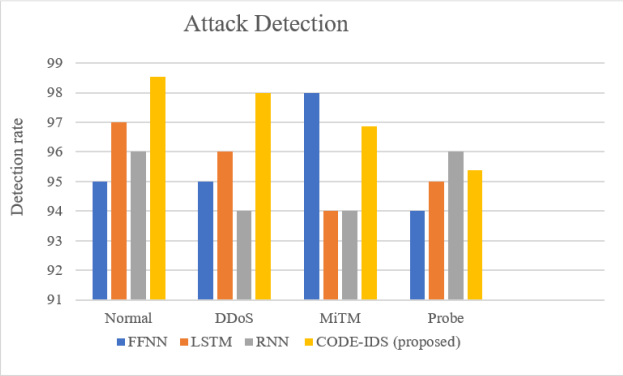

Figure 4. Attack Detection rate for Proposed model

Performance evaluation in terms of detection rate of suggested system with numerous methods. Figure 4 illustrates Attack Detection Rate (ADR) for various methods, comparing Normal, DDoS, MiTM, and Probe is the Attack detection performance. The proposed system attained a 98.54% detection rate, while the existing methods achieved only 93.85% for FFNN, 96.8% for LSTM, 97.12% for RNN.

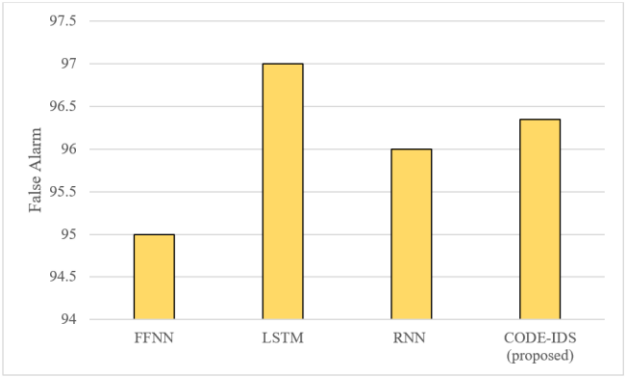

Figure 5. False alarm rate for CODE-IDS framework

Figure 5 represent the false alarm rate 96.35%% for various IDS across the false detection rates. Overall, the proposed CODE-IDS demonstrates superior effectiveness in minimizing false alarms compared to the other methods.

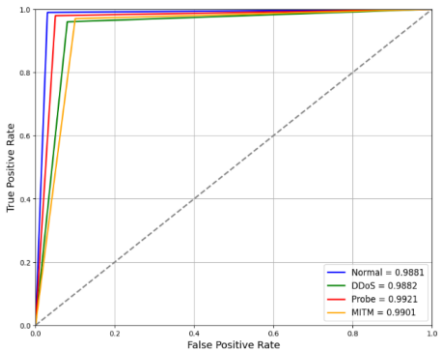

Figure 6. ROC curve for CODE-IDS

Figure 6 demonstrates the Receiver Operating Characteristic (ROC) curves for Normal, DDoS, MiTM, Probe. The ROC curves for the Positive, Negative, and Neutral classes show strong model performance indicating low FPR high and TPR. The model achieves high accuracy, with values of 98%, 97.5%, and 98.3% respectively. The performance across all three classes illustrates the approach's efficiency in accurately distinguishing between the attack detection.

5. CONCLUSION

In this study the novel CODE-IDS framework using deep learning network approach has been proposed to enhance network security by accurately identifying and mitigating cyber threats. The proposed methodology demonstrates a comprehensive and effective solution for enhancing intrusion detection. PCA for feature extraction and feature selection is applied by using Adaptive Weighted Particle Swarm Optimization. Then the deduction of cyberattack is classified as Normal, DDoS, MiTM, Probe, by using ConvBi-LSTM Network. The model framework highlights the need of cybersecurity measures by obtaining the role of the attacker attempting to exploit fault in a variety of smart systems. The overall accuracy of the CODE-IDS method is 98.78% and methods achieving a low accuracy of 93.85% 96.8% and 96.8% respectively. In future improve the model emerging cyberthreats and Testing framework on diverse dataset and to detect more refined attack types. This future validates its performance and stability in real-world 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] M. Udurume, V. Shakhov, and I. Koo, "Comparative Analysis of Deep Convolutional Neural Network—Bidirectional Long Short-Term Memory and Machine Learning Methods in Intrusion Detection Systems", *Applied Sciences*, vol. 14, no.16, pp. 6967, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Angelin, J.A.B. and Priyadharsini, C., 2024, January. Deep learning based network based intrusion detection system in industrial Internet of Things. In *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)* (pp. 426-432). IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[3] Bhuyan, M.K., Kamruzzaman, M., Nilima, S.I., Khatoon, R. and Mohammad, N., 2024. Convolutional Neural Networks Based Detection System for Cyber-Attacks in Industrial Control Systems. *Journal of Computer Science and Technology Studies*, *6*(3), pp.86-96. [CrossRef] [Google Scholar] [Publisher Link]

[4] Jihado, A.A. and Girsang, A.S., 2024. Hybrid deep learning network intrusion detection system based on convolutional neural network and bidirectional long short-term memory. *J. Adv. Inform. Technol*, *15*(2), pp.219-232. [CrossRef] [Google Scholar] [Publisher Link]

[5] Kimanzi, R., Kimanga, P., Cherori, D. and Gikunda, P.K., 2024. Deep Learning Algorithms Used in Intrusion Detection Systems--A Review. *arXiv preprint arXiv:2402.17020*. [CrossRef] [Google Scholar] [Publisher Link]

[6] Priyadarshini, I., 2024. Anomaly detection of iot cyberattacks in smart cities using federated learning and split learning. *Big Data and Cognitive Computing*, *8*(3), p.21. [CrossRef] [Google Scholar] [Publisher Link]

[7] Kumarraja Andanapalli and M. Suresh Kumar, "Dynamic Power Allocation in Iot-Cloud Environment for Healthcare Applications," International Journal of System Design and Computing, vol. 02, no.02, pp. 39-47, 2024 [CrossRef] [Google Scholar] [Publisher Link]

[8] K. Anusha, B. Muthu Kumar and J. Ragaventhiran, "INDIA-NET: IOT INTRUSION DETECTION VIA ENHANCED TRANSIENT SEARCH OPTIMIZED ADVANCED DEEP LEARNING TECHNIQUE," International Journal of Data Science and Artificial Intelligence, vol. 02, no.01, pp. 07-12, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] G. Sreetha and G. Santhiya, "SAFE-ACID: A NOVEL SECURITY ASSESSMENT FRAMEWORK FOR IOT INTRUSION DETECTION VIA DEEP LEARNING," International Journal of Data Science and Artificial Intelligence, vol. 02, no.01, pp. 20-26, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] M. Amanullakhan, M. Usha and S. Ramesh, "Intrusion Detection Architecture (IDA) In IOT Based Security System," International Journal of Computer and Engineering Optimization, Vol. 01, no. 01, pp. 33-42, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Jhansi Bharathi Madavarapu, "CAB-IDS: IoT-based Intrusion Detection using Bacteria Foraging Optimized BiGRU-CNN Network," International Journal of Computer and Engineering Optimization, Vol. 01, no. 02, pp. 63-68, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Vishnu Karthik Ravindran, "Hybrid Graph based Convolutional Neural Network for Intrusion Detection in IoT," International Journal of Computer and Engineering Optimization, Vol. 02, no. 03, pp. 75-79, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] T. Maris Murugan and A Jeyam, "IOT-Enabled Protein Structure Classification Via CSA-PSO Based CD4.5 Classifier," International Journal of Data Science and Artificial Intelligence, vol. 01, no.02, pp. 41-51, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] K. Paul Joshua and A. Jenice Prabhu, "EFFICIENT DATA SEARCH AND RETRIEVAL IN CLOUD ASSISTED IOT ENVIRONMENT," International Journal of Data Science and Artificial Intelligence, vol. 02, no.01, pp. 01-06, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] Souri, A., Norouzi, M. and Alsenani, Y., 2024. A new cloud-based cyber-attack detection architecture for hyper-automation process in industrial internet of things. *Cluster Computing*, *27*(3), pp.3639-3655. [CrossRef] [Google Scholar] [Publisher Link]

[16] M. Devaki, Jeyaraman Sathiamoorthy and M. Usha, "IOT BASED AIR QUALITY MONITORING USING DENSENET IN URBAN AREAS," International Journal of Data Science and Artificial Intelligence, vol. 02, no.04, pp. 121-127, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Bakhsh, S.A., Khan, M.A., Ahmed, F., Alshehri, M.S., Ali, H. and Ahmad, J., 2023. Enhancing IoT network security through deep learning-powered Intrusion Detection System. *Internet of Things*, *24*, p.100936. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

Ramakrishna Hegde currently working as Associate Professor and PG Coordinator, Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysore, Karnataka, India. He holds Ph.D in Computer Science and Information Science from Visvesvaraya Technological University(VTU), Belagavi, Karnataka, India and has vast professional experience of more than 22 years which includes 17 years of teaching. His area of specialization is Cyber Security, Information Security, Data Science, Computer Networks and Image Processing, Wireless Sensor Networks. He is a Senior Member of IEEE and served as secretary of IEEE Computer Society Bangalore Chapter during the year 2021 and 2022. He is currently Treasurer and EXECOM member of IEEE Mysore Subsection, and Chair Elect - IEEE Bangalore System Council. He is an active volunteer in many of the IEEE International Conferences as a Organizing Chair, Technical Committee Member, Session Chair, Reviewer etc., along with managing editor for few international journals. He published more than 30 research papers in reputed international journals and presented more than 25 research papers in high quality international conferences and published 25 patents. He has delivered many numbers of talks on Information and Cyber Security in India and abroad. Apart from this he also regularly delivers expert talks in All India Radio and few news channels. Dr Hegde is certified Cyber Crime Intervention Officer, Certified Lead Auditor – ISO 27001 – 2013 Information Security Management Systems (ISMS) and approved Cyber Volunteer from MHA, Govt. of India. In addition to this, he actively provides the awareness on cyber security to the students and general public. He is a member of many of the world's best technical professional bodies including IEEE, ISTE, CQI/IRCA/ISO(ISMS) etc. He also a research guide of University of Mysore and Visvesvaraya Technological University(VTU), Belgaum, Karnataka, India.

Soumyasri S.M holds Ph.D degree in faculty of science (Master of Computer Applications) under Visvesvaraya Technological University, Belgaum awarded in 2019. Currently working as Associate Professor in the department of MCA and have 15 years of teaching experience. Her area of specialization is WSN, Cyber security, data science, AI and ML, computer networks.She has published more than 20 research papers in reputed International journals and presented more than 15 research papers in high quality International conferences. She volunteered as session chair, reviewer for many IEEE conferences and guided more than 50 UG and PG projects.

Arrived: 20.07.2024
Accepted: 22.08.2024