JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cyber Attack Detection with Pattern Analysis in IoT enabled Wireless Sensor Networks

Dr.V.Lakshman Narayana [1*] , Dr.P.Radhika [2*] ,Mohammad Suhana[3], D.Vyshnavi[4], K.Sirisha[5], M.Manasa[6]

[1,2] Professor:Vignan's Nirula Institute of Technology and Science for Women.
[3,4,5,6] B.Tech Scholar: Vignan's Nirula Institute of Technology and Science for Women.

Abstract:

Due to its deployment in many remote and heterogeneous locations, where small sensor nodes transmit sensitive data on a short timescale, wireless sensor networks (WSNs) present serious security challenges. Battlegrounds, industry, and smart cities are among the areas where IoT-enabled WSNs find use. However, the automatic information flow and networked devices that come with their integration provide new security vulnerabilities. Deploying safe Internet of Things applications requires an understanding of wireless sensor weaknesses. The use of machine learning algorithms which achieve high accuracy in recognizing cyber attacks across various datasets, is highlighted in research on the creation of intrusion detection systems (IDS).To improve detection performance, these models make use of feature reduction methods including SVD, PCA, and K-means clustering. Large-scale deployment of WSNs integrated into IoT ecosystems still depends heavily on security, and current research is concentrated on improving network resilience against malicious actions and minimizing emerging threats. To efficiently identify the intrusions in the network, this research proposes a Multistage Node Pattern Analysis Model for Cyber Attack Detection (MNPAM-CAD) in the WSN. The proposed model when compared with the traditional models performs better in cyber attack detection in WSN.

Keywords: Wireless Sensor Networks (WSNs), Cyber Attacks, Pattern Analysis, Data Loss, Intrusion detection, malicious activities.

1. Introduction

The application of artificial intelligence (AI) for cyber attack detection in wireless sensor networks utilizing a hybrid feature reduction technique requires the creation of a system that can successfully identify and categorize cyber attacks in WSN environments[1]. This strategy combines machine learning and deep learning approaches to minimize the high-dimensional feature space and improve intrusion detection performance. Virtual computers, network topologies, and cloud services are all protected by cyber security[2-15]. It also discourages cybercrimes and helps with forensic investigations.Because the DNS server is not secure enough, hackers can still access its data with the help of external protection. Two applications of machine learning (ML), a form of artificial intelligence, in cyber-security include prediction systems and the detection of zero-day threats. Thus, cyber attacks could raise an unstable situation. Deep learning (DL) can be thought of as a group of machine learning algorithms that are trained on various datasets and go through several phases[16-23]. In light of the surge in cybercrime, cyber security is identifying attacks in WSNs to secure shared and stored data. Many machine learning approaches may render simulated attackers useless for SCADA and VANET intrusion detection systems[24-33]. It focuses on applying the fundamentals and subfields of machine learning to cyber-security, detecting malware, spam, and rejection attacks in addition to biometrically identifying individuals [34-40].

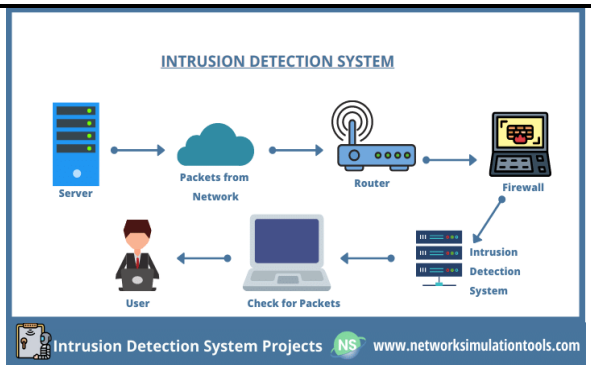

Fig 1: Intrusion detection system

The routing linkages between nodes in wireless sensor networks (WSN) can be interrupted by several types of attacks [41-45]. These attacks can include, but are not limited to, malicious attacks, fake data injection attacks, traffic attacks, HTTP flood attacks, nonrepudiation attacks, eavesdropping attacks, jamming attacks, clock synchronization attacks, spoofing attacks, node replication attacks [46-50]. Unlike other attacks that focus on a particular node or route, some attack disrupts connections between every node along the routing path, setting it apart from previous attacks . In particular, the CONNECT attack arbitrarily severes links between nodes during the routing process in order to purposefully break connections between nodes and obstruct the WSN's normal operation. Throughput adjustments made on a remote node can essentially make the connection vanish for the attacker. Wi-Fi network attacks are forecasted using the phase transition technique [8]. An impersonation attack occurs when a hacker uses a communication protocol or system to pretend to be a reliable party. Impersonation attacks are avoided by using deep feature extraction and selection (D-FES) techniques, which integrate weighted feature selection and stacked feature extraction.

Recent attacks, such as jammer attacks, have targeted wireless communication technologies like Bluetooth and Wi-Fi, highlighting the need of security in this domain. Although jamming attacks can be avoided with the use of the Moving Target Defense approach, there is still room for improvement, especially in relation to connection attacks. Because WSNs transfer a lot of data, intrusion detection is crucial. To combat low accuracy caused by WSN attacks, Multistage Node Pattern Analysis Model for Cyber Attack Detection (MNPAM-CAD) approach is employed. The steps an attacker needs to follow in order to successfully execute a cyber attack are described by the concept of the "cyber kill chain," often known as the lifecycle of a Cyber Attack[51-55]. The usual processes are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and target-oriented activities. Additionally, by understanding the attack lifecycle, businesses may anticipate potential threats and strengthen their defenses accordingly.

2. Literature Survey

Many strategies have been used in recent studies to improve the security and effectiveness of Internet of Things (IoT) infrastructures and wireless sensor networks (WSNs).

Singular Value Decomposition (SVD), Principal Component Analysis (PCA), K-Means Clustering and Information Gain (KMC-IG), Synthetic Minority Over-sampling Technique (SMOTE), and a feed-forward neural network based on deep learning are all combined in Mohamed H. Behiry's (2024) intelligent hybrid model. With the use of deep learning-based intrusion detection and feature reduction, this model aims to enhance WSN security. Using datasets including NSL-KDD, UNSW-NB 15, and CICIDS 2017, the model was assessed and showed good accuracy and performance, early cyber attack detection, and efficient data balancing. However, because of the dynamic conditions, it necessitates a huge amount of labeled data and involves resource consumption trade-offs.

Olivia Jullian (2023) created a distributed system for deep learning-based cyber attack detection in Internet of Things networks that makes use of feed-forward neural networks and Long Short-Term Memory (LSTM). The efficacy and performance of this framework were assessed; it demonstrated good cyber attack detection capabilities and a good fit for distributed IoT networks. Notwithstanding its benefits, there are a number of obstacles to overcome, including the framework's difficult deployment and requirement for big training datasets.

D. Prabakar (2023) introduced a methodology that uses artificial intelligence (AI) and network traffic analysis to detect cyber attacks against Internet of Things (IoT) devices in smart cities. This method adjusted to smart city

surroundings while improving detection capabilities and IoT device security. The hazards related to energy consumption data, the potential for false positives, and the high computational requirements were among the negatives.

Irfan Ahmad (2021) examined a number of security strategies, such as secure routing protocols and cryptographic algorithms, for underwater wireless sensor networks (UWSNs). The study offered a framework for creating safe UWSNs, a taxonomy of dangers, and an enhanced comprehension of UWSN security by recognizing several attacks. Notwithstanding these advantages, the approaches were constrained by the high energy consumption and underwater environment.

Gebrekiros Gebreyesus Gebremariam (2023) concentrated on employing hybrid machine learning techniques to develop sophisticated intrusion detection systems for hierarchically wireless sensor networks. By improving detection accuracy, scalability, and security, this research aims to improve efficiency and security. Nonetheless, the intricacy of execution and substantial computing overhead persisted as constraints.

Together, these studies show how WSN and IoT security are changing and emphasize the need to strike a compromise between controlling implementation complexity and resource requirements and obtaining high detection accuracy.

3. Proposed Model

In order to guarantee the security and dependability of these networked systems, which are being used more and more in a variety of industries, cyber attack detection in Internet of Things (IoT) and Wireless Sensor Networks (WSN) is essential. Traditional detection approaches face major problems from the specific characteristics of IoT and WSN, such as restricted computational resources, power limits, and wireless communication. Because these networks are deployed in open areas. Because there are so many different kinds of devices and communication protocols, efficient detection techniques need to be small, flexible, and able to work in tight spaces.

Researchers are looking into a number of strategies, including as artificial intelligence and machine learning, to improve detection accuracy and flexibility in order to overcome these issues. These techniques continuously learn from new threats, analyze massive amounts of data in real-time, and spot patterns suggestive of malicious behaviour. Through the utilization of these sophisticated methodologies and dynamic detection systems, it is possible to create more robust IoT and WSN systems that can effectively fend off the constantly changing cyber threat scenario.

XGBoost and linear regression are two well-liked machine learning techniques that are applied to various kinds of predictive modelling problems. For regression problems, where the objective is to predict a continuous outcome based on one or more predictor variables, linear regression is a popular model since it is straightforward and easy to understand. In contrast, XGBoost is a more sophisticated and potent ensemble learning method that is mainly employed for classification and regression applications.

3.1 Linear Regression (LR)

A basic statistical technique for simulating the relationship between a dependent variable (goal) and one or more independent variables (features) is called linear regression (LR). By minimizing the sum of squared residuals, it seeks to identify coefficients that best match the data under the assumption of a linear relationship. LR is simple to use, easy to understand, and appropriate in situations where a linear connection between the variables is anticipated. Because of its ease of use and capacity to shed light on variable interactions, it is extensively employed in disciplines such as economics, social sciences, and biological research.

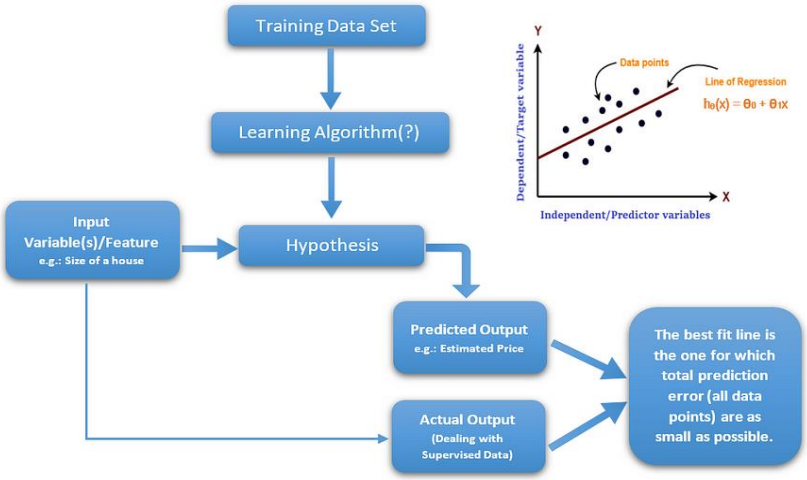

Fig 2: Flow chart of Linear Regression Model

3.2 XGBoost (Extreme Gradient Boosting)

Conversely, XGBoost (Extreme Gradient Boosting) is a sophisticated ensemble learning method that has become well-known for its high predicted accuracy and capacity to manage intricate relationships in structured/tabular data. It functions by gradually constructing a number of weak learners (usually decision trees) and merging them to form a more potent predictive model. XGBoost uses gradient boosting, which adds new models that predict the errors or residuals of previous models iteratively to minimize a loss function. It performs exceptionally well in situations where predictive performance is critical, such machine learning contests and high-accuracy real-world applications. The characteristics include handling missing data,regularization to prevent overfitting, and insights into featurerelevance that help with feature selectionand model interpretability.

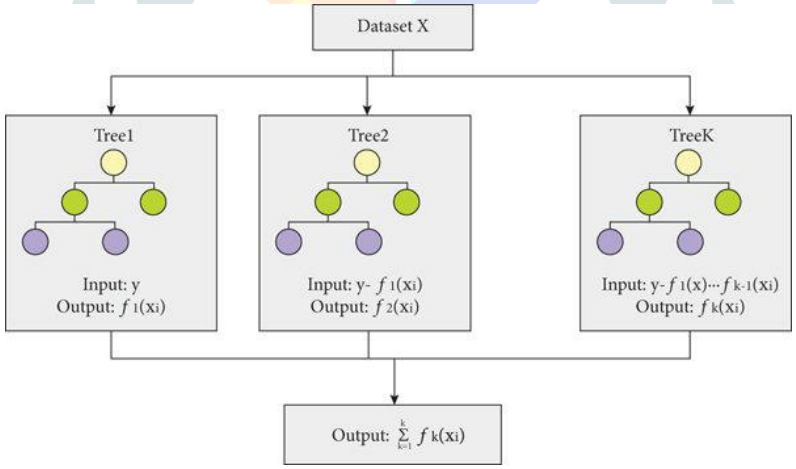

Fig 3: Flow chart of XGBoost framework.

Algorithm 1:Pseudo-code of LR-PFR algorithm

Input Dataset D = DS UDT with feature representation xi
Output Dataset D = DS UDT with feature representation fi
1. Train the LLP classifier with D
2. Predict the pseudo-label values for target data
3. Noisy labels dataset: P ={Xi, Yi}$_{i=1}^{n_s+n_r}$
4. forr=1 to R do
5. Training subset: P^r={m random samples}
6. Train projection functions f^r(.) with P^r using eqn. (4)
7. end

8. for i=1 to $n_s + n_r$ do
for r=1 to R do
Obtain projection vector: $V_i^{\gamma} = f^{\gamma}(x_i)$
end
$V_1 = ((v_i^{\gamma})', ..., (V_i^{R})')'$
End

Algorithm 2: XGBoost Algorithm: Generate Feature Importances

Input: Unormalized(fnorm..... fnorm)
Output: Uoptimal: the selected feature vector
1. Load the normalized feature vector
2. Create an empty dictionary S to save the scores.
3. Instantiate a Gradient BoostingClassifier as clf
4. fit clf
5. Generate Fls
6. Determine the FI threshold FIp
7. for n from Unnormalized do
if (FI(x) FIp) then
append FI(x) into S
end if
end for
8. Use the scores in S to generate Uoptimal

4.Results

The results and discussions section of research articles is essential because it provides context, explanations, and insights along with the Authors analysis of the study's findings. Based on the given facts, the following insightful conclusions may be made from the research and brainstorming sessions in the paper: good detection accuracy across datasets the article shows consistently strong identification accuracy under limited feature conditions for all three datasets. For example, accuracy rates of 99.7%, 99.1%, and 99.8% demonstrate the durability of the proposed MNPAM-CAD technique. High precision rates (e.g., 99.8%) are frequently correlated with high recall rates (97.7 to 98.4%). The comparison demonstrates the potential of the proposed MNPAM-CAD algorithm to outperform conventional methods and validates its superiority both generalizability and adaptability.By efficiently reducing feature dimensionality and leveraging machine learning and deep learning, the system reduces the time it takes to react to potential threats. Future directions examining the algorithm's scalability for larger WSNs, analyzing the impact of new cyberthreats, or looking at real-time implementation in WSN environments are some potential avenues for further research. All of these can be proposed in the discussion section. Evaluation of the proposed method on the dataset in comparison with traditional methods.

This study assesses the suggested approach for binary and multi-class categorization. The approach aims to construct an intrusion detection model. Based on the findings, the suggested MNPAM-CAD method outperforms traditional machine learning algorithms in terms of precision (PRE), recall (RE), maximum accuracy (ACY), and F1-Score. Additionally, MNPAM-CAD models are proven to perform better than traditional machine learning algorithms in exposing sample occurrences with hidden characteristics and identifying more complex forms. The performance of existing machine learning classifiers is enhanced by thefeature reduction techniques. This method outperforms other conventional machine algorithms internationally according to the metrics employed in the study. To conduct multi-class classification on the dataset, the model goes through testing, validation, and training phases. The proposed MNPAM-CAD model is compared with the traditional Cyber attack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods (CAD-HFRT) and Energy Analysis-Based Cyber Attack Detection by IoT with Artificial Intelligence in a Sustainable Smart City (EA-CAD-AI).

4.1. Node Information Accessing Time Levels

Node Information Accessing Time Levels allow for faster data analysis and real-time monitoring, which enhances system resilience to assaults and improves system performance. The node accessing time levels for 3 different models(MNPAM-CAD,CAD-HFRT Model,EA-CAD-AI Model) with respect to the nodes in the network are shown in table1 and fig4 as

Table 1: Node Information Accessing Time Levels

Nodes in the Network	Models Considered		
	MNPAM-CAD Model	CAD-HFRT Model	EA-CAD-AI Model
100	12.6	15.9	20.1
200	12.9	16.1	20.3
300	13.1	16.4	20.5
400	13.5	16.7	20.9
500	13.7	17.0	21.2
600	14	17.2	21.5

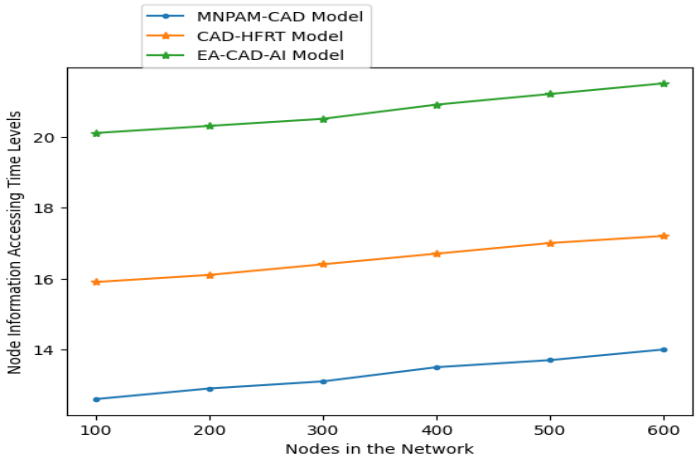

Fig 4: Node Information Accessing Time Levels

4.2. Node Pattern Checking Accuracy Levels

Node pattern checking accuracy levels accurately distinguish between normal and suspicious activity, they improve response times, decrease false positives, and improve the identification of harmful patterns. The node pattern checking accuracy levels for 3 different models(MNPAM-CAD,CAD-HFRT Model,EA-CAD-AI Model) with respect to the nodes in the network are shown in table2 and fig5 as

Table 2: Node Pattern Checking Accuracy Levels

Nodes in the Network	Models Considered		
	MNPAM-CAD Model	CAD-HFRT Model	EA-CAD-AI Model
100	95.6	93.2	88.3
200	95.8	93.5	88.5
300	96.2	93.8	88.8
400	96.5	94.2	89.2
500	96.9	94.5	89.5
600	97.2	94.7	89.8

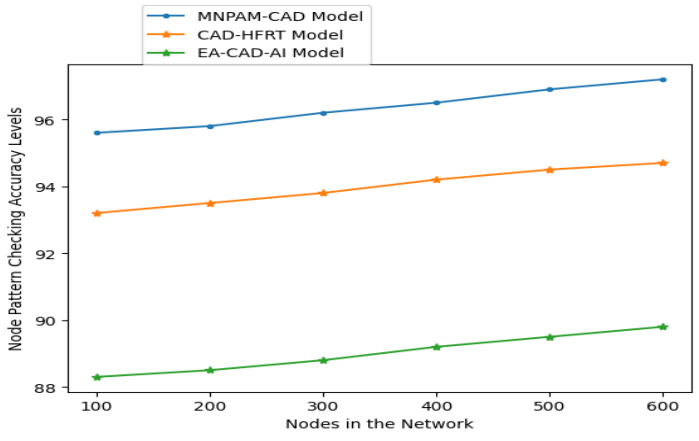

Fig 5: Node Pattern Checking Accuracy Levels

4.3. Multistage Node Information Verification Accuracy Levels

Multistage Node Information Verification Accuracy Levels improve detection accuracy while lowering false positives and false negatives.Multistage node information verification accuracy levels for 3 different models(MNPAM-CAD,CAD-HFRT Model,EA-CAD-AI Model) with respect to the nodes are shown in table3 and fig6 as

Table 3: Multistage Node Information Verification Accuracy Levels

Nodes in the Network	Models Considered		
	MNPAM-CAD Model	CAD-HFRT Model	EA-CAD-AI Model
100	96.1	89.8	90.2
200	96.3	92.2	90.5
300	96.5	92.5	90.9
400	96.9	92.8	91.2
500	97.2	93.2	91.5
600	97.5	93.6	91.8

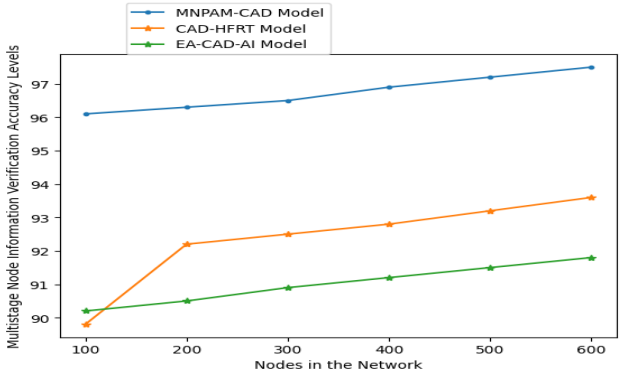

Fig 6: Multistage Node Information Verification Accuracy Levels

4.4. Cyber Attack Detection Accuracy Levels

Cyber attack detection accuracy levels accurately detect real threats, guaranteeingsecurity, and avoiding false positivesandnegatives.Cyber Attack Detection Accuracy Levels for 3 different models(MNPAM-CAD,CAD-HFRT Model,EA-CAD-AI Model) with respect to the nodes are shown in table4 and fig7 as

Table 4: Cyber Attack Detection Accuracy Levels

Nodes in the Network	Models Considered		
	Model	CAD-HFRT Model	EA-CAD-AI Model
100	95.3	92.8	87.1
200	95.6	93.1	87.4
300	95.8	93.4	87.7
400	96.1	93.6	87.9
500	96.5	94.0	88.2
600	96.8	94.3	88.5

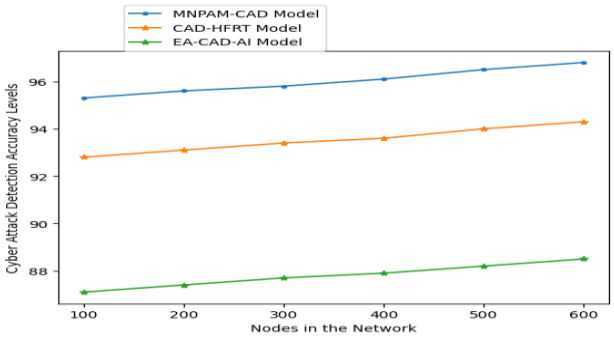

Fig 7: Cyber Attack Detection Accuracy Levels

5. Conclusion

This study evaluated the recommended strategy's recall, accuracy, precision, and F-measure in two different scenarios: with full features and with reduced features. Furthermore, the proposed MNPAM-CAD was compared with machine learning methods that are commonly used in the industry. For the dataset used in, the proposed approach yielded results of 99.7%, 99.8%, 97.8%, and 98.8%, respectively, for accuracy, precision, recall, and F-measure. The proposed method yielded an accuracy, an attack classification, and the parameters for the general machine-learning model. The recommended intelligent hybrid cyber-security system worked wonders in WSN environments for locating and preventing associated attacks. The system effectively reduced the dataset's features for classification. The system generated high-performance features for efficient early detection and learning systems by merging ML and DL. Cyber Attacks are frequent in IoT-WSN. In WSN, cyber attacks take place; they break packets and connections between nodes, making it challenging to pinpoint the attacking node. In the first case, the forward selection approach and in the second, the backward elimination method, comprise the suggested CAM. In order to find several discontinuous loop-free routes in IoT-WSN and identify cyber assaults, the CAM generates routing data and examines IoT-WSN behaviour.CAM collects data metrics from each node, such as CPU and memory usage, and employs a forward and backward selection-based method to detect cyber attack nodes in IoT-WSNs. CAM performance is analyzed using cyber attack node detection accuracy, connection, packet loss, and network traffic. Compared to traditional methods, the CAM in cyber attacks detects around 99% more attack nodes. CAM finds and identifies all of the cyber attacked nodes with efficiency. Using the CAM technique to detect the cyber attack requires less effort and no hardware. CAM is a straightforward method that locates the cyber attack using information from the node. A deep learning hybrid approach for heterogeneous nodes in the network can improve the CAM method even more based on the testing results.

References:

1. Behiry, M. H., & Aly, M. (2024). Cyber attack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods. *Journal of Big Data*, *11*(1), 16.
2. Jullian, O., Otero, B., Rodriguez, E., Gutierrez, N., Antona, H., & Canal, R. (2023). Deep-learning based detection for cyber-attacks in iot networks: A distributed attack detection framework. *Journal of Network and Systems Management*, *31*(2), 33
3. Keerthika, M., & Shanmugapriya, D. (2021). Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures. *Global Transitions Proceedings*, *2*(2), 362-367.
4. Patibandla, R. S. M. L., Rao, B. T., Narayana, V. L., & Srinivas, V. S. (2021). An overview of ontology-based artificial intelligence services in health care systems. In Proceedings of the International Conference on Health Care Systems (pp. 47–63).
5. Maddumala, V. R., Maha Lakshmi, K., Anusha, P., & Lakshman Narayana, V. (2020). Enhanced morphological operations for improving the pixel intensity level. Journal of Computational and Theoretical Nanoscience, 29(3), 9191–9201.
6. Narayana, V. L., Malleswari, K. S. N., Divyanjali, M., Nandini, S., & Purnima, G. (2023). Video frame based prompt compression model with steganography for secure data transmission. In Proceedings of the International Conference on Advanced Intelligent Systems (pp. 373–377). https://doi.org/10.1109/ICAIS56108.2023.10073883
7. Naresh, A., Pavani, V., Meghana Chowdary, M., & Lakshman Narayana, V. (2020). Energy consumption reduction in cloud environment by balancing cloud user load. Journal of Critical Reviews, 7(7), 1003–1010. https://doi.org/10.31838/jcr.07.07.184
8. Patibandla, R. S. M. L., & Vejendla, L. N. (2022). Significance of blockchain technologies in industry. In Advances in Blockchain Technologies (pp. 19–31). https://doi.org/10.1007/978-3-030-70501-5_2

9. Pasala, S., Pavani, V., Lakshmi, G. V., & Narayana, V. L. (2020). Identification of attackers using blockchain transactions using cryptography methods. Journal of Critical Reviews, 7(6), 368–375. https://doi.org/10.31838/jcr.07.06.65
10. Mounika, B., Anusha, P., Narayana, V. L., & Lakshmi, G. V. (2020). Use of blockchain technology in providing security during data sharing. Journal of Critical Reviews, 7(6), 338–343. https://doi.org/10.31838/jcr.07.06.59
11. Narayana, V. L., Vinayaki, K. V., Swetha, P. A., Sri, K. D., & Chaithanya, G. (2024). Superior attribute weighted set for object skeleton detection using ResNet50 with edge-based segmentation model. In Proceedings of the International Conference on Smart Computing and Systems (pp. 1132–1139). IEEE. https://doi.org/10.1109/ICSCSS60660.2024.10624879
12. Gopi, A. P., & Naik, K. J. (2022). An IoT model for fish breeding analysis with water quality data of pond using modified multilayer perceptron model. 2022 International Conference on Data Analytics for Business and Industry (ICDABI), 448-453. https://doi.org/10.1109/ICDABI56818.2022.10041617
13. Arepalli, P. G., & Naik, K. J. (2024). A deep learning-enabled IoT framework for early hypoxia detection in aqua water using lightweight spatially shared attention-LSTM network. Journal of Supercomputing, 80(2), 2718-2747. https://doi.org/10.1007/s11227-023-05580-x
14. Arepalli, P. G., & Naik, K. J. (2023). An IoT-based water contamination analysis for aquaculture using lightweight multi-headed GRU model. Environmental Monitoring and Assessment, 195(12), Article 1516. https://doi.org/10.1007/s10661-023-12126-4
15. Gopi, A. P., Gowthami, M., Srujana, T., Gnana Padmini, S., & Durga Malleswari, M. (2023). Classification of denial-of-service attacks in IoT networks using AlexNet. In Smart Innovation, Systems and Technologies (Vol. 316, pp. 349-357). https://doi.org/10.1007/978-981-19-5403-0_30
16. Bikku, T., Gopi, A. P., & Prasanna, R. L. (2019). Swarming the high-dimensional datasets using ensemble classification algorithm. In Advances in Intelligent Systems and Computing (Vol. 815, pp. 583-591). https://doi.org/10.1007/978-981-13-1580-0_56
17. Arepalli, P. G., & Khetavath, J. N. (2024). Water quality classification using multi-cell RNN in aquaculture ponds for Catla fish. In Lecture Notes in Networks and Systems (Vol. 897, pp. 363-370). https://doi.org/10.1007/978-981-99-9704-6_34
18. Arepalli, P. G., & Naik, K. J. (2024). Water contamination analysis in IoT-enabled aquaculture using deep learning-based AODEGRU. Ecological Informatics, 79, Article 102405. https://doi.org/10.1016/j.ecoinf.2023.102405
19. Arepalli, P. G., & Naik, K. J. (2024). An IoT-based smart water quality assessment framework for aqua-ponds management using Dilated Spatial-temporal Convolution Neural Network (DSTCNN). Aquacultural Engineering, 104, Article 102373. https://doi.org/10.1016/j.aquaeng.2023.102373
20. Gopi, A. P., Narayana, V. L., & Kumar, N. A. (2018). Dynamic load balancing for client-server assignment in distributed systems using genetic algorithm. Ingenierie des Systemes d'Information, 23(6), 87-98. https://doi.org/10.3166/ISI.23.6.87-98
21. Sarada, K., Narayana, V. L., Gopi, A. P., & Pavani, V. (2020). An iterative group based anomaly detection method for secure data communication in networks. Journal of Critical Reviews, 7(6), 208-212. https://doi.org/10.31838/jcr.07.06.39
22. Narayana, V. L., Gopi, A. P., & Chaitanya, K. (2019). Avoiding interoperability and delay in healthcare monitoring system using blockchain technology. Revue d'Intelligence Artificielle, 33(1), 45-48. https://doi.org/10.18280/ria.330108
23. Gopi, A. P., Jyothi, R. N. S., Narayana, V. L., & Sandeep, K. S. (2023). Classification of tweets data based on polarity using improved RBF kernel of SVM. International Journal of Information Technology, 15(2), 965-980. https://doi.org/10.1007/s41870-019-00409-4
24. Narayana, V. L., Gopi, A. P., Khadherbhi, S. R., & Pavani, V. (2020). Accurate identification and detection of outliers in networks using group random forest methodology. Journal of Critical Reviews, 7(6), 381-384. https://doi.org/10.31838/jcr.07.06.67
25. Rao, B. T., Patibandla, R. S. M. L., Narayana, V. L., & Gopi, A. P. (2021). Medical data supervised learning ontologies for accurate data analysis. In Semantic Web for Effective Healthcare Systems (pp. 249-267). https://doi.org/10.1002/9781119764175.ch11
26. Patibandla, R. S. M. L., Gopi, A. P., Narayana, V. L., & Rao, B. T. (2023). Decentralized smart healthcare systems using blockchain and AI. In Blockchain applications in healthcare: Innovations and practices (Vol. 1, pp. 139-154). DOI: 10.1002/9781394229512.ch8

27. Lakshman Narayana, V., & Gopi, A. P. (2020). Enterotoxigenic Escherichia coli detection using the design of a biosensor. Journal of New Materials for Electrochemical Systems, 23(3), 164-166. DOI: 10.14447/jnmes.v23i3.a02
28. Rani, B. M. S., Majety, V. D., Pittala, C. S., Vijay, V., Sandeep, K. S., & Kiran, S. (2021). Road Identification Through Efficient Edge Segmentation Based on Morphological Operations. Traitement du Signal, 38(5).
29. Kanumalli, S. S., Ch, A., & Murty, P. S. R. C. (2020). Secure V2V Communication in IOV using IBE and PKI based Hybrid Approach. International Journal of Advanced Computer Science and Applications, 11(1).
30. .Kiran, S., Kanumalli, S. S., Krishna, K. V. S. S. R., & Chandra, N. (2021). WITHDRAWN: internet of things integrated smart agriculture for weather predictions and preventive mechanism.
31. Chaitanya, Kosaraju, and Sankara Narayanan. "Security and Privacy in Wireless Sensor Networks Using Intrusion Detection Models to Detect DDOS and Drdos Attacks: A Survey." 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2023.
32. Krishna, Komanduri Venkata Sesha Sai Rama, et al. "Classification of Glaucoma Optical Coherence Tomography (OCT) Images Based on Blood Vessel Identification Using .CNN and Firefly Optimization." Traitement du Signal 38.1 (2021).
33. Chaitanya, Kosaraju, et al. "Predicting the Spread of Covid Disease Based on Chest X-Ray Images Using Convolutional Neural Network with Improved Accuracy." 2023 6th International Conference on Advances in Science and Technology (ICAST). IEEE, 2023.
34. Ekkurthi, A., Sujatha, V., Kumar, K.V.,"Effective Moving Object Tracking Using Adaptive Background Subtraction with Advanced Probability Evolutionary Algorithm",International Journal on Recent and Innovation Trends in Computing and Communication, 2023, 11, pp. 1–3
35. Sujatha, V., Yaddala, M., Kollipara, V., Shaik, K., Burri, R.K(23),"Movie reviews data classification using convolution neural networks",AIP Conference Proceedings. 2023, 2724, 030009
36. Godavarthi, B., Majety, V. D., Mrudula, Y., & Nalajala, P. (2019). Fault identification in power lines using GSM and IoT technology. Advances in Intelligent Systems and Computing, 815, 647–655. https://doi.org/10.1007/978-3-319-91117-2_70
37. Majety, V. D., & Murali, G. (2018). A remote epileptic patient supervising system. Advances in Modelling and Analysis B, 61(4), 207–210. https://doi.org/10.18280/ama_b.610402
38. Naresh, A., TSLP, H., Ch, G., & Kumari, G. R. P. (2023, July). Early Prophecy of Low-Birth-Weight Babies Using BM Error Rate Classifier. In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
39. Kumari, G. R. P., Reddy, A. H., Lakshmi, K., Abhinaya, B., Sanjana, S., & Naresh, A. (2024, March). Time-Frame-Based Drowsiness Detection System Using CNN. In 2024 2nd International Conference on Disruptive Technologies (ICDT) (pp. 711-716). IEEE.
40. V. Pavani, K. Divya, V. V. Likhitha, G. S. Mounika and K. S. Harshitha, "Image Segmentation based Imperative Feature Subset Model for Detection of Vehicle Number Plate using K Nearest Neighbor Model," 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2023, pp. 704-709, doi: 10.1109/ICAIS56108.2023.10073848.
41. V. Pavani, M. N. Swetha, Y. Prasanthi, K. Kavya and M. Pavithra, "Drowsy Driver Monitoring Using Machine Learning and Visible Actions," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022, pp. 1269-1279, doi: 10.1109/ICEARS53579.2022.9751890.
42. Sri, Kurra Santhi, et al. "Advanced system control with traffic handling for secure communication in IoT routing protocol." Journal Européen des Systèmes Automatisés 54.2 (2021): 229-233.
43. Arumugham, Vinothini, et al. "An explainable deep learning model for prediction of early-stage chronic kidney disease." Computational Intelligence 39.6 (2023): 1022-1038.
44. Majety, Vasumathi Devi, et al. "Enhanced secure communication AODV routing protocol using SVM in MANETS." AIP Conference Proceedings. Vol. 2724. No. 1. AIP Publishing, 2023.
45. Krisha, P.S., Peram, S.R. (2023). CT image precise denoising model with edge based segmentation with labeled pixel extraction using CNN based feature extraction for oral cancer detection. Traitement du Signal, Vol. 40, No. 3, pp. 1297-1304. https://doi.org/10.18280/ts.400349
46. P. S. Krishna, V. R. Aparna, V. Priyanka, P. T. Niharika and T. Shivangi, "Convolution Neural Network Model with Feature Linked Vector for Oral Cancer Detection," 2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 2023, pp. 304-308, doi: 10.1109/CSNT57126.2023.10134660.
47. Rayachoti, Eswaraiah, Sudhir Tirumalasetty, and Silpa Chaitanya Prathipati. "SLT based watermarking system for secure telemedicine." Cluster Computing 23.4 (2020): 3175-3184.
48. Eswaraiah, Rayachoti, Tirumalasetty Sudhir, and Prathipati Silpa Chaitanya. "Curvelet transform based watermarking for telemedicine." Wireless Personal Communications 122.1 (2022): 309-329.

49. Varshini, Y., Mounika, T., Kumari, G. R. P., Sirisha, G., & Deepthi, Y. (2023, March). Crop Yield Forecast Using Machine Learning. In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 2310-2315). IEEE.
50. B. Aruna Kumari "Time Series Data Classification for Precise Stock Market Price Prediction using ML" ICICACS International Conference on Integrated Circuits and Communication Systems, Scopus indexed, ISBN:979-8-3503-1755-8/ https://ieeexplore.ieee.org/document/10498248,18 April 2024
51. B.Aruna Kumari "HumanvAction Recognition From Video Frames Using Recurrent Neural Networks" ICDT 2nd International Conference on Disruptive Technologies (ICDT),Scopis indexed , ISBN:979-8-3503-7105-5/ https://ieeexplore.ieee.org/document/10489658, 11 April 2024
52. Prabakar, D., Sundarrajan, M., Manikandan, R., Jhanjhi, N. Z., Masud, M., & Alqhatani, A. (2023). Energy Analysis-Based Cyber Attack Detection by IoT with Artificial Intelligence in a Sustainable Smart City. *Sustainability*, *15*(7), 6031.
53. Ortiz-Ruiz, E., Bermejo, J. R., Sicilia, J. A., & Bermejo, J. (2024). Machine Learning Techniques for Cyber attack Prevention in IoT Systems: A Comparative Perspective of Cyber security and Cyberdefense in Colombia. *Electronics*, *13*(5), 824.
54. Ahmad, I., Rahman, T., Zeb, A., Khan, I., Ullah, I., Hamam, H., & Cheikhrouhou, O. (2021). Analysis of security attacks and taxonomy in underwater wireless sensor networks. *Wireless Communications and Mobile Computing*, *2021*(1), 1444024.
55. Gebremariam, G. G., Panda, J., & Indu, S. (2023). Design of advanced intrusion detection systems based on hybrid machine learning techniques in hierarchically wireless sensor networks. *Connection Science*, *35*(1), 2246703.