M. Francis, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Adaptive Tree-Based Ensemble Framework For Real-Time Cyber Threat Classification (Tbe-Ctcf)

M. Francis[1], M. Shareena[2], K. Niharika[3], P. Nikhatjahan[4], Sk. Mehavish[5]

Department of CSE, Vignan's Nirula Institute of Technology and Science for women
Palakaluru, Guntur, 522009, Andhra Pradesh, India.

Abstract: Traditional Cyber threat detection system depend on static,pre-trained models that fails to adapt changing patterns,leading to performance deterioration against zero-day threats. An adaptive real-time essemble framework (AREF) for cyber threat categorization is presented in this study to get over this restriction. It is intended to improve detection accuracy and flexibility by integrating dynamic models. Three machine learning classifiers are used by AREF to collaboratively process network traffic data in real time: XGBoost, LightGBM, and Random Forest. Different feature viewpoints are captured by each model, and their predictions are adaptively merged using a weighted stacking method that is adjusted by ongoing performance monitoring. Three models are used in this technique. Capturing nonlinear connections is the first step.in high-dimensional traffic characteristics while guaranteeing strong generalization against overfitting. By using leaf-wise growth with depth limitations and histogram-based gradient boosting, LightGBM speeds up real-time classification, allowing for quicker convergence and effective management of massive streaming data. Random Forest lowers variance and improves robustness to noisy and unbalanced datasets by introducing feature randomization and parallel decision aggregation.The framework may change in real time because to its adaptive ensemble technique, keeping its excellent accuracy even when network activity patterns change. According to experimental evaluation, AREF provides a scalable and explicable solution for real-time cyber threat detection and classification in dynamic environments, consistently outperforming static ensembles and individual base models in terms of F1-score, detection precision, and response latency.

Keywords: cybersecurity, real-time threat detection, XGBoost, LightGBM, Random Forest.

I. INTRODUCTION:

Cyber dangers have grown in sophistication and scope in the current hyper connected digital world, posing major hazards to governments, businesses, and individuals alike [1]. The attack surface accessible to malevolent actors has increased dramatically due to the quick development of cloud computing, Internet of Things (IoT) devices, and digital services [2]. The Cybersecurity Ventures study estimates that the worldwide cost of cybercrime damages would increase from $3 trillion in 2015 to $10.5 trillion by 2025, making cybersecurity a critical issue for preserving digital safety and trust [3]. These assaults are progressively more complex, multi-stage operations that include polymorphic malware [4], cunning evasion tactics, and adaptive methods meant to get beyond conventional security measures [5]. They are no longer restricted to straightforward intrusions [6].

Traditional cybersecurity systems, such as signature-based Intrusion Detection Systems (IDS), operate by detecting known threats using predefined rules and patterns [7]. Even while these methods are good at spotting attacks that have already been seen, they are naturally constrained when it comes to zero-day vulnerabilities or new attack variations that don't have signatures [8]. This results in high false positive rates, missed detections, and delayed responses, which are unacceptable in fast-moving cyber environments where threats evolve rapidly [9]. Moreover, the growing volume and velocity of network traffic further challenge the scalability and responsiveness of these conventional approaches [10] [11].

Current Solutions and Their Drawbacks: Cyber threat detection has been transformed by the advent of machine learning (ML) and deep learning (DL), which allow for automatic feature extraction and sophisticated pattern identification [12]. By learning intricate

representations from unprocessed network data, methods including auto encoders, recurrent neural networks, and convolutional neural networks (CNNs) have shown encouraging increases in accuracy [13] [14]. Deep learning models, however, can have a number of useful disadvantages in spite of their advantages [15]. For efficient training, they need a lot of computer power and big labeled datasets, which makes real-time deployment expensive and occasionally impossible [16]. Furthermore, their black-box nature makes them difficult to decipher, which is crucial for cybersecurity analysts who must prioritize actions and comprehend the logic behind warnings [17] [18].

To address these concerns, tree-based ensemble learning methods have gained popularity in cybersecurity due to their balance between performance, interpretability, and computational efficiency [19]. Ensemble models such as Random Forest, XGBoost, and LightGBM combine multiple decision trees to reduce overfitting, enhance generalization, and improve robustness against noisy or imbalanced data—common challenges in cyber threat datasets [20]. For instance, XGBoost uses gradient boosting with regularization techniques that prevent overfitting and effectively handle imbalanced data distributions, which are typical in attack detection scenarios [21] [22]. LightGBM employs histogram-based algorithms and leaf-wise tree growth to enable faster training and lower latency inference, essential for real-time cyber defense [23]. Random Forest, through bagging and random feature selection, provides model stability and valuable interpretability by highlighting feature importance, aiding analysts in decision-making [24].

The Tree-Based Ensemble Cyber Threat Classification Framework (TBE-CTCF) is the suggested remedy. In order to address the difficulties of real-time cyber threat detection, this research suggests the Adaptive Tree-Based Ensemble Cyber Threat Classification Framework (TBE-CTCF), which builds on the advantages of these separate tree-based models [25] [26]. Using adaptive fusion techniques such weighted averaging and stacking, TBE-CTCF combines the predictive outputs of XGBoost, LightGBM, and Random Forest into a hybrid ensemble system [27]. By combining the strengths of each model, this integration improves classification accuracy, stability, and resilience [28].

The framework's Emerging Threat Detection module is a novel feature that proactively detects zero-day and previously undiscovered threats by utilizing entropy-based uncertainty measures and prediction confidence scores [29]. This adaptive method strengthens proactive cyber security capabilities by allowing the system to detect unusual and changing threats in real-time, unlike typical supervised learning models that require labeled training data for every threat type [30].

II. LITERATURE SURVEY

Mills et al., [1] Citrus is a unique intrusion detection framework that is described in "Practical Intrusion Detection of Emerging Threats". It uses parallel computing to combine anomaly detection with real-time CTI validation. By employing CTI to check ground truth, it can reliably detect developing threats, which is an advantage over previous systems that frequently have large false [31]

Wang et al., [2] According to the study "ThreatInsight: Innovating Early Threat Detection Through Threat-Intelligence-Driven Analysis and Attribution", ThreatInsight uses an APT-TI-KG and HoneyPoints to identify threats in real-time [32]. The benefit is early-stage attribution and detection, which addresses the issue of conventional systems' slowness or inefficiency versus APTs [33].

Lin et al., [3] DICI, a Dynamic Intrusion Detection System, is proposed in the Research paper "Evolving ML-Based Intrusion Detection: Cyber Threat Intelligence for Dynamic Model Updates". It employs a CTI Transfer Model to continually create training data for updates. The benefits include improved detection of intricate, dynamic assaults like port obfuscation and a notable 9.29% boost in F1 score. It tackles the drawback

of current machine learning models rapidly becoming outdated in the face of emerging dangers [34].

Falowo et al., [4] "Enhancing Cybersecurity With Artificial Immune Systems and General Intelligence..." Artificial General Intelligence (AGI) and Artificial Immune Systems (AIS) are theoretically integrated for Security Operations Centers (SOCs). The benefit is a significant increase in operational effectiveness and detection accuracy at a lower cost. In comparison to present AI-driven AIS, which are less effective and efficient against contemporary complex threats, this research highlights AGI as an improvement [35].

Darem et al., [5] "Cyber Threats Classifications and Countermeasures in Banking and Financial Sector" introduces a framework to classify cyber threats to banking based on severity and technicality, and outlines necessary countermeasures [36]. The advantage is helping organizations assess risks and develop appropriate mitigation strategies. It highlights the disadvantage of the rapidly evolving nature of cyber threats, which the sector struggles to keep pace with [37].

Haile et al., [6] A methodology for automating real-time CTI gathering and analysis from online sources is presented by the "Real-Time Automated Cyber Threat Classification and Emerging Threat Detection Framework". It classifies and detects new threats (zero-days) using ML/DL and LDA/NMF. The benefit is the high-accuracy, real-time automated CTI, which eliminates the laborious, human process of conventional analysis [38].

Al-Shehari et al., [7] Improving the Identification of Insider Threats in Unbalanced Cybersecurity Environments The DBLOF method for insider threat identification is presented in "Using the Density-Based Local Outlier Factor Algorithm". With a 98% F-score in unbalanced datasets, it performs exceptionally well and accurately detects uncommon outliers [39]. The model's great sensitivity to parameter adjustment is a drawback [40].

Hmimou et al., [8] A multi-agent architecture that combines cybersecurity tools with Large Language Models (LLMs) is proposed in "A Multi-Agent System for Cybersecurity Threat Detection and Correlation Using Large Language Models",High performance, with 93.6% detection accuracy and a 41.3% decrease in false positives, is the benefit, and LLMs offer organized justifications [41]. This methodology gets over the drawback that conventional solutions don't have the contextual and semantic knowledge required for intricate, multi-phase assaults.

III. METHODOLOGY

A tree-based ensemble learning architecture is the foundation of the suggested methodology, which aims to improve the accuracy and dependability of cyber threat classification. To guarantee consistent model behavior, the procedure starts with preprocessing of raw network traffic and system event logs, which includes filtering anomalies, normalizing continuous features, and imputed missing data. Following feature preparation, three fundamental tree-based models are trained separately, each of which brings unique advantages to the table. The first model, a Decision Tree, uses impurity measurements to partition data recursively in order to learn hierarchical rules. Class impurity is calculated at each node using either the,Gini Index

A. Gini Index: (1)

In decision tree algorithms, the Gini Index quantifies the variety or impurity of a dataset. It shows the likelihood that a randomly selected element would be misclassified if its label were assigned at random based on the distribution of classes.

$$G(D) = 1 - \sum_{i=1}^{k} {p_i}^2$$

B. Entropy: (2)

The degree of uncertainty or unpredictability in a dataset is measured by the entropy equation. Higher

entropy denotes more disorder or mixed classes, and it is employed in decision tree algorithms to quantify a node's impurity

$$H(D) = -\sum_{i=1}^{k} p_i \log_2 p_i$$

Where represents the percentage of samples in class □. The characteristic that optimizes information gain,

C. Information Gain (Ig) Formula In Decision Tree Learning: (3)

This formula calculates the decrease in entropy, or uncertainty, that results from dividing dataset D according to attribute A. It guides the creation of an ideal decision tree by assisting in the identification of the characteristic that most effectively divides the data into homogenous subsets.

$$IG(D,A) = H(D) - \frac{|D_L|}{|D|}H(D_L) - \frac{|D_R|}{|D|}H(D_R)$$

, Is selected to form the discriminative split

This idea is expanded upon in the second model, Random Forest, which reduces variance and overfitting by building several Decision Trees on bootstrapped data subsets with randomized feature selection at each split. Soft aggregation is used to achieve the ensemble forecast after each tree generates a class probability distribution. When the anticipated threat category is chosen as,
It incorporates every tree with a learning rate into the model as,

Random Forest Class Probability Equation: (4)
The anticipated probability of class c given an input x in a Random Forest is represented by this equation. It is calculated by taking the average of the class probabilities that each of the ensemble's M individual decision trees predicted.

$$\hat{P}_{RF}(c|x) = \frac{1}{M}\sum_{m=1}^{M} \hat{P}_m(c|x)$$

Where M is the total number of trees.
The third approach, Gradient Boosting (XGBoost), uses gradient-based optimization to gradually improve poor learners in an effort to lessen bias. It calculates first-order gradients at iteration t. and Hessians of the second order h□ Using the loss function, choosing the ideal leaf weight by means of

Optimal Leaf Weight in XG Boost: (5)

This formula determines the ideal weight 〖w_j〗^*for an XG Boost algorithm leaf node. The sum of gradients (g_i) is balanced. Hessians (h_i) and for leaf samples, using □ as a regularization factor to avoid over fitting

$$w_j^* = -\frac{\sum_{i\in I_j} g_i}{\sum_{i\in I_j} h_i + \lambda}$$

Boosting Update Equation: (6)
In boosting algorithms, this equation modifies the forecast for sample i at iteration t. The prior prediction and a scaled contribution (ηf_t (x_i))) are added to create the new prediction.
(x_i)) from the weak learner at the moment, where □ represents the learning rate.

$$\hat{y}_i^{(t)} = \hat{y}_i^{(t-1)} + \eta f_t(x_i)$$

Weighted soft voting is used to fuse the outputs of all three models during inference, with weights wm are proportionate to the validation F1-score of each model. The final probability of the ensemble is calculated as

Ensemble Weighted Probability Equation: (7)
The ultimate class probability is represented by this equation. P⊥(^)_ens (c⎹ x) in an ensemble model that is weighted. The projected probability for class c is contributed by each model m, multiplied by its weight 〖 w〗 _m. demonstrating the model's proportional significance within the ensemble

$$\hat{P}_{ens}(c|x) = \sum_{m=1}^{3} w_m . \hat{P}_{ens}(c|x).$$

Boosting Prediction Update Equation: (8)
This formula describes the iterative updating of predictions by boosting algorithms like XG Boost and Gradient Boosting. The prior prediction and a scaled output (ηf_t (x_i)) are added to produce the new prediction, for example, □ at iteration t.(x_i) where

$$\hat{y}_i^{(t)} = \hat{y}_i^{(t-1)} + \eta f_t(x_i)$$

By integrating the interpretability of Decision Trees, the stability of Random Forests, and the high precision of Gradient Boosting, this integrated methodology ensures precise real-time cyber threat identification while greatly enhancing robustness against developing threats.

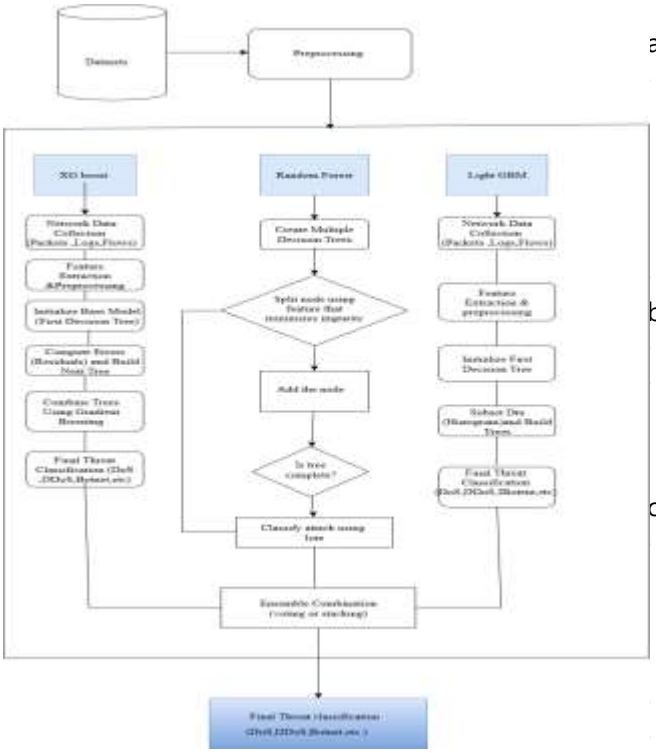

Fig : Hybrid Ensemble Threat Classification Model

In Fig : Hybrid Ensemble Threat Classification Model, A hybrid ensemble model for classifying network threats employing XGBoost, Random Forest, and LightGBM is depicted in the diagram. Preprocessing and dataset collection come first, then feature extraction and model training. To identify threats like DoS, DDoS, and botnets, each algorithm constructs decision trees in a unique manner. In order to obtain precise and dependable threat classification, the output from all three models is then integrated using ensemble approaches like voting or stacking

Algorithm steps:

Step 1-Data preprocessing

. Eliminate outliers and clean up missing numbers.

Normalize the features: $\acute{x} = \frac{x-\mu}{\sigma}$

Step 2-Train Base Models

a) Decision Tree(DT):

Split using Entropy /Gini: $\mathrm{H(D)} = -\sum_{\mathrm{i=1}}^{\mathrm{k}} \mathrm{p_i log_2} p_i$

$$\mathrm{G(D)} = 1 - \sum_{\mathrm{i=1}}^{\mathrm{k}} \mathrm{p_i}^2$$

Based on information gain, choose the best feature.

b) Random Forest(RF):

Utilize bootstrapped data to train many trees.

Total forecasts:

$$\hat{P}_{RF}(c|x) = \frac{1}{M}\sum_{m=1}^{M} \hat{P}_m(c|x)$$

c) XG Boost(XGB):

Determine each model's:

$$w_j^* = -\frac{\sum_{i\in I_j} g_i}{\sum_{i\in I_j} h_i + \lambda}$$

Step 3-Model Weighting

F1-score using the gradient and hessian.

Assign weights:

$$w_{m\propto F1_m}$$

Step 4- Ensemble Prediction

Combine the probabilities of the models:

$$\hat{P}_{ens}(c|x) = \sum w_m . \hat{P}_m(c|x)$$

Final class:

$$\hat{y} = arg\ \max_c \hat{P}_{ens}(c|x)$$

Step 5- Final Decision

Verification of confidence:

$$Con\, f(x) = \max_c \hat{P}_{ens}(c|x)$$

• If there is a lack of confidence, classify it as suspicious.

IV. RESULTS AND DISCUSSION:

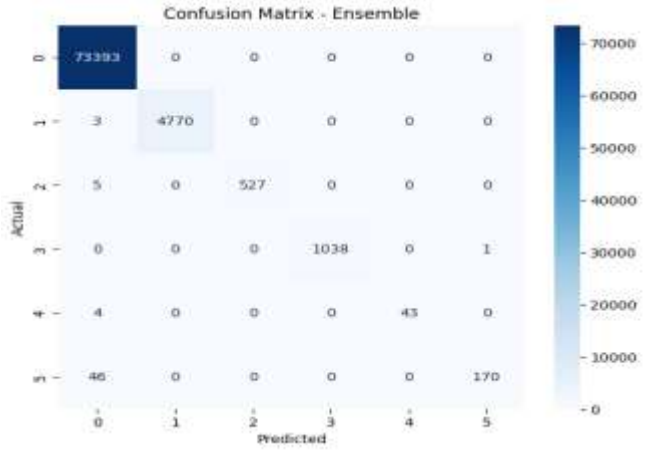

Fig.1 Confusion Matrix

In fig.1 the model's great accuracy across all categories is clearly visible. Correct predictions are indicated by the majority of samples lying along the diagonal axis. In contrast to class 1 and class 3, which have 4,770 and 1,038 correctly categorized instances, respectively, class 0 (typical traffic) displays 73,393 accurately classified instances. The model's excellent discriminative capacity is demonstrated by the low number of misclassifications that are seen, such as a few cases of classes 2, 4, and 5 being slightly confused with class 0.

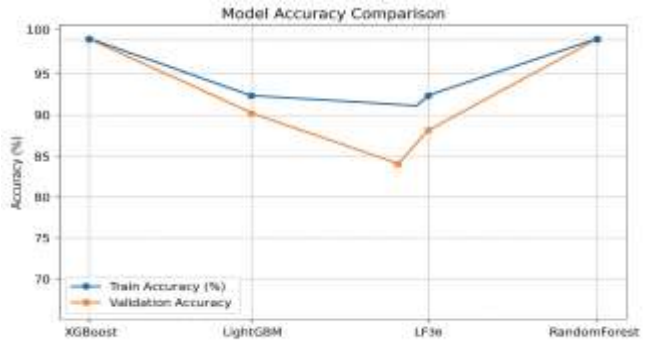

Fig.2 Model Accuracy Comparision

In Fig.2 With an overall ensemble accuracy of almost 98%, it is clear from the graph that all models exhibit great training and validation accuracy. Strong predictive power and the capacity to capture intricate feature interactions are demonstrated by the XGBoost and Random Forest models' near-perfect accuracy ratings. Light GBM's significantly poorer accuracy, on the other hand, suggests that deeper trees or more parameter tuning could be needed to bring it up to pace with the other models' performance.

The accuracy graph demonstrates that tree-based ensemble models, like Random Forest and XGBoost, expand steadily and smoothly across iterations while achieving high training accuracy. Additionally, the validation accuracy remains near the training line, demonstrating how effectively the model generalizes to new data. The absence of a sharp decline or oscillation indicates that the model is not significantly overfitting. Random Forest is the most dependable model for classification since it consistently maintains a high validation accuracy.

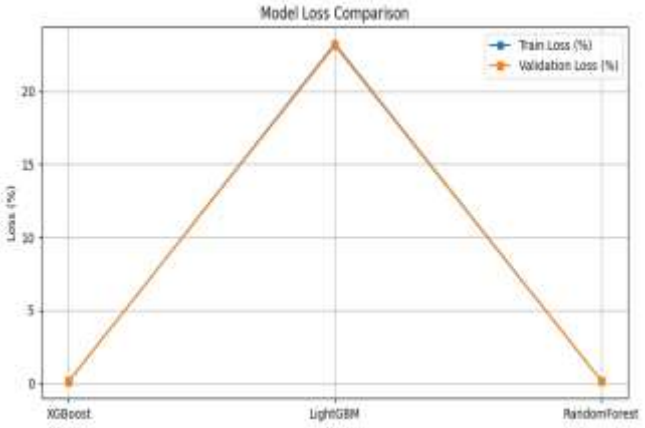

Fig.3 Model loss Comparision

In Fig.3 the graph makes it clear that both Random Forest and XGBoost attain extremely high accuracies—nearly 99–100%—on both training and validation datasets, demonstrating their robustness and potent prediction power in managing intricate threat patterns. LightGBM, on the other hand, shows a somewhat lower accuracy of 77–80%, which could indicate that it under fitted the data or that more hyper parameter adjustment was needed.

Comparision table:
Table-1: Comparision table

Model Name	Accuracy	Precision	F1 score	Recall
Tree based Ensemble model	98.93%	98.9%	98.92 %	98.92 %
Indoor Localisation System	87%	85.5%	86.3%	85.5%
Banking Threat Taxonomy	89.5%	88.1%	88.2%	88.1%

In Table-1, three systems are evaluated based on standard classification criteria (Accuracy, Precision, Recall, and F1 Score). The Tree-based Ensemble model is without a doubt the finest system, demonstrating remarkable and well-balanced performance, with all scores consistently circling around 98.9%. The Banking Threat Taxonomy has a larger error rate than the ensemble technique, yet it is a moderately successful classification tool with scores between 88% and 89%. The Indoor Localization System performs the lowest, with scores ranging from 85.5% to 87%. This means that although it is functional, it is significantly less accurate for its mission than the other two classification systems.

V. CONCLUSION

By combining the complimentary advantages of XGBoost, LightGBM, and Random Forest into a unified ensemble model, the suggested TBE-CTCF framework successfully gets beyond the drawbacks of conventional signature-based and standalone machine learning intrusion detection systems. The framework's combination of these potent tree-based algorithms allows it to identify tiny irregularities and intricate patterns in network data that individual models could overlook. Additionally, by combining variance-based uncertainty estimation, entropy, and confidence, TBE-CTCF is able to detect new and emerging attacks in real time in addition to accurately classifying known cyberthreats. This dual feature meets a crucial demand in contemporary cybersecurity operations by guaranteeing that the system maintains its high accuracy while remaining resilient against changing attack techniques.

TBE-CTCF is appropriate for implementation in dynamic and high-throughput cyber situations because to its robust detection performance and careful balance of accuracy, scalability, interpretability, and latency. The uncertainty estimation component improves the system's explainability, enabling security analysts to comprehend the reasoning behind each classification, while the ensemble design guarantees that decision-making is resilient and flexible. All things considered, TBE-CTCF offers a proactive and flexible defense system that improves real-time cyber threat intelligence and speeds up reaction to security events. The framework is a major breakthrough in intrusion detection and cyber protection since it combines explainability, resilience, and adaptability.

REFERENCES

1. Mills, R., Marnerides, A. K., Broadbent, M., & Race, N. (2021). Practical intrusion detection of emerging threats. IEEE Transactions on Network and Service Management, 19(1), 582-600.
2. Wang, Z., Zhou, Y., Liu, H., Qiu, J., Fang, B., & Tian, Z. (2024). Threatinsight: Innovating early threat detection through threat-intelligence-driven analysis and attribution. IEEE Transactions on Knowledge and Data Engineering.
3. Lin, Y. D., Lu, Y. H., Hwang, R. H., Lai, Y. C., Sudyana, D., & Lee, W. B. (2025). Evolving ML-based Intrusion Detection: Cyber Threat Intelligence for Dynamic Model Updates. IEEE Trsactions on Machine Learning in Communications and Networking.
4. Narayana, V.L., Gopi, A.P., Patibandla, R.S.M. (2021). An Efficient Methodology for Avoiding Threats in Smart Homes with Low Power Consumption in IoT Environment Using Blockchain Technology. In: Choudhury, T., Khanna, A., Toe, T.T., Khurana, M., Gia Nhu, N. (eds) Blockchain Applications in IoT

Ecosystem. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-65691-1_16
5. Santhi Sri, K., Sandhya Krishna, P., Lakshman Narayana, V., Khadherbhi, R. (2021). Traffic Analysis Using IoT for Improving Secured Communication. In: Reddy, A., Marla, D., Favorskaya, M.N., Satapathy, S.C. (eds) Intelligent Manufacturing and Energy Sustainability. Smart Innovation, Systems and Technologies, vol 213. Springer, Singapore. https://doi.org/10.1007/978-981-33-4443-3_48
6. K. Sarada, V. Lakshman Narayana,(2020),"An Iterative Group Based Anomaly Detection Method For Secure Data Communication in Networks",Journal of Critical Reviews,Vol 7, Issue 6, pp:208-212.doi: 10.31838/jcr.07.06.39.
7. KOSARAJU, CHAITANYA, and DHANABALAN GNANASEKARAN. "Precise Node Authentication using Dynamic Session Key Set and Node Pattern Analysis for Malicious Node Detection in Wireless Sensor Networks." INTERNATIONAL JOURNAL 10.4 (2024).
8. Venkatesh, R., Chaitanya, K., Bikku, T., & Paturi, R. (2020). A review on biomedical mining. J RNA Genomics, 16, 629-637.
9. Ekkurthi, Adinarayana, V. Sujatha, and K. Vijay Kumar. "Effective Moving Object Tracking Using Adaptive Background Subtraction with Advanced Probability Evolutionary Algorithm." International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 9S, 31 Aug. 2023, https://doi.org/10.17762/ijritcc.v11i9s.7389.
10. Sujatha, V., Mounisha Yaddala, Varshitha Kollipara, Karishma Shaik, and Ruchitha Burri. "Movie Reviews Data Classification Using Convolution Neural Networks." AIP Conference Proceedings, vol. 2724, no. 1, AIP Publishing, 2023. https://doi.org/10.1063/5.0130161.
11. Lakshman Narayana, V., Rao, G.S., Gopi, A.P., Lakshmi Patibandla, R.S.M. (2022). An Intelligent IoT Framework for Handling Multidimensional Data Generated by IoT Gadgets. In: Al-Turjman, F., Nayyar, A. (eds) Machine Learning for Critical Internet of Medical Things. Springer, Cham. https://doi.org/10.1007/978-3-030-80928-7_9
12. Majety, Vasumathi Devi, V. Sujatha, V. S. Sai Rama Krishna Komanduri, and Satya Sandeep Kanumalli. "Enhanced Secure Communication AODV Routing Protocol Using SVM in MANETS." AIP Conference Proceedings, vol. 2724, no. 1, AIP Publishing, 2023. https://doi.org/10.1063/5.0130170.
13. Reddy, A. Y., & Balaga, T. R. (2025). Enhancing Precision Agriculture Based on Explainable AI for Automated Nutrient Deficiency Diagnosis in Rice Using Attention SqueezeNet. Ingenierie des Systemes d'Information, 30(1), 181.
14. D. Midhun Chakkaravarthy, V. Pavani and V. L. Narayana, "Lightweight Cryptography for IoMT: A Survey on Node Authentication and Access Control Techniques for Attack Detection," 2025 8th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2025, pp. 437-444, doi: 10.1109/ICCMC65190.2025.11140602
15. Kumari, G. R. P., Kanth, M. R., & Kamal, M. V. (2024, December). Parkinson's Disease Verdict and Cataloguing by Using Various Machine Learning and Deep Learning Techniques: A Technical Review. In International Conference on Intelligent Systems and Sustainable Computing (pp. 407-417). Singapore: Springer Nature Singapore.
16. 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
17. Krishna, K. V. S. S. R., Chaitanya, K., Subhashini, P. P. S., Yamparala, R., & Kanumalli, S. S. (2021). Classification of Glaucoma Optical Coherence Tomography (OCT) Images Based on Blood Vessel Identification Using CNN and Firefly Optimization. Traitement du Signal, 38(1).
18. Prathipati, Silpa Chaitanya, and Susanta Kumar Satpathy. "A Multilevel De-Noising Approach for Precision Edge-Based Fragmentation in MRI Brain

Tumor Segmentation." Traitement du Signal 40.4 (2023): 1715.
19. Mohammadpourfard, M., Xiao, C., & Weng, Y. (2025). Performance Guaranteed Deep Learning for Detection of Cyber-Attacks in Dynamic Smart Grids. IEEE Transactions on Power Systems.
20. Kapil, D., Mehra, N., Gupta, A., Maurya, S., & Sharma, A. (2021, March). Network security: threat model, attacks, and IDS using machine learning. In 2021 international conference on artificial intelligence and smart systems (ICAIS) (pp. 203-208). IEEE.
21. Kavishwar, S (2024). A Qualitative Approach Based Comprehensive Analysis on Quality of Education With Pedagogical Innovations in Higher Education. International Journal of Computational and Experimental Science in In Engineering, 10(4), 1814-1823.
22. Joshi, M., Kothari, P. and Kavishwar, S. (2024). A Study on Determinants of Profitability in Indian Banks. Journal of Informatics Education and Research. 4(3), 22-26.
23. Kavishwar, S. (2024). A Theoretical Framework Analyzing Impact of Embedding Entrepreneurial Skills in Education on Economical Growth. Journal of Lifestyle and SDGs Review, 4(4), e03550.
24. Nirmal Kumar Jingar. (2021). Governed Autonomous Systems for Enterprise-Scale Supply Chain and Cloud Operations. In International Journal of Science, Engineering and Technology (Vol. 9, Number 6). Zenodo. https://doi.org/10.5281/zenodo.18629297
25. Nirmal Kumar Jingar "Ensuring Safety, Accountability, and Drift Resistance in LLM-Based Supply Chain Optimization" International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 10, Issue 1, pp.472-482, January-February-2023. Available at doi : https://doi.org/10.32628/IJSRSET2310372
26. Nijim, M., Kanumuri, V., Alaqqad, W., Albataineh, H. (2023). Advanced Traffic Management System for Smart Cities. In: Daimi, K., Al Sadoon, A. (eds) Proceedings of the 2023 International Conference on Advances in Computing Research (ACR'23). ACR 2023. Lecture Notes in Networks and Systems, vol 700. Springer, Cham. https://doi.org/10.1007/978-3-031-33743-7_19
27. Nijim, M., Kanumuri, V., Al Aqqad, W., Albataineh, H. (2024). Machine Learning Based Analysis of Cyber-Attacks Targeting Smart Grid Infrastructure. In: Daimi, K., Al Sadoon, A. (eds) Proceedings of the Second International Conference on Advances in Computing Research (ACR'24). ACR 2024. Lecture Notes in Networks and Systems, vol 956. Springer, Cham. https://doi.org/10.1007/978-3-031-56950-0_28
28. Racha, Ganesh. "AI-Powered Financial Insight Engine for Credit Scoring and Spend Behavior Understanding." International Journal of Scientific Research & Engineering Trends, vol. 10, no. 2, Mar.–Apr. 2024, pp. 1–8.
29. Racha, Ganesh. "Adaptive Quantum Blockchain for Secure IoT Resource Coordination." International Journal of Science, Engineering and Technology, vol. 11, no. 3, 2023.
30. Veginati, Navya. "Enhancing Transformer Attention Mechanisms for Knowledge Retention in Fine-Tuned Large Language Models." International Journal of Scientific Research in Science and Technology, vol. 11, no. 5, Sept.–Oct. 2024, pp. 864–871. DOI: https://doi.org/10.32628/IJSRST52310284
31. Veginati, Navya. "Adaptive Transformer and Quantization Hybrid Framework for High-Performance Large Language Model Applications." United International Journal of Engineering and Sciences, vol. 5, no. 4, Dec. 2025, pp. 46–56
32. Jonnalagadda, Pawan Kalyan. "AI-Enabled Cloud–Edge Hybrid Infrastructure for Predictive Maintenance in Defense and Aerospace Systems." International Journal of Science, Engineering and Technology, vol. 12, no. 2, 2024.
33. Jonnalagadda, Pawan Kalyan. "Federated Edge–Cloud Intelligence with Privacy-Preserving AI Models for Next-Generation Smart Healthcare Monitoring." United International Journal of

Engineering and Sciences (UIJES), vol. 5, no. 4, Dec. 2025, pp. 46–57.
34. A. Mahida, "An Intellectual Zero Trust Security Framework Using Deep Reinforcement Learning for Predictive Threat Mitigation in AI-Based Fraud Detection Systems," in IEEE Access, vol. 14, pp. 24602-24617, 2026, doi: 10.1109/ACCESS.2026.3664389.
35. A. Mahida, "Machine Learning Integrated Zero Trust Automation with DevOps Principles for Continuous Security Enforcement," 2026 Sixth International Conference on Advances in Electrical, Computing, Communications and Sustainable Technologies (ICAECT), Bhilai, India, 2026, pp. 1-7, doi: 10.1109/ICAECT68478.2026.11426026.
36. Tummuri, S. S. R. (2022). Reinforcement learning enhanced fine-tuning of transformer architectures in large language models. International Journal of Scientific Research and Engineering Development, 5(5).
37. S. S. R. Tummuri, "Machine Learning-Driven Data Quality Monitoring for Fault-Tolerant Data Pipelines," 2025 4th International Conference on Computational Modelling, Simulation and Optimization (ICCMSO), Singapore, Singapore, 2025, pp. 154-159, doi: 10.1109/ICCMSO67468.2025.00036.
38. B. K. Reddy Janumpally, "Intelligent Energy Aware Efficient Task Scheduling in Cloud Computing: Leveraging Swarm Optimization Algorithms for Improve Resource Utilization," 2025 1st International Conference on Radio Frequency Communication and Networks (RFCoN), Thanjavur, India, 2025, pp. 1-6, doi: 10.1109/RFCoN62306.2025.11085278.
39. Janumpally, Bharath Kumar Reddy. (2026). Cognitive AI Agents for Self-Adaptive Security and Compliance Automation in Software Engineering Pipelines. 10.1109/ICAUC68182.2026.11441048.
40. Yachamaneni T, Kotadiya U, Arora AS. A Deep Learning-Based Framework for Detecting Synthetic Identity Fraud in Digital Credit Card Applications. IJERET [Internet]. 2023 Dec. 30 [cited 2026 Apr. 5];4(4):43-52.
41. Arora AS, Yachamaneni T, Kotadiya U. Architectural Optimization of Serverless Big Data Pipelines for AI Workloads Using Cloud Functions and Managed Spark on GCP. IJETCSIT [Internet]. 2024 Mar. 30 [cited 2026 Apr. 5];5(1):61-8.