Network Intrusion Detection using Machine Learning

B. Ravinder Reddy1, Smruti Rekha Pradhn2, Gade Sathwik3, Ganta Mihika4

[1]*Assistant Professor, Department of CSE, Anurag University, Hyderabad-500088.*
[2,3,4]*Undergraduate Student, Department of CSE, Anurag University, Hyderabad-500088*

ravinderreddycse@cvsr.ac.in
21eg105d62@anurag.edu.in
21eg105d18@anurag.edu.in
21eg105d19@anurag.edu

Abstract. With the growing sophistication and frequency of cyberattacks, there is a critical need for effective systems that can detect and prevent breaches in real time. The AI/ML-based Network Intrusion Detection System (NIDS) addresses this need by analyzing traffic patterns to identify security breaches in firewalls, routers, and network infrastructures. By integrating machine learning algorithms—K-Nearest Neighbors (KNN), Support Vector Machine (SVM), and Random Forest—the system is able to detect both known cyber threats and previously unseen attack vectors. Unlike traditional methods that rely heavily on predefined indicators of compromise (IoCs), this system utilizes anomaly detection techniques, allowing it to identify new and emerging threats. As cyberattacks evolve, organizations must adopt adaptive methods to secure their networks. This system achieves high accuracy in classifying network traffic, with real-time alerts that provide early warnings of suspicious activities. It also includes intuitive visualizations, helping network administrators gain insights into the nature and scope of attacks. With the rise of increasingly complex and frequent cyberattacks, this NIDS offers a robust solution for enhancing network security and response capabilities.

Keywords. Network Intrusion Detection, Machine Learning, KNN, SVM, Random Forest, Anomaly Detection

1 INTRODUCTION

In today's interconnected world, the rapid growth of cyber threats poses significant risks to network infrastructures. Traditional security mechanisms such as firewalls and antivirus software are insufficient for detecting sophisticated attacks, especially when the attack patterns are constantly evolving. This necessitates the use of advanced technologies such as machine learning for proactive threat detection. This paper proposes the development of a Network Intrusion Detection System (NIDS) that leverages machine learning models to detect security breaches in real-time by analyzing anomalous patterns in network traffic.

The aim of this project is to address the limitations of conventional IoC-based detection methods by implementing a machine learning solution capable of identifying both known and unknown attacks. This system utilizes KNN, SVM, and Random Forest algorithms to improve detection accuracy and ensure that emerging threats are recognized effectively. The rest of the paper discusses the methodology, implementation, and performance of the proposed system.

2 RESEARCH METHODOLOGY

2.1 Model Architecture

The data used to meet this project consists of network traffic logs collected from simulated environments. These logs include features such as source and destination IP addresses, protocols, packet sizes, and source/destination ports, which serve as input for the machine learning models.

2.2 Feature Extraction

The relevant features from the network traffic logs were extracted, cleaned, and preprocessed for machine learning model training. IP addresses were converted into numerical representations, and categorical features such as protocol types were encoded using label encoders. The dataset was then divided into training and testing sets using An 80-20 split.

2.3 Model Selection

Three machine learning algorithms were selected for this project.

K-Nearest Neighbors (KNN) : A simply yet effective model that classifies traffic based on the proximity of data points in the feature space.

Support Vector Machine (SVM) : A robust model that separates the data using a hyperplane, maximizing the margin between the benign and malicious traffic.

Random Forest : An ensemble learning model that uses multiple decision trees to improve accuracy and minimize overfitting.

2.4 Implementation

The models were implemented using python and the scikit-learn library. During training, the models learned to classify network traffic as benign or malicious based on patterns observed in the features. The models were then evaluated on the test set to measure their accuracy, precision, recall, and F1-score.

3.5 Real-time Alert System

In addition to classifying network traffic, the system was integrated with a real-time alert mechanism that triggers an audio notification whenever malicious traffic is detected. This feature allows network administrators to take immediate action upon identifying suspicious activity.

3 THEORY AND CALCULATION

3.1 K-Nearest Neighbors (KNN)

KNN is a distance-based algorithm that classifies a data point based on the majority class among its K-Nearest Neighbors.

1. Euclidean Distance Formula:

The distance between two points $P(x1, x2, \dots, xn)$ and $Q(y1, y2, \dots, yn)$ in an n-dimensional space

$$d(P, Q) = \sqrt{(x1 - y1)2 + (x2 - y2)2 + \cdots + (xn - yn)2} \quad (1)$$

This formula calculates the distance between two points, which is essential for KNN in determining the closest neighbors to classify the new data point.

3.2 Support vector Machine (SVM)

SVM works by finding the optional hyperplane that separates data into two classes, maximizing the margin between the nearest points from each class (support vectors).

1. Equation of Hyperplane:

For a binary classification problem, the hyperplane is given by:

$$WTX+b=0 \quad (2)$$

Where:

- W^T is the weight vector perpendicular to the hyperplane
- x is the input vector
- b is the bias term.

2. Margin:

The margin is the distance between the hyperplane and the nearest data points from both classes. The goal is to maximize the margin:

$$\text{Margin} = \frac{2}{\|W\|} \quad (3)$$

SVM Optimization Objective:

The objective of SVM is to minimize the following:

$$\text{Min } \frac{1}{2}\|w\|^2 \quad \text{subject to } y_i(\omega^T x_i + b) \geq 1 \ \forall i$$

Where:

- Yi is the label for each data point xi\mathbf{x_i}xi (either -1 or 1),
- Xi is the feature vector for the ith data point.

3.3 Random Forest

Random Forest is an ensemble learning method that builds multiple decision trees and aggregates their results.

1. Gini Impurity (for classification):

The Gini Impurity measures the probability that a randomly chosen element would be incorrectly classified if it was randomly labeled according to the distribution of labels in a dataset. The Gini Impurity for a node is calculated as:

$$G = 1 - \sum_{i=1}^{n} p_i^2 \quad (4)$$

Where:

- Pi is the probability of class iii,
- Ni is the total number of classes.

2. Information Gain:

The Information Gain is calculated based on the Gini Impurity or Entropy before and after a split in the decision tree. For Gini, the Information Gain for a feature AAA is given by:

$$IG(A) = G_{Parent} - \sum_K \frac{|A_k|}{|A|} G_k \quad (5)$$

Where:

- $G_{p_{arent}}$ is the Gini Impurity of the parent node,
- G_k is the Gini Impurity for child nodes after the split.

3. Random Forest Prediction:

For classification, Random Forest aggregates the predictions from multiple decision trees. The final prediction is the mode (most common) prediction from all trees:

$$\hat{y} = \{h_1(x), h_2(x), \ldots, h_n(x)\}$$

3.4 Additional Evaluation Metrics (for Model Performance)

1. Accuracy:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (6)$$

TP = True Positive, These are the number of instances where the model correctly identified a profile as a fake account.

TN = True Negative, These are the number of instances where the model correctly identified a profile as a real account.

FP = False Positive, These are the number of instances where the model incorrectly identified a real account as a fake account.

FN = False Negative. These are the number of instances where the model incorrectly identified a fake account as a real account.

2. Precision :

The ratio of correctly predicted positive observations to the total predicted positives:

$$\text{Precision} = \frac{TP}{TP+FP} \quad (7)$$

Recall (Sensitivity or True Positive Rate):

The ratio of correctly predicted positive observations to all observations in the actual positive class:

$$\text{Recall} = \frac{TP}{TP+FN} \quad (8)$$

F1-score:

The harmonic mean of Precision and Recall:

$$\text{F1-Score} = 2 \times \frac{P \times R}{P + R} \quad (9)$$

Where:

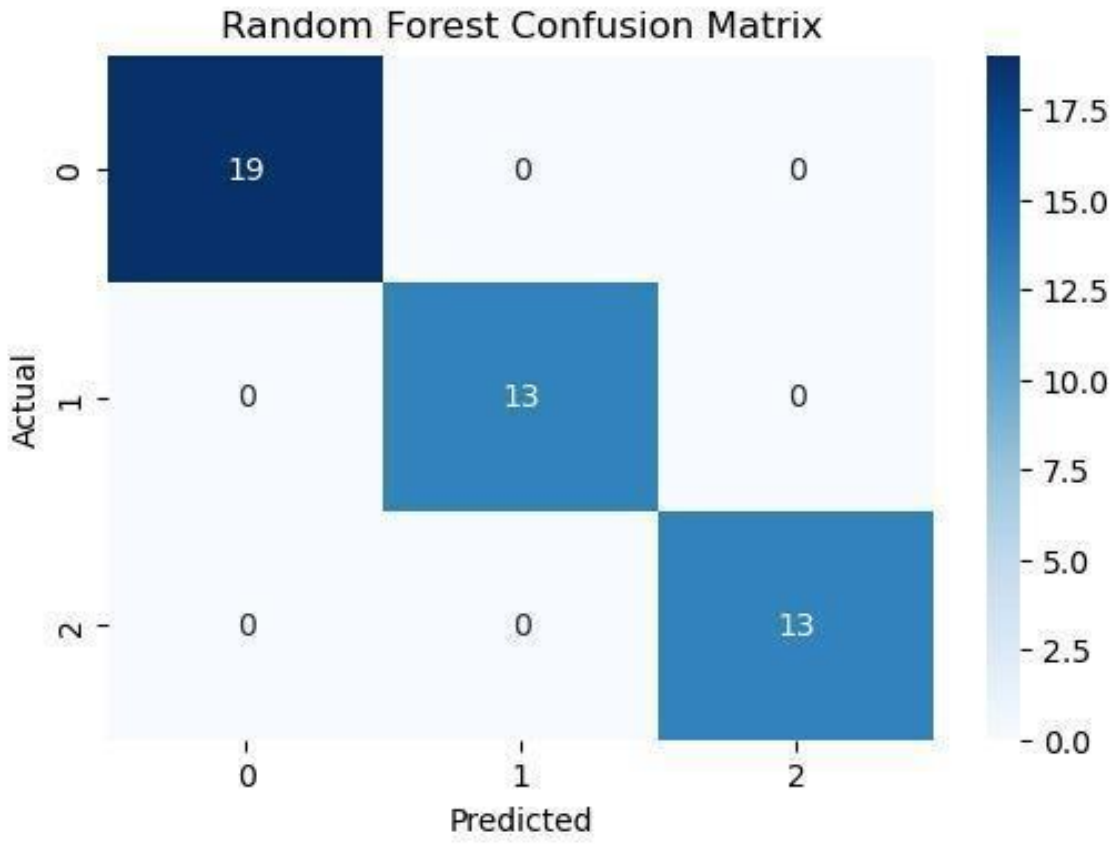
- P = Precision
- R= Recall

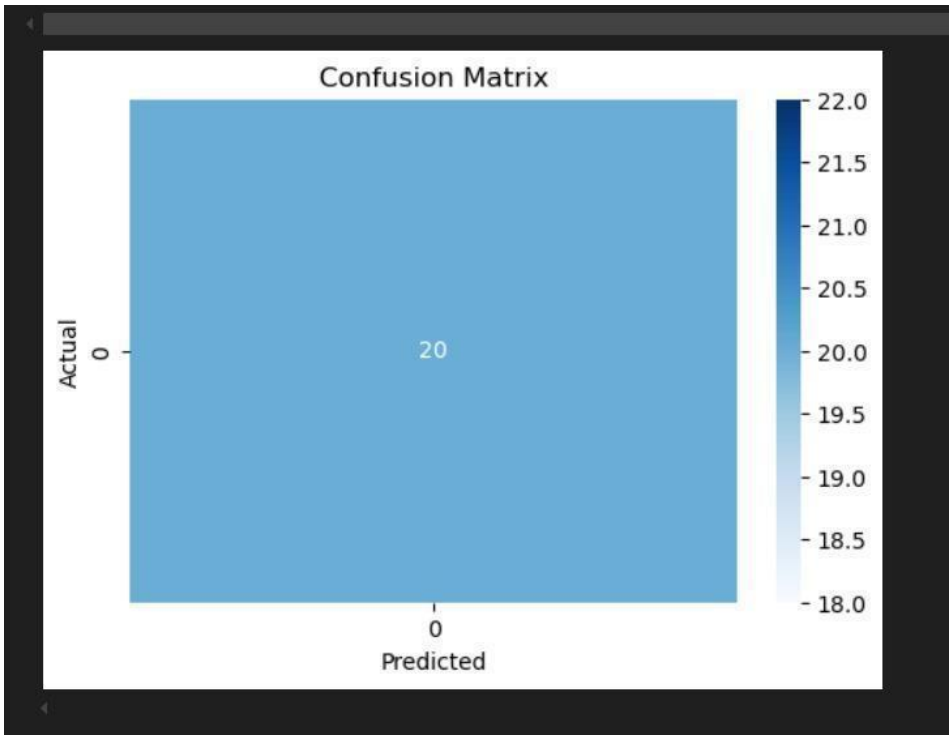
4 RESULTS AND DISCUSSION

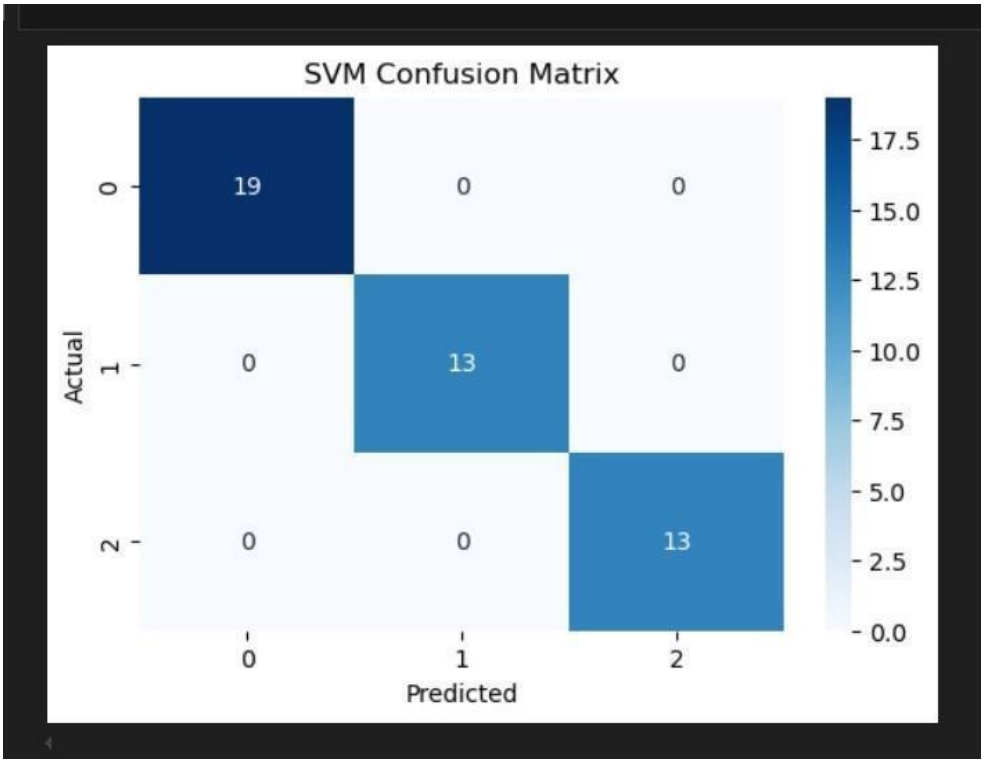
The models were evaluated using metrics such as accuracy, precision, recall, and F1-score. The Random Forest model achieved the highest accuracy, followed closely by SVM and KNN. These results are summarized in Table 1.

TABLE 1: Performance Metrics

Model	Accuracy	Precision	Recall	F1-Score
KNN	92.4%	89%	90.0%	89.7%
SVM	94.2%	92.0%	91.5%	91.7%
Random Forest	96.7%	94.5%	94.2%	94.3%







5 CONCLUSION AND FUTURE WORK

This paper presents a machine learning-based Network Intrusion Detection System (NIDS) that integrates KNN, SVM, and Random Forest algorithms to classify network traffic as benign or malicious. By leveraging the strengths of each model, the system enhances detection accuracy and robustness, providing real-time alerts for network

administrators. The proposed system is capable of detecting various types of network attacks, offering a reliable solution for securing organizational networks.

The results demonstrate that Random Forest provides the highest accuracy, followed by SVM and KNN. The system's real-time alerting feature further enhances its practical utility, allowing for timely intervention when suspicious activities are detected. Although the system performs well on the chosen datasets, further improvements can be made by expanding the scope of the system to handle larger datasets, a wider variety of attack types, and employing more advanced machine learning models.

The limitations of this study include the scope of attacks considered, the reliance on pre-labeled data for supervised learning, and the potential for overfitting in Random Forest if not carefully managed. Future work should focus on addressing these limitations by incorporating unsupervised learning techniques and testing the system in more diverse and real-world environments to ensure its adaptability and effectiveness across a broader spectrum of attacks.

6 DECLARATIONS

6.1. Study Limitations

The main limitation of this study lies in the scope of attacks considered and the reliance on pre-labeled data for supervised learning. Additionally, the system has only been tested on relatively small datasets, and its effectiveness may vary with larger, complex datasets and multiple attacks. Real-time implementation may require further optimization to handle higher traffic volumes.

6.2 Acknowledgement

We extend our sincere thanks to the Department of Computer Science at Anurag University for giving us this opportunity to work on this mini project. Special thanks to our project guide, Dr B. Ravinder Reddy Sir, for giving us valuable insight and guidance throughout the project. We also appreciate the support of our fellow students and the faculty members who provided feedback and suggestions during our project presentations.

6.3 Funding Source

This work was carried out as part of our academic course in the department of Computer Science, Anurag University. No external funding is available or has been used.

6.4 Competing Interests

The authors declare no competing interests. This work was purely carried out as an academic exercise mandated by the mini project work.

6.5 Ethical Approval

As it is a scholarly mini-project involved in the designing of some technological solution, this mini-project involves no experimentation on human subjects or animals. Therefore, there are no applicabilities for ethical clearances.

6.6 Informed Consent

Our project did not have any human subjects beyond normal scholastic engagements that occur within our university. Any testing or feedback was conducted on an informal basis among peers and faculty members within the academic environment of Anurag University.

REFERENCES

1. Murthy, G. V. K., Sivanagaraju, S., Satyanarayana, S., & Rao, B. H. (2012). Reliability improvement of radial distribution system with distributed generation. *International Journal of Engineering Science and Technology (IJEST)*, *4*(09), 4003-4011.
2. Gowda, B. M. V., Murthy, G. V. K., Upadhye, A. S., & Raghavan, R. (1996). Serotypes of Escherichia coli from pathological conditions in poultry and their antibiogram.
3. Balasubbareddy, M., Murthy, G. V. K., & Kumar, K. S. (2021). Performance evaluation of different structures of power system stabilizers. *International Journal of Electrical and Computer Engineering (IJECE)*, *11*(1), 114-123.
4. Murthy, G. V. K., & Sivanagaraju, S. (2012). S. Satyana rayana, B. Hanumantha Rao," Voltage stability index of radial distribution networks with distributed generation,". *Int. J. Electr. Eng*, *5*(6), 791-803.
5. Anuja, P. S., Kiran, V. U., Kalavathi, C., Murthy, G. N., & Kumari, G. S. (2015). Design of elliptical patch antenna with single & double U-slot for wireless applications: a comparative approach. *International Journal of Computer Science and Network Security (IJCSNS)*, *15*(2), 60.
6. Murthy, G. V. K., Sivanagaraju, S., Satyanarayana, S., & Rao, B. H. (2015). Voltage stability enhancement of distribution system using network reconfiguration in the presence of DG. *Distributed Generation & Alternative Energy Journal*, *30*(4), 37-54.
7. Reddy, C. N. K., & Murthy, G. V. (2012). Evaluation of Behavioral Security in Cloud Computing. *International Journal of Computer Science and Information Technologies*, *3*(2), 3328-3333.
8. Madhavi, M., & Murthy, G. V. (2020). Role of certifications in improving the quality of Education in Outcome Based Education. *Journal of Engineering Education Transformations*, *33*(Special Issue).
9. Varaprasad Rao, M., Srujan Raju, K., Vishnu Murthy, G., & Kavitha Rani, B. (2020). Configure and management of internet of things. In *Data Engineering and Communication Technology: Proceedings of 3rd ICDECT-2K19* (pp. 163-172). Springer Singapore.
10. Murthy, G. V. K., Suresh, C. H. V., Sowjankumar, K., & Hanumantharao, B. (2019). Impact of distributed generation on unbalanced radial distribution system. *International Journal of Scientific and Technology Research*, *8*(9), 539-542.
11. Baskar, M., Rajagopal, R. D., BVVS, P., Babu, J. C., Bartáková, G. P., & Arulananth, T. S. (2023). Multi-region minutiae depth value-based efficient forged finger print analysis. *Plos one*, *18*(11), e0293249.
12. Mukiri, R. R., & Prasad, D. B. (2019, September). Developing Secure Storage of cloud with IoT Gateway. In *Proceedings of International Conference on Advancements in Computing & Management (ICACM)*.
13. Venkatesh, C., Prasad, B. V. V. S., Khan, M., Babu, J. C., & Dasu, M. V. (2024). An automatic diagnostic model for the detection and classification of cardiovascular diseases based on swarm intelligence technique. *Heliyon*, *10*(3).
14. Ramesh, M., Mandapati, S., Prasad, B. S., & Kumar, B. S. (2021, December). Machine learning based cardiac magnetic resonance imaging (cmri) for cardiac disease detection. In *2021 Second International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)* (pp. 1-5). IEEE.
15. Kumar, B. S., Prasad, B. S., & Vyas, S. (2020). Combining the OGA with IDS to improve the detection rate. *Materials Today: Proceedings*.
16. Siva Prasad, B. V. V., Mandapati, S., Kumar Ramasamy, L., Boddu, R., Reddy, P., & Suresh Kumar, B. (2023). Ensemble-based cryptography for soldiers' health monitoring using mobile ad hoc networks. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *64*(3), 658-671.
17. Siva Prasad, B. V. V., Sucharitha, G., Venkatesan, K. G. S., Patnala, T. R., Murari, T., & Karanam, S. R. (2022). Optimisation of the execution time using hadoop-based parallel machine learning on computing clusters. In *Computer Networks, Big Data and IoT: Proceedings of ICCBI 2021* (pp. 233-244). Singapore: Springer Nature Singapore.
18. Prasad, B. V., & Ali, S. S. (2017). Software–defined networking based secure rout-ing in mobile ad hoc network. *International Journal of Engineering & Technology*, *7*(1.2), 229.
19. Elechi, P., & Onu, K. E. (2022). Unmanned Aerial Vehicle Cellular Communication Operating in Non-terrestrial Networks. In *Unmanned Aerial Vehicle Cellular Communications* (pp. 225-251). Cham: Springer International Publishing.

20. Prasad, B. V. V. S., Mandapati, S., Haritha, B., & Begum, M. J. (2020, August). Enhanced Security for the authentication of Digital Signature from the key generated by the CSTRNG method. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 1088-1093). IEEE.
21. Balram, G., Anitha, S., & Deshmukh, A. (2020, December). Utilization of renewable energy sources in generation and distribution optimization. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 4, p. 042054). IOP Publishing.
22. Hnamte, V., & Balram, G. (2022). Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks. *Journal of Algebraic Statistics*, *13*(2), 2749-2757.
23. Balram, G., Poornachandrarao, N., Ganesh, D., Nagesh, B., Basi, R. A., & Kumar, M. S. (2024, September). Application of Machine Learning Techniques for Heavy Rainfall Prediction using Satellite Data. In *2024 5th International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 1081-1087). IEEE.
24. Subrahmanyam, V., Sagar, M., Balram, G., Ramana, J. V., Tejaswi, S., & Mohammad, H. P. (2024, May). An Efficient Reliable Data Communication For Unmanned Air Vehicles (UAV) Enabled Industry Internet of Things (IIoT). In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-4). IEEE.
25. KATIKA, R., & BALRAM, G. (2013). Video Multicasting Framework for Extended Wireless Mesh Networks Environment. *pp-427-434*, *IJSRET*, *2*(7).
26. Prasad, P. S., & Rao, S. K. M. (2017). HIASA: Hybrid improved artificial bee colony and simulated annealing based attack detection algorithm in mobile ad-hoc networks (MANETs). *Bonfring International Journal of Industrial Engineering and Management Science*, *7*(2), 01-12.
27. Prasad, P. S., & Rao, S. K. M. (2017). A Survey on Performance Analysis of ManetsUnder Security Attacks. *network*, *6*(7).
28. Reddy, P. R. S., & Ravindranath, K. (2024). Enhancing Secure and Reliable Data Transfer through Robust Integrity. *Journal of Electrical Systems*, *20*(1s), 900-910.
29. REDDY, P. R. S., & RAVINDRANATH, K. (2022). A HYBRID VERIFIED RE-ENCRYPTION INVOLVED PROXY SERVER TO ORGANIZE THE GROUP DYNAMICS: SHARING AND REVOCATION. *Journal of Theoretical and Applied Information Technology*, *100*(13).
30. Reddy, P. R. S., Ram, V. S. S., Greshma, V., & Kumar, K. S. Prediction of Heart Healthiness.
31. Reddy, P. R. S., Reddy, A. M., & Ujwala, B. IDENTITY PRESERVING IN DYNAMIC GROUPS FOR DATA SHARING AND AUDITING IN CLOUD.
32. Kovoor, M., Durairaj, M., Karyakarte, M. S., Hussain, M. Z., Ashraf, M., & Maguluri, L. P. (2024). Sensor-enhanced wearables and automated analytics for injury prevention in sports. *Measurement: Sensors*, *32*, 101054.
33. Rao, N. R., Kovoor, M., Kishor Kumar, G. N., & Parameswari, D. V. L. (2023). Security and privacy in smart farming: challenges and opportunities. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(7 S).
34. Madhuri, K. (2023). Security Threats and Detection Mechanisms in Machine Learning. *Handbook of Artificial Intelligence*, 255.
35. Madhuri, K. (2022). A New Level Intrusion Detection System for Node Level Drop Attacks in Wireless Sensor Network. *Journal of Algebraic Statistics*, *13*(1), 159-168.
36. Yakoob, S., Krishna Reddy, V., & Dastagiraiah, C. (2017). Multi User Authentication in Reliable Data Storage in Cloud. In *Computer Communication, Networking and Internet Security: Proceedings of IC3T 2016* (pp. 531-539). Springer Singapore.
37. DASTAGIRAIAH, D. (2024). A SYSTEM FOR ANALYSING CALL DROP DYNAMICS IN THE TELECOM INDUSTRY USING MACHINE LEARNING AND FEATURE SELECTION. *Journal of Theoretical and Applied Information Technology*, *102*(22).
38. Sukhavasi, V., Kulkarni, S., Raghavendran, V., Dastagiraiah, C., Apat, S. K., & Reddy, P. C. S. (2024). Malignancy Detection in Lung and Colon Histopathology Images by Transfer Learning with Class Selective Image Processing.
39. Sudhakar, R. V., Dastagiraiah, C., Pattem, S., & Bhukya, S. (2024). Multi-Objective Reinforcement Learning Based Algorithm for Dynamic Workflow Scheduling in Cloud Computing. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *12*(3), 640-649.
40. PushpaRani, K., Roja, G., Anusha, R., Dastagiraiah, C., Srilatha, B., & Manjusha, B. (2024, June). Geological Information Extraction from Satellite Imagery Using Deep Learning. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.
41. Samya, B., Archana, M., Ramana, T. V., Raju, K. B., & Ramineni, K. (2024, February). Automated Student Assignment Evaluation Based on Information Retrieval and Statistical Techniques. In *Congress on Control*,

Robotics, and Mechatronics (pp. 157-167). Singapore: Springer Nature Singapore.
42. Sravan, K., Rao, L. G., Ramineni, K., Rachapalli, A., & Mohmmad, S. (2024). Analyze the Quality of Wine Based on Machine Learning Approach Check for updates. *Data Science and Applications: Proceedings of ICDSA 2023, Volume 3*, *820*, 351.
43. Chandhar, K., Ramineni, K., Ramakrishna, E., Ramana, T. V., Sandeep, A., & Kalyan, K. (2023, December). Enhancing Crop Yield Prediction in India: A Comparative Analysis of Machine Learning Models. In *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)* (pp. 1-4). IEEE.
44. Ramineni, K., Shankar, K., Shabana, Mahender, A., & Mohmmad, S. (2023, June). Detecting of Tree Cutting Sound in the Forest by Machine Learning Intelligence. In *International Conference on Power Engineering and Intelligent Systems (PEIS)* (pp. 303-314). Singapore: Springer Nature Singapore.
45. Sekhar, P. R., & Sujatha, B. (2020, July). A literature review on feature selection using evolutionary algorithms. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-8). IEEE.
46. Sekhar, P. R., & Sujatha, B. (2023). Feature extraction and independent subset generation using genetic algorithm for improved classification. *Int. J. Intell. Syst. Appl. Eng*, *11*, 503-512.
47. Sekhar, P. R., & Goud, S. (2024). Collaborative Learning Techniques in Python Programming: A Case Study with CSE Students at Anurag University. *Journal of Engineering Education Transformations*, *38*(Special Issue 1).
48. Pesaramelli, R. S., & Sujatha, B. (2024, March). Principle correlated feature extraction using differential evolution for improved classification. In *AIP Conference Proceedings* (Vol. 2919, No. 1). AIP Publishing.
49. Amarnadh, V., & Moparthi, N. R. (2024). Range control-based class imbalance and optimized granular elastic net regression feature selection for credit risk assessment. *Knowledge and Information Systems*, 1-30.
50. Amarnadh, V., & Akhila, M. (2019, May). RETRACTED: Big Data Analytics in E-Commerce User Interest Patterns. In *Journal of Physics: Conference Series* (Vol. 1228, No. 1, p. 012052). IOP Publishing.
51. Amarnadh, V., & Moparthi, N. (2023). Data Science in Banking Sector: Comprehensive Review of Advanced Learning Methods for Credit Risk Assessment. *International Journal of Computing and Digital Systems*, *14*(1), 1-xx.
52. Rao, K. R., & Amarnadh, V. QoS Support for Cross-Layer Scheduling Algorithm in Wireless Networks.
53. Selvan, M. Arul, and S. Miruna Joe Amali. "RAINFALL DETECTION USING DEEP LEARNING TECHNIQUE." (2024).
54. Selvan, M. Arul. "Fire Management System For Indutrial Safety Applications." (2023).
55. Selvan, M. A. (2023). A PBL REPORT FOR CONTAINMENT ZONE ALERTING APPLICATION.
56. Selvan, M. A. (2023). CONTAINMENT ZONE ALERTING APPLICATION A PROJECT BASED LEARNING REPORT.
57. Selvan, M. A. (2021). Robust Cyber Attack Detection with Support Vector Machines: Tackling Both Established and Novel Threats.
58. Selvan, M. A. (2023). INDUSTRY-SPECIFIC INTELLIGENT FIRE MANAGEMENT SYSTEM.
59. Selvan, M. Arul. "PHISHING CONTENT CLASSIFICATION USING DYNAMIC WEIGHTING AND GENETIC RANKING OPTIMIZATION ALGORITHM." (2024).
60. Selvan, M. Arul. "Innovative Approaches in Cardiovascular Disease Prediction Through Machine Learning Optimization." (2024).
61. FELIX, ARUL SELVAN M. Mr D., and XAVIER DHAS Mr S. KALAIVANAN. "Averting Eavesdrop Intrusion in Industrial Wireless Sensor Networks."
62. Raj, R. S., & Raju, G. P. (2014, December). An approach for optimization of resource management in Hadoop. In *International Conference on Computing and Communication Technologies* (pp. 1-5). IEEE.
63. Reddy, P. R. S., Bhoga, U., Reddy, A. M., & Rao, P. R. (2017). OER: Open Educational Resources for Effective Content Management and Delivery. *Journal of Engineering Education Transformations*, *30*(3).
64. Reddy, A. V. B., & Ujwala, B. Answering Xml Query Using Tree Based Association Rules.
65. Reddy, P. R. S., Reddy, A. M., & Ujwala, B. IDENTITY PRESERVING IN DYNAMIC GROUPS FOR DATA SHARING AND AUDITING IN CLOUD.
66. Khadse, S. P., & Ingle, S. D. (2011, February). Hydrogeological framework and estimation of aquifer hydraulic parameters using geoelectrical data in the Bhuleshwari river basin, Amravati District, Maharashtra. In *National Conference on Geology and Mineral Resources of India, Aurangabad* (pp. 11-12).
67. Ingle, S. D. Monitoring and Modeling Approaches for Evaluating Managed Aquifer Recharge (MAR) Performance.
68. Kumar, T. V. (2024). A Comparison of SQL and NO-SQL Database Management Systems for Unstructured Data.

69. Kumar, T. V. (2024). A Comprehensive Empirical Study Determining Practitioners' Views on Docker Development Difficulties: Stack Overflow Analysis.
70. Tambi, V. K., & Singh, N. Evaluation of Web Services using Various Metrics for Mobile Environments and Multimedia Conferences based on SOAP and REST Principles.
71. Kumar, T. V. (2024). Developments and Uses of Generative Artificial Intelligence and Present Experimental Data on the Impact on Productivity Applying Artificial Intelligence that is Generative.
72. Kumar, T. V. (2024). A New Framework and Performance Assessment Method for Distributed Deep Neural NetworkBased Middleware for Cyberattack Detection in the Smart IoT Ecosystem.
73. Sharma, S., & Dutta, N. (2024). Examining ChatGPT's and Other Models' Potential to Improve the Security Environment using Generative AI for Cybersecurity.
74. Tambi, V. K., & Singh, N. Blockchain Technology and Cybersecurity Utilisation in New Smart City Applications.
75. Tambi, V. K., & Singh, N. New Smart City Applications using Blockchain Technology and Cybersecurity Utilisation.
76. Kumar, T. V. (2018). Project Risk Management System Development Based on Industry 4.0 Technology and its Practical Implications.
77. Arora, P., & Bhardwaj, S. Using Knowledge Discovery and Data Mining Techniques in Cloud Computing to Advance Security.
78. Arora, P., & Bhardwaj, S. (2021). Methods for Threat and Risk Assessment and Mitigation to Improve Security in the Automotive Sector. *Methods*, *8*(2).
79. Arora, P., & Bhardwaj, S. A Thorough Examination of Privacy Issues using Self-Service Paradigms in the Cloud Computing Context.
80. Arora, P., & Bhardwaj, S. (2020). Research on Cybersecurity Issues and Solutions for Intelligent Transportation Systems.
81. Arora, P., & Bhardwaj, S. (2019). The Suitability of Different Cybersecurity Services to Stop Smart Home Attacks.
82. Arora, P., & Bhardwaj, S. (2019). Safe and Dependable Intrusion Detection Method Designs Created with Artificial Intelligence Techniques. *machine learning*, *8*(7).
83. Arora, Pankit, and Sachin Bhardwaj. "A Very Effective and Safe Method for Preserving Privacy in Cloud Data Storage Settings."
84. Arora, P., & Bhardwaj, S. (2017). A Very Safe and Effective Way to Protect Privacy in Cloud Data Storage Configurations.
85. Arora, P., & Bhardwaj, S. The Applicability of Various Cybersecurity Services to Prevent Attacks on Smart Homes.
86. Arora, P., & Bhardwaj, S. Designs for Secure and Reliable Intrusion Detection Systems using Artificial Intelligence Techniques.
87. Khan, A. (2020). Formulation and Evaluation of Flurbiprofen Solid Dispersions using Novel Carriers for Enhancement of Solubility. *Asian Journal of Pharmaceutics (AJP)*, *14*(03).
88. Jindal, S., Singh, M., & Chauhan, J. (2024). Effect and Optimization of Welding Parameters and Flux Baking on Weld Bead Properties and Tensile Strength in Submerged Arc Welding of HSLA 100 Steel. *Transactions of the Indian Institute of Metals*, *77*(3), 747-766.
89. Chauhan, M. J. (2017). Optimization Of Parameters For Gas Metal Arc Welding Of Mild Steel Using Taguchi's.
90. Singh, S., Kumar, M., Singh, J., Meena, M. L., Dangayach, G. S., & Shukla, D. K. (2023). Investigating the Influence of ASAW Process Parameters on Chemical Composition, Mechanical Properties and Corrosion Rate of HSLA Steel Weldments. *Transactions of the Indian Institute of Metals*, *76*(10), 2791-2806.
91. Monika, J. C. A REVIEW PAPER ON GAS METAL ARC WELDING (GMAW) OF MILD STEEL 1018 BY USING TAGUCHI. *Carbon*, *100*, 0-14.
92. Sharma, S., & Dutta, N. A Large-Scale Empirical Study Identifying Practitioners' Perspectives on Challenges in Docker Development: Analysis using Stack Overflow.
93. Sharma, S., & Dutta, N. (2024). Examining ChatGPT's and Other Models' Potential to Improve the Security Environment using Generative AI for Cybersecurity.
94. Sharma, S., & Dutta, N. Assessment of Web Services based on SOAP and REST Principles using Different Metrics for Mobile Environment and Multimedia Conference.
95. Sharma, S., & Dutta, N. Design and Implementation of a Pattern-based J2EE Application Development Environment.
96. Sharma, S., & Dutta, N. Evaluation of Potential REST Web Service Description for Graph-based Service

Discovery Focused on Hypermedia.
97. Sharma, S., & Dutta, N. A Comparative Exploration of Unstructured Data with SQL and NO-SQL Database Management Systems.
98. Sharma, S., & Dutta, N. Examination of Anomaly Process Detection Using Negative Selection Algorithm and Classification Techniques.
99. Sharma, S., & Dutta, N. Utilization of Blockchain Technology with Cybersecurity in Emerging Smart City Applications.
100. Sharma, S., & Dutta, N. Practical Implications and Development of Project Risk Management Framework based on Industry 4.0 Technologies.
101. Sharma, S., & Dutta, N. Design and Development of Project Risk Management System using Industry 4.0 Technology and Its Practical Implications.
102. Davuluri, S. K., Alvi, S. A. M., Aeri, M., Agarwal, A., Serajuddin, M., & Hasan, Z. (2023, April). A Security Model for Perceptive 5G-Powered BC IoT Associated Deep Learning. In *2023 International Conference on Inventive Computation Technologies (ICICT)* (pp. 118-125). IEEE.
103. Rathod, C. H. A. N. D. A. R., & Reddy, G. K. (2016). Experimental investigation of angular distortion and transverse shrinkage in CO2 arc welding process. *International Journal of Mechanical Engineering*, *5*, 21-28.
104. Rao, G. V., Reddy, G. K., Jagadish Babu, G., & Rao, V. V. S. (2012). Prediction of thermal post buckling and deduction of large amplitude vibration behavior of spring–hinged beams. *Forschung im Ingenieurwesen*, *76*, 51-58.
105. Reddy, E. J., Reddy, G. K., & Rajendra, D. (2021). Design of lifting tackle for armor plate of sinter machine. *International Journal on Technical and Physical Problems of Engineering*, *13*, 23-28.
106. Reddy, G. K., & Sravanthhi, B. (2019). Design and analysis of a propeller blade used for marine engine. *International Journal of Scientific Research in Science, Engineering and Technology*, *6*(1), 440-445.
107. Reddy, H., Reddy, G., Phanindra, G., & Kumar, K. (2018). Design and Analysis of Condenser Using 3D Modelling Software. *International Journal of Research in Engineering and Technology*, *7*, 2319-1168.
108. Reddy, E. J., & Sridhar, C. N. V., Rangadu VP (2015) Knowledge Based Engineering: Notion, Approaches and Future Trends. *Am J Intell Syst*, *5*, 1-17.
109. Reddy, E. J., & Rangadu, V. P. (2018). Development of knowledge based parametric CAD modeling system for spur gear: An approach. *Alexandria engineering journal*, *57*(4), 3139-3149.
110. Jayakiran Reddy, E., Sridhar, C. N. V., & Pandu Rangadu, V. (2016). Research and development of knowledge based intelligent design system for bearings library construction using solidworks API. In *Intelligent Systems Technologies and Applications: Volume 2* (pp. 311-319). Springer International Publishing.
111. Reddy, E. J., Venkatachalapathi, N., & Rangadu, V. P. (2018). Development of an approach for Knowledge-Based System for CAD modelling. *Materials Today: Proceedings*, *5*(5), 13375-13382.
112. Reddy, E., Kumar, S., Rollings, N., & Chandra, R. (2015). Mobile application for dengue fever monitoring and tracking via GPS: case study for fiji. *arXiv preprint arXiv:1503.00814*.
113. Parthiban, K. G., & Vijayachitra, S. (2015). Spike detection from electroencephalogram signals with aid of hybrid genetic algorithm-particle swarm optimization. *Journal of Medical Imaging and Health Informatics*, *5*(5), 936-944.
114. Mathew, O. C., Dhanapal, R., Visalakshi, P., Parthiban, K. G., & Karthik, S. (2020). Distributed security model for remote healthcare (dsm-rh) services in internet of things environment. *Journal of Medical Imaging and Health Informatics*, *10*(1), 185-193.
115. Parthiban, K. G., Vijayachitra, S., & Dhanapal, R. (2019). Hybrid dragonfly optimization-based artificial neural network for the recognition of epilepsy. *International Journal of Computational Intelligence Systems*, *12*(2), 1261-1269.
116. Bhat, S. (2024). Building Thermal Comforts with Various HVAC Systems and Optimum Conditions.
117. Bhat, S. Automobile Cabin Pre-Conditioning Method Driven by Environmental Conditions with Multi-Satisfaction Goals.
118. Bhat, S. Thermal Comfort Models' Applicability to Automobile Cabin Environments.
119. Bhat, S. Discovering the Attractiveness of Hydrogen-Fuelled Gas Turbines in Future Energy Systems.
120. Bhat, S. Increasing the Cooling Efficiency of Data Centre Servers with Heat Pipes Based on Liquid Cooling.
121. Bhat, S. Deep Reinforcement Learning for Energy-Efficient Thermal Comfort Control in Smart Buildings.
122. Bhat, S. (2020). Enhancing Data Centre Energy Efficiency with Modelling and Optimisation of End-To-End Cooling.
123. Bhat, S. (2015). Design and Function of a Gas Turbine Range Extender for Hybrid Vehicles.
124. Bhat, S. (2015). Deep Reinforcement Learning for Energy-Saving Thermal Comfort Management in Intelligent Structures.

125. Bhat, S. (2016). Improving Data Centre Energy Efficiency with End-To-End Cooling Modelling and Optimisation.
126. Tayal, S., Upadhyay, A. K., Kumar, D., & Rahi, S. B. (Eds.). (2022). *Emerging low-power semiconductor devices: Applications for future technology nodes*. CRC Press.
127. Kumar, T. V., & Balamurugan, N. B. (2018). Analytical modeling of InSb/AlInSb heterostructure dual gate high electron mobility transistors. *AEU-International Journal of Electronics and Communications*, *94*, 19-25.
128. Karthick, R., Rinoj, B., Kumar, T. V., Prabaharan, A. M., & Selvaprasanth, P. (2019). Automated Health Monitoring System for Premature Fetus. *Asian Journal of Applied Science and Technology (AJAST)(Peer Reviewed Quarterly International Journal) Volume*, *3*, 17-23.
129. Venish Kumar, T., & Balamurugan, N. B. (2020). Three-dimensional analytical modeling for small-geometry AlInSb/AlSb/InSb double-gate high-electron-mobility transistors (DG-HEMTs). *Journal of Computational Electronics*, *19*, 1107-1115.
130. Tejani, A. (2021). Integrating energy-efficient HVAC systems into historical buildings: Challenges and solutions for balancing preservation and modernization. *ESP Journal of Engineering & Technology Advancements*, *1*(1), 83-97.
131. Tejani, A., Yadav, J., Toshniwal, V., & Gajjar, H. (2022). Achieving net-zero energy buildings: The strategic role of HVAC systems in design and implementation. *ESP Journal of Engineering & Technology Advancements*, *2*(1), 39-55.
132. Govindaraj, V. (2024). The Future of Mainframe IDMS: Leveraging Artificial Intelligence for Modernization and Efficiency. *International Journal of Advanced Computer Science & Applications*, *15*(11).
133. Jayasingh, S. K., Mishra, R. K., Swain, S., & Sahoo, A. K. SENTIMENT ANALYSIS TO HANDLE COMPLEX LINGUISTIC STRUCTURES: A REVIEW ON EXISTING METHODOLOGIES.
134. Bandi, M., Masimukku, A. K., Vemula, R., & Vallu, S. (2024). Predictive Analytics in Healthcare: Enhancing Patient Outcomes through Data-Driven Forecasting and Decision-Making. *International Numeric Journal of Machine Learning and Robots*, *8*(8), 1-20.
135. Harinath, D., Bandi, M., Patil, A., Murthy, M. R., & Raju, A. V. S. (2024). Enhanced Data Security and Privacy in IoT devices using Blockchain Technology and Quantum Cryptography. *Journal of Systems Engineering and Electronics (ISSN NO: 1671-1793)*, *34*(6).
136. Harinath, D., Patil, A., Bandi, M., Raju, A. V. S., Murthy, M. R., & Spandana, D. (2024). Smart Farming System–An Efficient technique by Predicting Agriculture Yields Based on Machine Learning. *Technische Sicherheit (Technical Security) Journal*, *24*(5), 82-88.
137. Masimukku, A. K., Bandi, M., Vallu, S., Patil, A., Vasundhara, K. L., & Murthy, M. R. (2025). Innovative Approaches in Diabetes Management: Leveraging Technology for Improved Healthcare Outcomes. *International Meridian Journal*, *7*(7).
138. Harinath, D., Patil, A., Ramadevi, G. R., Bandi, M., Murthy, M. R., & Reddy, K. S. Enhancing Routing Efficiency and Performance in Mobile Ad-Hoc Networks Using Deep Learning Techniques.
139. Thamma, S. R. (2024). A Comprehensive Evaluation and Methodology on Enhancing Computational Efficiency through Accelerated Computing.
140. Thamma, S. R. (2024). An Experimental Analysis of Revolutionizing Banking and Healthcare with Generative AI.
141. Thamma, S. R. (2024). A Case Study on Transforming Legacy Databases Seamless Migration to Snowflake.
142. Vadisetty, R. (2020). Privacy-Preserving Machine Learning Techniques for Data in Multi Cloud Environments. *Corrosion Management ISSN: 1355-5243*, *30*(1), 57-74.
143. Vadisetty, R. (2024, November). Multi Layered Cloud Technologies to achieve Interoperability in AI. In *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)* (pp. 1-5). IEEE.
144. Vadisetty, R. (2024, November). The Effects of Cyber Security Attacks on Data Integrity in AI. In *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)* (pp. 1-6). IEEE.
145. Vadisetty, R. (2024, November). Efficient Large-Scale Data based on Cloud Framework using Critical Influences on Financial Landscape. In *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)* (pp. 1-6). IEEE.
146. Mahalakshmi, A., Goud, N. S., & Murthy, G. V. (2018). A survey on phishing and it's detection techniques based on support vector method (Svm) and software defined networking (sdn). *International Journal of Engineering and Advanced Technology*, *8*(2), 498-503.
147. Swapna Goud, N., & Mathur, A. (2019). A certain investigations on web security threats and phishing website detection techniques. *International Journal of Advanced Science and Technology*, *28*(16), 871-879.

148. Swapna, N. (2017). „Analysis of Machine Learning Algorithms to Protect from Phishing in Web Data Mining". *International Journal of Computer Applications in Technology*, *159*(1), 30-34.
149. SAIPRASANNA, S., GOUD, N. S., & MURTHY, G. V. (2021). ENHANCED RECURRENT CONVOLUTIONAL NEURAL NETWORKS BASED EMAIL PHISHING DETECTION. *Elementary Education Online*, *20*(5), 5970-5970.
150. Balakrishna, G., & Nageshwara Rao, M. (2019). Study report on using IoT agriculture farm monitoring. In *Innovations in Computer Science and Engineering: Proceedings of the Sixth ICICSE 2018* (pp. 483-491). Springer Singapore.
151. Balakrishna, G., & Moparthi, N. R. (2020). Study report on Indian agriculture with IoT. *International Journal of Electrical and Computer Engineering*, *10*(3), 2322.
152. Moparthi, N. R., Balakrishna, G., Chithaluru, P., Kolla, M., & Kumar, M. (2023). An improved energy-efficient cloud-optimized load-balancing for IoT frameworks. *Heliyon*, *9*(11).
153. Balakrishna, G., & Moparthi, N. R. (2019). ESBL: design and implement a cloud integrated framework for IoT load balancing. *International Journal of Computers Communications & Control*, *14*(4), 459-474.
154. Shailaja, K., & Anuradha, B. (2016, December). Effective face recognition using deep learning based linear discriminant classification. In *2016 IEEE international conference on computational intelligence and computing research (ICCIC)* (pp. 1-6). IEEE.
155. Reddy, K. S. S., Manohara, M., Shailaja, K., Revathy, P., Kumar, T. M., & Premalatha, G. (2022). Power management using AI-based IOT systems. *Measurement: Sensors*, *24*, 100551.
156. Swetha, A., & Shailaja, K. (2020). An Effective Approach for Security Attacks Based on Machine Learning Algorithms. In *Advances in Computational Intelligence and Informatics: Proceedings of ICACII 2019* (pp. 293-299). Springer Singapore.
157. Shailaja, K., Vaishnavi, K., Shilpa, P., Naveen, S., & Goud, C. U. Data Augmentation for Medical Image Analysis.
158. Ahmad, S. S., Tejaswi, S., Latha, S. B., Kumari, D. S., Prasad, S. D. V., & Bethu, S. (2023, December). Deep learning based mitosis detection for breast cancer prognosis. In *AIP Conference Proceedings* (Vol. 2938, No. 1). AIP Publishing.
159. Tejaswi, S., Sivaprashanth, J., Bala Krishna, G., Sridevi, M., & Rawat, S. S. (2023, December). Smart Dustbin Using IoT. In *International Conference on Advances in Computational Intelligence and Informatics* (pp. 257-265). Singapore: Springer Nature Singapore.