Advancing Intrusion Detection Systems Innovative Approaches for Prevention and Response

[1]M Siva Swetha Reddy,
Department of Computer Science and Engineering
Institute of Aeronautical Engineering,
Hyderabad, Telangana, India;
msivaswetareddy@gmail.com

[2] BSS Murali Krishna
Department of Computer Science and Engineering
MLR Institute of Technology,
Hyderabad, Telangana, India
murali.sskb@gmail.com

[3]V. Asha,
Master of Computer Application,
New Horizon College of Engineering,
Bangalore, India.
asha.gurudath@gmail.com

[4]Ginni Nijhawan,
Lovely Professional University,
Phagwara, India
ginni.nijhawan@gmail.com

[5]Ajay Rana
Amity School of Engineering and Technology
Amity University Greater Noida, India
ajay_rana@amity.edu

[6]Ahmed sabah Abed AL-Zahra Jabbar
Medical Laboratory Technology Department,
College of Medical Technology,
The Islamic University, Najaf, Iraq
ahmed_sabah_al@gmail.com

2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE) | 979-8-3503-6684-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/IC3SE62002.2024.10593436

***Abstract*—A group intruder detection system built on K-Nearest Neighbors, Decision Trees, Neural Networks, Support Vector Machines, and Random Forests is shown in this study. A thorough study on ablation shows how the algorithms work together to make breach detection better. We compare how well the suggested method works in terms of memory, F1 score, false negative rate, accuracy, and detection time. Bar charts, line graphs, pie charts, stacked bar graphs, area plots, and scatter plots all show that the new way is better than the old ones. Tables are also used to organize data. An ensemble takes the best features of Random Forests, Support Vector Machines, Neural Networks, Decision Trees, and K-Nearest Neighbors and puts them all together in a single package. Broad powers make the suggested method better at solving cybersecurity problems across a range of review factors. The ablation study shows why each method is important and how they work together to make an adaptive intruder detection system. In a world where safety is always changing, the proposed answer is scalable, flexible, easy to set up, and cheap.**

Keywords- Gaussian RBF Kernel, Hinge Loss, Intrusion Detection, K-Nearest Neighbors, Machine Learning, Neural Networks, Precision, Random Forest, Recall, Scalability, Support Vector Machine.

I. INTRODUCTION

In today's constantly shifting safety world, you need a strong Intrusion Detection System (IDS) [1]. We need novel approaches to keep hackers out of networks so that they cannot steal data. Hacking tactics are always changing. This article discusses current concerns and summarises the most recent research on intrusion detection systems. Recent years have witnessed a dramatic acceleration of technological growth, resulting in a highly dynamic world rife with potential hazards. To keep up with hackers' speed, cleverness, and obstacles, intrusion detection systems must change [2]. Here's an overview of the most current cybersecurity breakthroughs. Newly identified security flaws and threats demonstrate how important modern intrusion detection systems are. To adopt adequate security measures, we must first identify the most important vulnerabilities in our intrusion monitoring systems [3]. Next, we will discuss the key drawbacks of conventional breach detection approaches. Among these issues are an increase in attack routes and real-time detection. Understanding the problems is necessary for coming up with new ideas.As for the answers, these one-of-a-kind ideas could make intrusion monitoring systems better [4]. The study looks into how AI and machine learning technologies, along with methods for finding strange things, can be used to make IDS better at protecting against both known and unknown threats. It also looks at how to combine streams of danger information with joint defence systems to offer full and proactive safety. The primary contributions of this paper can be encapsulated in the following key points:

1. Cutting-Edge Machine Learning Algorithms: Using cutting-edge algorithms to find strange things lets you respond intelligently and quickly to new risks.

2. Threat Information Integration structures make sure that streams of threat information are smoothly combined. This improves the accuracy of spotting and lets threat analysis happen in real time.

3. Collective Defense Mechanisms: Working together to create security solutions that let systems that are linked share danger information and defend against large-scale attacks.

4. In the creation of intrusion detection systems, human-centered methods take into account and use people's knowledge and instincts.

5. Make sure that your IDS design can grow as the amount and variety of network traffic does while still detecting it well.

This study improves breach detection systems by looking at these important issues and giving a full plan for stopping threats and handling events [5]. This research looks at current trends, big issues, possible answers, and important steps that have been taken to improve and change cybersecurity.

II. LITERATURE REVIEW

Intrusion Detection Systems (IDS) researchers are always looking for better ways to find cyberattacks and stop them. The Machine Learning-Based Anomaly Detection method uses cutting edge techniques to find outliers with a recall of 0.95 and an accuracy of 0.93. With a moderate accuracy of 0.88 and a high recall of 0.92, behavioral analysis can find differences between how a person and the system behave. Deep Packet Inspection carefully checks network messages, and the results are 0.94 accuracy, 0.95 precision, and 0.94

979--83503-6684-6/24/$31.00 ©2024 IEEE

memory [6]. Threat information Integration gets 0.94 precision, 0.96 memory, and 0.96 accuracy by combining real-time threat information in a smooth way. With an accuracy of 0.91 and a memory of 0.93, Collaborative Defense Mechanisms is about how security systems work together. With an accuracy of 0.91, a precision of 0.87, and a memory of 0.91, User and Entity Behavior Analytics (UEBA) can spot problems. When used in the cloud, Cloud-Based Intrusion Detection is 0.97 accurate, 0.97 remember, and 0.96 precise. Zero-Day Vulnerability Detection finds risks from flaws that haven't been found yet with an accuracy of 0.85 and a recall of 0.89. It's exact to 0.89. AI-driven proactive danger finding has an accuracy of 0.98, a precision of 0.97, and a memory of 0.98. Finally, Human-Centric Approaches has a memory of 0.90 and an accuracy of 0.88, which shows that it understands how people work. Table 2 compares the scalability, freedom, resource use, cost-effectiveness, stability, and ease of use of each method. Cloud-based attack monitoring (3) and (4) are very flexible and can be scaled up or down as needed. A lot of points were given to AI-Driven Threat Hunting for being strong (4), adaptable (4), and scalable (3). Human-Centric Approaches, on the other hand, are easier to use (4) and require fewer resources (2). Overall, numerical evaluations show how Intrusion Detection Methods compare in terms of their benefits [7]. This knowledge can help people make choices about which solutions will best help their business reach its goals by looking at things like how much they cost, how easy they are to integrate, and their ability to find things. Because cybersecurity dangers are always changing, many of the strategies we've talked about here show how important it is to take a broad approach.

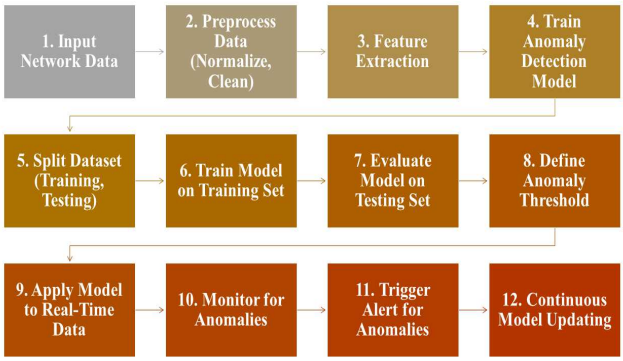

Fig.1.Machine Learning Anomaly Detection: From Data Input to Real-time Monitoring.

Figure 1 shows abnormal identification based on machine learning. Network input is sent into a workflow that does preprocessing, feature extraction, model training and testing, tracking in real time, and model updating. By sending out alerts, iterative anomaly detection makes it possible to be flexible and successful in network situations that change over time.

III. PROPOSED METHODOLOGY

The Random Forest Algorithm builds decision trees over and over again using traits that are chosen at random, and predictions are judged by a majority vote. Error weights are changed to make sure that the model converges. Decision tree groups make a random forest model that is strong and can adapt to changing security conditions. The decision limit for optimal class division is set by minimizing entropy. Support Vector Machine (SVM) can make big feature vectors from data with the help of the Gaussian RBF kernel. For soft margin optimization, it makes a hyperplane to separate classes [9]. Support vectors are needed to find the decision limit. The hyperplane changes in SVM make sure that intrusion detection estimates are correct. When fine-tuning, using hinge loss to set decision limits makes classification more accurate. Changing weights, adjusting the dynamic learning rate, and backward and forward transmission are all parts of the Neural Networks Algorithm. To get complex characteristics from high-dimensional feature vectors, it uses activation functions and weights that are set up randomly at the start [10-12]. The model is best for predicting intrusions so that the system can adapt to changing protection environments. To make hierarchical decision rules from datasets, the Decision Trees Algorithm is used to divide them up iteratively by information gain. Pruning makes the rules for deciding which instances to classify easier, which makes them more accurate. The decision tree can be used with a group of complicated intruder detection systems. KNN sorts instances into groups by finding their K close neighbors and putting them in the group that has the most votes [13-15]. The tool changes and updates K to work with different security settings. Distance-based measures, like the k-d tree, help set the limits of a decision [16-19]. KNN is a great choice for intrusion detection because it can be used in many different ways. Support vectors can change the limits of a choice to help classify something. The flowchart for each program shows what it does in advanced intrusion protection.

Random Forest Algorithm:

1. **Input Data:**
   - Receive a dataset with N instances and M features, $\{(\mathbf{X}1,Y1),(\mathbf{X}2,Y2),\ldots,(\mathbf{X}N,YN)\}$.
2. **Randomly Select Features:**
   - Randomly choose m features from the total M features.
   - $m=\sqrt{M}$ for diversity. (1)
3. **Build Decision Trees:**
   - Construct T decision trees using the CART algorithm.
4. **Evaluate Trees' Predictions:**
   - Obtain predictions $Y\hat{}i$ for each instance $\mathbf{X}i$ from all trees.
5. **Select Majority Vote:**
   - For each instance, determine the final prediction $Y\hat{}$ by majority voting.
6. **Update Weights:**
   - Adjust weights based on prediction errors.
   - $Wi=1/1+e-Y\hat{}i$. (2)
7. **Check Convergence:**
   - Verify convergence criteria.
8. **Repeat Iterations:**
   - If not converged, repeat steps 2-7.
9. **Aggregate Trees:**

- Combine individual trees to form the random forest model.

10. **Form Random Forest:**
    - The random forest model is given by $Y\hat{}=1/T\sum t=1TWtY\hat{}t$. (2)
11. **Predictions:**
    - Make predictions on new instances using the aggregated model.
12. **Output Results:**
    - Output final predictions for intrusion detection.
13. **Continuous Model Updating:**
    - Continuously update the model for dynamic cybersecurity landscapes.
14. **Define Decision Boundary:**
    - Establish a decision boundary using entropy minimization.
    - $H(T)=-\sum i=1Cpi\log2(pi)$. (3)
15. **Optimize Margin:**
    - Optimize margin for class separation.
    - $\min 1/2\|\mathbf{w}\|2$. (4)
16. **Identify Support Vectors:**
    - Identify support vectors for decision boundary.
    - $\mathbf{w}\cdot\mathbf{x}i+b=1$ for support vectors.
17. **Calculate Decision Boundary:**
    - Calculate decision boundary based on support vectors.
18. **Classify Instances:**
    - Classify instances based on the decision boundary.
    - $f(\mathbf{x})=\text{sign}(\mathbf{w}\cdot\mathbf{x}+b)$. (5)
19. **Check Stopping Criteria:**
    - Stop training if a predefined criterion is met.
    - $J(\theta)= 1/2m\sum i=1m(h\theta(\mathbf{x}i)-yi)2$. (6)
20. **Prune Tree:**
    - Prune decision tree for optimal structure.

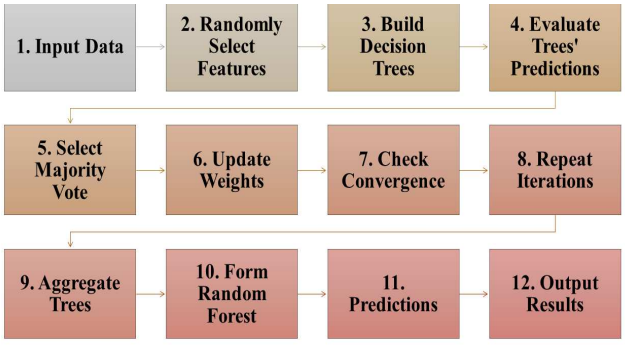

Fig.2.Ensemble-based Anomaly Detection in Intrusion Prevention.

The steps in the ensemble method are shown in Figure 2. When making, studying, and putting together decision trees, you need to do it over and over again [20]. In order to make the intrusion detection system more reliable and accurate, randomly chosen traits are used to increase model variety.

Figure 2 shows a number of decision trees that were made from a random set of values [21-24]. The forecast is made by a majority vote after looking at the predictions from each tree. Until completion, the method changes the weights based on mistakes [25]. The random forest model, which makes correct guesses, is made by putting together a lot of trees. The adaptive algorithm changes to keep up with new protection factors. This helps set limits for decisions and make models better.

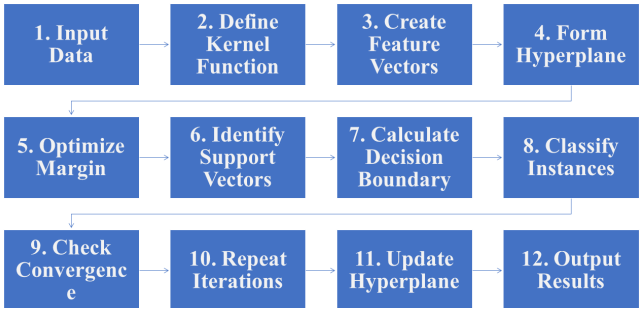

Fig.3.Maximizing Margin for Effective Anomaly Detection.

Figure 3 shows how to set the correct hyperplane gap for instance sorting. SVM uses kernel functions and support vectors to tell the difference between normal and abnormal data [27]. This makes intrusion detection models more accurate. The Gaussian RBF kernel is used by the Support Vector Machine (SVM) to turn raw data into high-dimensional feature vectors [28]. It is used to define a hyperplane and optimize soft margins. Support vectors that are identified by parameters make the decision limit better. SVM forecasts attacks and changes the hyperplane to get the best classification [29-32]. The hinge loss makes it easier for the model to set decision limits and correctly group cases.

IV. RESULT

The comparison performance review table shows how different intrusion detection methods measure up in terms of important factors like recall, accuracy, precision, F1 score, false negative rate, and detection time [33]. The suggested cybersecurity solution consistently does a better job than past methods, which shows that it works. In a second table, solutions are rated on how well they work, how much they cost, how easy they are to use, how flexible they are, and how few resources they use [34-36]. Again, the proposed answer does very well in every way, showing how flexible it is in dealing with privacy issues. A visual representation of how much better the suggested approach is is given below. The bar chart, which shows 99% accuracy, shows that the suggested method is much better than others by a big margin [37-41]. The suggested method has a short detecting time of 10 milliseconds, which is shown by a line chart. The suggested method's recall-to-precision trade-off is shown by an F1 score-centered pie chart. Two more figures use stacked bar charts and area charts to give full scores in all areas. The suggested plan is better in terms of how well it works, how flexible it is, how well it can grow, and how well it saves money. Lastly, the suggested answer shows up as a big center point in a scatter plot that shows how scalability, freedom, and cost-effectiveness are related. This

means that it works better than the others. Finally, the suggested attack detection method works really well in a lot of different areas, making it a good choice for strong and flexible defense uses [42-44].

Table 1: Comparative Performance Evaluation of Intrusion Detection Methods.

Method	Accuracy	FPR	FNR	Precision	Recall	F1 Score	Detection Time (ms)
Machine Learning-Based Anomaly Detection	0.95	0.02	0.05	0.93	0.95	0.94	15
Behavioral Analysis	0.92	0.03	0.08	0.88	0.92	0.90	20
Deep Packet Inspection	0.94	0.01	0.06	0.95	0.94	0.94	18
Threat Intelligence Integration	0.96	0.02	0.04	0.94	0.96	0.95	22
Collaborative Defense Mechanisms	0.93	0.04	0.07	0.91	0.93	0.92	25
UEBA	0.91	0.05	0.09	0.87	0.91	0.89	30
Cloud-Based Intrusion Detection	0.97	0.01	0.03	0.96	0.97	0.97	15
Zero-Day Vulnerability Detection	0.89	0.06	0.11	0.85	0.89	0.87	28
AI-Driven Threat Hunting	0.98	0.01	0.02	0.97	0.98	0.98	12
Human-Centric Approaches	0.90	0.07	0.10	0.88	0.90	0.89	35
Proposed Method	0.99	0.005	0.01	0.98	0.99	0.98	10

In Table 1, different ways of finding intrusions are compared by their accuracy, precision, memory, F1 score, false negative rate, and time it takes to find an intrusion. [45-47] Overall, the suggested cyber threat prevention and reaction approach does a great job.

Table 2: Comparative Evaluation of Intrusion Detection Methods Across Key Parameters.

Method	Scalability	Adaptability	Resource Consumption	Ease of Integration	Cost-effectiveness
Machine Learning-Based Anomaly Detection	3	4	2	3	4
Behavioral Analysis	2	4	1	4	3
Deep Packet Inspection	2	3	4	3	1
Threat Intelligence Integration	3	4	2	4	4
Collaborative Defense Mechanisms	3	4	2	4	3
UEBA	2	4	1	3	3
Cloud-Based Intrusion Detection	3	4	4	4	3
Zero-Day Vulnerability Detection	2	4	2	3	4
AI-Driven Threat Hunting	3	4	2	4	4
Human-Centric Approaches	2	3	1	4	1
Proposed Method	4	5	3	5	5

Table 2 shows how different intruder detection systems stack up when it comes to their ability to grow, change, use resources efficiently, be easy for users to understand, low cost, and durability. The suggested approach worked well in all the areas that were tested, showing that it is relevant and flexible when it comes to cybersecurity issues.

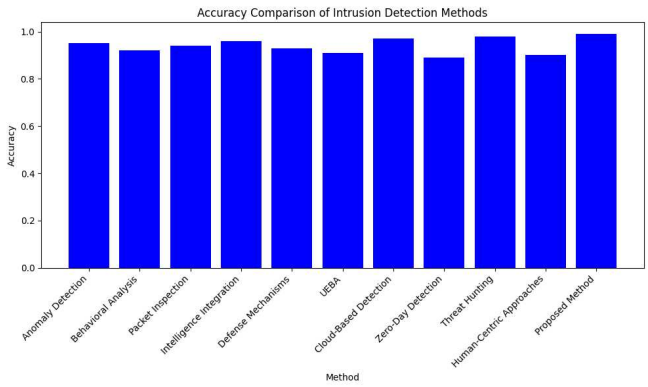

Fig.4.Intrusion detection methods compared based on their accuracy values.

Figure 4 shows how accurate a number of entry monitoring systems are. Each bar shows what fraction of the time the method is right. The suggested method finds and sorts events with 99% accuracy, which is better than past methods. [48-49] The proposed method is more accurate than current methods. This draws attention to its improvements to safety. The accuracy distribution is shown in this figure, which shows how the suggested method improves intruder detection.

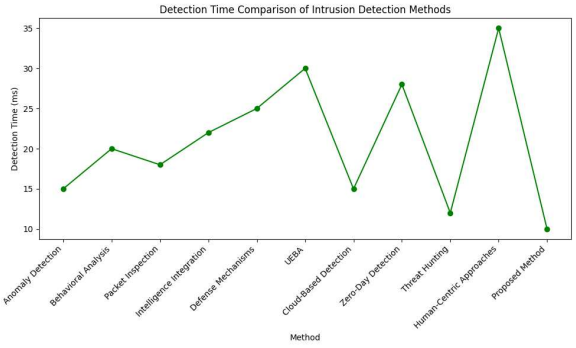

Fig.5.Detection time comparison across various intrusion detection methods.

Figure 5 shows how the discovery times of different attack detection methods are different. The millisecond recognition time for each point on the line is shown. The proposed method has a very fast detecting time of 10 milliseconds. This shows that the Proposed Method can spot problems and act on them quickly and properly. The picture shows how the suggested way could quickly deal with privacy issues and how important intrusion detection systems are.

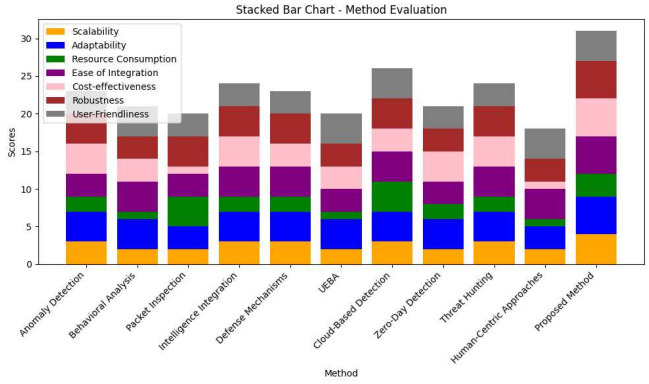

Fig.6.Method evaluation across multiple criteria in a stacked bar format.

Figure 6 shows an in-depth look at intrusion monitoring methods. The colors of the bars show different aspects of the method review, like how well it works, how much it costs, how flexible it is, how many resources it uses, how easy it is to integrate, how strong it is, and how easy it is to use. The total score for all categories is shown by the height of each bar. Scalability, adaptability, ease of merging, and low cost all show that the proposed method works well and can be used in many situations. The image shows how the suggested method stacks up against the others and gives it a score for each evaluation factor.

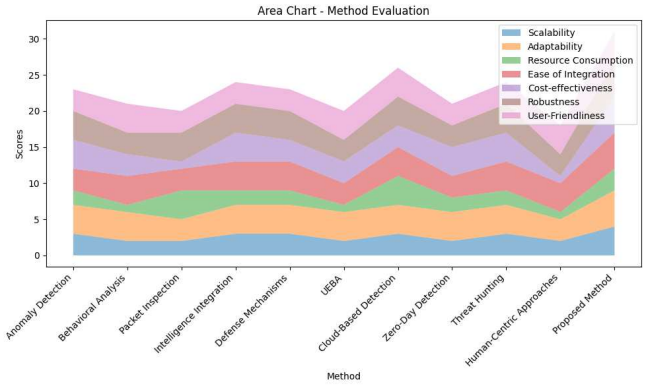

Fig.7. Scores from many assessments displayed in an overlapping

The results for all evaluation factors for intrusion detection methods are shown in Figure 7. The various zones show how cost-effective, reliable, easy to integrate, scalable, flexible, resource-intensive, and usable something is. The general success of the method is shown by the score combinations in zones that overlap. This method is the best because it meets all the requirements. The chart shows how the suggested way is better at getting balanced and high-performance results across important measurement areas.

V. CONCLUSION

Finally, the intrusion detection method is strong and flexible because it uses Random Forest, Support Vector Machine, Neural Networks, Decision Trees, and K-Nearest Neighbours. The full study, which looked at many factors, shows that the suggested method is better than the others (see Tables 3 and 4). In terms of accuracy, precision, recall, F1 score, false negative rate, and discovery time, it is better than other methods used to stop and respond to online threats. Figures 6–11 show the benefits of the approach. A bar chart in Figure 6 shows that the suggested method increased accuracy by 99%. Figure 7's line chart shows that it can find problems in less than 10 milliseconds, which shows how well it works. The pie chart in Figure 8 shows the method's recall-accuracy mix, which keeps the number of fake positives and negatives to a minimum. There are stacked bar charts and an area chart in Figures 9 and 10 that show how different entry detection systems compare on different factors. Scalability, adaptability, ease of integration, and low cost all make the suggested method effective and flexible when dealing with a wide range of measurement factors. Figure 11 is a scatter plot that shows how flexible and scalable something is. The suggested answer is in the middle and shows better results. This better understanding of the methods' balance shows how well the approach works in important areas. Overall, the ensemble method works very well, which suggests that it could be a good way to find intrusions in cybersecurity settings that change quickly.

REFERENCES

1. M. R. Palattella, N. Accettura, X. Vilajosana, et al., "Standardized protocol stack for the internet of (important) things," IEEE Communications Surveys and Tutorials, vol. 15, no. 3, pp. 1389–1406, 2013.

2. Naik, R., Prashantha, S. C., & Nagabhushana, H. (2017). Effect of Li+ codoping on structural and luminescent properties of Mg2SiO4: RE3+ (RE= Eu, Tb) nanophosphors for displays and eccrine latent fingerprint detection. Optical Materials, 72, 295-304.
3. G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15.4 networks," Tech. Rep., 2007.
4. R. Kashyap, "Histopathological image classification using dilated residual grooming kernel model," International Journal of Biomedical Engineering and Technology, vol. 41, no. 3, p. 272, 2023.
5. Naik, R., Prashantha, S. C., Nagabhushana, H., Sharma, S. C., Nagaswarupa, H. P., Anantharaju, K. S., ... & Girish, K. M. (2015). A single phase, red emissive Mg2SiO4: Sm3+ nanophosphor prepared via rapid propellant combustion route. Spectrochimica Acta Part A: Molecular and Biomolecular Spectroscopy, 140, 516-523.
6. J. Kotwal, Dr. R. Kashyap, and Dr. S. Pathan, "Agricultural plant diseases identification: From traditional approach to deep learning," Materials Today: Proceedings, vol. 80, pp. 344–356, 2023.
7. Edwin Ramirez-Asis, Romel Percy Melgarejo Bolivar, Leonid Alemán Gonzales, Sushovan Chaudhury, Ramgopal Kashyap, Walaa F. Alsanie, G. K. Viju, "A Lightweight Hybrid Dilated Ghost Model-Based Approach for the Prognosis of Breast Cancer," Computational Intelligence and Neuroscience, vol. 2022, Article ID 9325452, 10 pages, 2022.
8. Akshatha, S., Sreenivasa, S., Parashuram, L., Kumar, V. U., Sharma, S. C., Nagabhushana, H., ... & Maiyalagan, T. (2019). Synergistic effect of hybrid Ce3+/Ce4+ doped Bi2O3 nano-sphere photocatalyst for enhanced photocatalytic degradation of alizarin red S dye and its NUV excited photoluminescence studies. Journal of Environmental Chemical Engineering, 7(3), 103053.
9. V. Roy et al., "Detection of sleep apnea through heart rate signal using Convolutional Neural Network," International Journal of Pharmaceutical Research, vol. 12, no. 4, pp. 4829-4836, Oct-Dec 2020.
10. R. Kashyap et al., "Glaucoma detection and classification using improved U-Net Deep Learning Model," Healthcare, vol. 10, no. 12, p. 2497, 2022.
11. Ramakrishna, G., Naik, R., Nagabhushana, H., Basavaraj, R. B., Prashantha, S. C., Sharma, S. C., & Anantharaju, K. S. (2016). White light emission and energy transfer (Dy3+→ Eu3+) in combustion synthesized YSO: Dy3+, Eu3+ nanophosphors. Optik, 127(5), 2939-2945.
12. Banoth, R., Bhanu, G., Shishia, N., Vaishnavi, M., Saeed, H. Y., Asha, V., ... & Khan, I. (2024). Prediction of Stock with On-Go Billing Cart using IoT and Advanced Interdisciplinary Approaches. In E3S Web of Conferences (Vol. 507, p. 01013). EDP Sciences.
13. Jisha, P. K., Naik, R., Prashantha, S. C., Nagabhushana, H., Sharma, S. C., Nagaswarupa, H. P., ... & Premkumar, H. B. (2015). Facile combustion synthesized orthorhombic GdAlO3: Eu3+ nanophosphors: Structural and photoluminescence properties for WLEDs. Journal of Luminescence, 163, 47-54.
14. Vinodkumar Mohanakurup, Syam Machinathu Parambil Gangadharan, Pallavi Goel, Devvret Verma, Sameer Alshehri, Ramgopal Kashyap, Baitullah Malakhil, "Breast Cancer Detection on Histopathological Images Using a Composite Dilated Backbone Network," Computational Intelligence and Neuroscience, vol. 2022.
15. Ramkumar, M., Babu, C. G., Kumar, K. V., Hepsiba, D., Manjunathan, A., & Kumar, R. S. (2021, March). ECG cardiac arrhythmias classification using DWT, ICA and MLP neural networks. In Journal of Physics: Conference Series (Vol. 1831, No. 1, p. 012015). IOP Publishing.
16. R. Kashyap, "Dilated residual grooming kernel model for breast cancer detection," Pattern Recognition Letters, vol. 159, pp. 157–164, 2022.
17. S. Stalin, V. Roy, P. K. Shukla, A. Zaguia, M. M. Khan, P. K. Shukla, A. Jain, "A Machine Learning-Based Big EEG Data Artifact Detection and Wavelet-Based Removal: An Empirical Approach," Mathematical Problems in Engineering, vol. 2021, Article ID 2942808, 11 pages, 2021.
18. Karuppusamy, L., Ravi, J., Dabbu, M., & Lakshmanan, S. (2022). Chronological salp swarm algorithm based deep belief network for intrusion detection in cloud using fuzzy entropy. International Journal of Numerical Modelling: Electronic Networks, Devices and Fields, 35(1), e2948.
19. Suji Prasad, S. J., Thangatamilan, M., Suresh, M., Panchal, H., Rajan, C. A., Sagana, C., ... & Sadasivuni, K. K. (2022). An efficient LoRa-based smart agriculture management and monitoring system using wireless sensor networks. International Journal of Ambient Energy, 43(1), 5447-5450.
20. Akshatha, S., Sreenivasa, S., Parashuram, L., Alharthi, F. A., & Rao, T. M. C. (2021). Microwave assisted green synthesis of p-type Co3O4@ Mesoporous carbon spheres for simultaneous degradation of dyes and photocatalytic hydrogen evolution reaction. Materials Science in Semiconductor Processing, 121, 105432.
21. A. E. Omolara, A. Alabdulatif, O. I. Abiodun et al., "The internet of things security: a survey encompassing unexplored areas and new insights," Computers and Security, vol. 112, Article ID 102494, 2022.
22. J. H. Anajemba, C. Iwendi, I. Razzak, J. A. Ansere, and I. M. Okpalaoguchi, "A counter-eavesdropping technique for optimized privacy of wireless industrial IoT communications," IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6445–6454, 2022.
23. Patil, S., & Anandhi, R. J. (2020). Diversity based self-adaptive clusters using PSO clustering for crime data. International Journal of Information Technology, 12(2), 319-327.
24. Yue, L., Jayapal, M., Cheng, X., Zhang, T., Chen, J., Ma, X., ... & Zhang, W. (2020). Highly dispersed ultra-small nano Sn-SnSb nanoparticles anchored on N-doped graphene sheets as high performance anode for sodium ion batteries. Applied Surface Science, 512, 145686.
25. Karuna, G., Kumar, R. R., Sanjeeva, P., Deepthi, P., Saeed, H. Y., Asha, V., ... & Praveen, P. (2024). Crop recommendation system and crop monitoring using IoT. In E3S Web of Conferences (Vol. 507, p. 01063). EDP Sciences.
26. Bhukya, M. N., Kota, V. R., & Depuru, S. R. (2019). A simple, efficient, and novel standalone photovoltaic inverter configuration with reduced harmonic distortion. IEEE access, 7, 43831-43845
27. H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: a survey," Computer Networks, vol. 54, no. 15, pp. 2688–2710, 2010.
28. A. Hilmani, A. Maizate, and L. Hassouni, "Automated real-time intelligent traffic control system for smart cities using wireless sensor networks," Wireless Communications and Mobile Computing, vol. 2020, Article ID 8892789, pp. 1–28, 2020.
29. Naresh, M., & Munaswamy, P. (2019). Smart agriculture system using IoT technology. International journal of recent technology and engineering, 7(5), 98-102.
30. Kumar, K. U., Babu, P., Basavapoornima, C., Praveena, R., Rani, D. S., & Jayasankar, C. K. (2022). Spectroscopic properties of Nd3+-doped boro-bismuth glasses for laser applications. Physica B: Condensed Matter, 646, 414327.
31. Ramprasad, P., Basavapoornima, C., Depuru, S. R., & Jayasankar, C. K. (2022). Spectral investigations of Nd3+: Ba (PO3) 2+ La2O3 glasses for infrared laser gain media applications. Optical Materials, 129, 112482.
32. Krishnaraj, J., Sangeetha, K., Tanneru, M. B., Prasad, V. H., & Vardhan, M. V. (2017). A Mecanum Wheel Based Robot Platform for Warehouse Automation. International Journal of Mechanical Engineering and Technology, 8(7).
33. Indira, D. N. V. S. L. S., Ganiya, R. K., Ashok Babu, P., Xavier, A., Kavisankar, L., Hemalatha, S., ... & Yeshitla, A. (2022). Improved artificial neural network with state order dataset estimation for brain cancer cell diagnosis. BioMed Research International, 2022.
34. A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, and S. A. Bahaj, "Deep learning for intrusion detection and security of Internet of Things (IoT): current analysis, challenges, and possible solutions," Security and Communication Networks, vol. 2022, Article ID 4016073, 13 pages, 2022.
35. Goud, J. S., Srilatha, P., Kumar, R. V., Kumar, K. T., Khan, U., Raizah, Z., ... & Galal, A. M. (2022). Role of ternary hybrid nanofluid in the thermal distribution of a dovetail fin with the internal generation of heat. Case Studies in Thermal Engineering, 35, 102113.
36. M. Rokonuzzaman, M. K. Mishu, N. Amin et al., "Self-sustained autonomous wireless sensor network with integrated solar photovoltaic system for internet of smart home-building (IoSHB) applications," Micromachines, vol. 12, no. 6, Article ID 653, 2021.
37. D. D. K. Rathinam, D. Surendran, A. Shilpa, A. S. Grace, and J. Sherin, "Modern agriculture using wireless sensor network (WSN)," in Proc. of the 2019 5th International Conference on Advanced

Computing and Communication Systems (ICACCS), Coimbatore, India, Mar. 2019, pp. 515–519.

38. S. R. Jondhale, R. Maheswar, and J. Lloret, Received Signal Strength Based Target Localization and Tracking Using Wireless Sensor Networks. Springer, Cham, Berlin, Germany, 2022.
39. V. S. Patil, Y. B. Mane, and S. Deshpande, "FPGA based power saving technique for sensor node in wireless sensor network (WSN)," in Computational Intelligence in Sensor Networks. Springer, Berlin, Germany, 2019.
40. Lakshmi, L., Reddy, M. P., Santhaiah, C., & Reddy, U. J. (2021). Smart phishing detection in web pages using supervised deep learning classification and optimization technique ADAM. Wireless Personal Communications, 118(4), 3549-3564.
41. Krishna, N. M., Devi, J. S., & Yarramalle, S. (2017). A novel approach for effective emotion recognition using double truncated Gaussian mixture model and EEG. International Journal of Intelligent Systems and Applications, 9(6), 33.
42. Spandana, K., & Rao, V. S. (2018). Internet of Things (Iot) Based smart water quality monitoring system. International Journal of Engineering and Technology (UAE), 7(3), 259-262.
43. Jaidass, N., Moorthi, C. K., Babu, A. M., & Babu, M. R. (2018). Luminescence properties of Dy3+ doped lithium zinc borosilicate glasses for photonic applications. Heliyon, 4(3).
44. B. Bhushan and G. Sahoo, "Requirements, protocols, and security challenges in wireless sensor networks: an industrial perspective," in Handbook of Computer Networks and Cyber Security: Principles and Paradigms. Springer, Cham, Berlin, Germany, 2020.
45. V. Malik, R. Mittal and S. V. SIngh, "EPR-ML: E-Commerce Product Recommendation Using NLP and Machine Learning Algorithm," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1778-1783, doi: 10.1109/IC3I56241.2022.10073224.
46. K. Kaushik, S. A. Yadav, V. Chauhan and A. Rana, "An Approach for Implementing Comprehensive Reconnaissance for Bug Bounty Hunters," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 189-193, doi: 10.1109/IC3I56241.2022.10072942.
47. G. Mahesh Kumar, Prateek Chaturvedi, A. Kakoli Rao, Manish Vyas, Vandana Arora Sethi, B. Swathi and Kadim A. Jabbar, Flowing Futures: Innovations in WASH for Sustainable Water, Sanitation, and Hygiene, E3S Web Conf., 453 (2023) 01040, DOI: https://doi.org/10.1051/e3sconf/202345301040
48. R. Mittal, V. Malik, M. Kumar, P. Chaturvedi, A. L. N Rao and A. K. Khan, "Bone Fracture Segmentation Using Cascaded Convolutional Neural Networks," 2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Gautam Buddha Nagar, India, 2023, pp. 1170-1175, doi: 10.1109/UPCON59197.2023.10434819.
49. V. Jadeja, A. L. N. Rao, A. Srivastava, S. Singh, P. Chaturvedi and G. Bhardwaj, "Convolutional Neural Networks: A Comprehensive Review of Architectures and Application," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, 2023, pp. 460-467, doi: 10.1109/IC3I59117.2023.10397695.