International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802063

Physical Layer Security: Detection of Active Eavesdropping Attacks

S.Amutha, Mariselvam M, Mohamed Irfan M, Vishnu V

Department of Computer Science and Engineering Erode Sengunthar Engineering College, Erode, Tamil Nadu, India

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: Frothy Disturbance Intrusion Detection Systems (FIDSs) can help detect and prevent security attacks using the SVM algorithm. Recognizing the importance of Frothy Disturbance Intrusion Detection Systems (FIDSs) in protecting various domains linked to the internet, we concentrate on adapting traditional intrusion detection methods for the landscape, which faces challenges such as resource constraints and limited memory and battery capacity. Our study entails the creation of a lightweight attack detection technique that uses a supervised machine learning-based FIDS using the Multivariate correlation analysis algorithm. We use simulations to demonstrate the usefulness of the proposed SVM-based FIDS classifier, which uses a combination of two or three complex features and achieves satisfactory classification accuracy and detection time. This approach shows potential for improving application security by efficiently addressing the specific limits and requirements of intrusion detection in resource-constrained contexts.

KEYWORDS: Edge Computing, Frothy Disturbance, Distributed Systems

I. INTRODUCTION

Within the field of cybersecurity, the increasing intricacy and refinement of network threats present a formidable obstacle to traditional Intrusion Detection Systems (IDS), especially when it comes to unbalanced network traffic. When datasets are imbalanced and the distribution of malicious and legitimate activity is skewed, traditional intrusion detection systems (IDS) frequently fail to identify and handle abnormalities in an efficient manner. This study offers a novel solution by utilizing Transformer-based transfer learning approaches in order to get beyond these restrictions. Through the utilization of Transformer models, which have proven to be very effective in sequence processing tasks, this suggested IDS seeks to improve its flexibility and ability to generalize to scenarios including imbalanced network traffic. By enhancing intrusion detection's precision and effectiveness in the face of changing cybersecurity threats, this revolutionary method aims to strengthen network infrastructures' resistance to malicious activity.

1.1 INTRUSION DETECTION SYSTEM (IDS)

Intrusion Detection Systems (IDS) are critical protectors in the constantly changing field of cybersecurity, acting as watchful sentinels against the numerous threats that might lie within digital networks. An intrusion detection system (IDS) is an essential part of the defense against malicious activity, illegal access, and potential security breaches. IDS acts as an advanced surveillance system, watching over network traffic in real time

and examining trends and behaviors to spot anomalies that can point to possible security risks. IDS is essential to bolstering the resilience of digital infrastructures since it combines anomaly detection, heuristic analysis, and signature-based detection. The relevance of intrusion detection systems (IDS) is growing as the digital world gets bigger and more diverse. IDS gives businesses a vital tool to protect critical data in advance and keep their networks intact.

1.2 IMBALANCED NETWORK TRAFFIC

The idea of imbalanced network traffic arises as a crucial difficulty in the complex field of network communication, with significant implications for the effectiveness of information transmission and system performance. When data flows between different nodes or channels within a network are distributed disproportionately, it is known as imbalanced network traffic and can result in inefficiencies, congestion, and increased susceptibility to security attacks. An unequal distribution of communication patterns, where some nodes receive noticeably more or less traffic than others, is a common characteristic of this phenomena. It is critical to comprehend and resolve unbalanced network traffic in order to maximize network resources, guarantee fair data delivery, and improve overall system reliability. Navigating the complexities of imbalanced network traffic becomes crucial for fostering effective and secure communication infrastructures as digital interconnection of systems continues to grow.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802063

1.3 FROTHY DISTURBANCE

The term "frothy disturbance" evokes a sense of turbulence, possibly in the context of science, nature, or even allegory. When referring to interruptions or oscillations in a fluid or gas that are accompanied by bubbles or foam, scientists may use the term "frothy disturbance." Numerous variables, such as variations in composition, pressure, or temperature, could be the cause of this disruption. It could conjure images of choppy seas in the outdoors, signifying a dynamic and constantly shifting setting. A foamy disturbance could be used metaphorically to depict an exciting or unpredictable situation where things are constantly changing. This word provides a unique prism through which to grasp the dynamics at play and stimulates investigation into the sources and effects of such disruptions, whether in natural events, scientific phenomena, or abstract conceptions.

II. LITERATURE SURVEY

Adewale Lukman [1] Research on the incorporation of smart technology into home automation systems is expanding, with the main goal being to improve the efficiency and comfort of living spaces. Although conventional manual window controls have fulfilled their intended function, the emergence of Internet of Things (IoT) technology has created novel opportunities for automating several facets of household administration. Although a lot of literature has been written about automated windows, there is still a clear need to build complete smart window control systems that take into account various environmental factors. In order to close this gap, a cyber-physical system (CPS) for windows automation control and smart rooms (SRWAC) is presented in this study. In order to determine how the system would react to input data gathered from inside and outdoor sensing units, the suggested system makes use of a set of rules produced by a Petri Net simulator. These sensing systems, which offer a comprehensive approach to environmental monitoring, comprise temperature, dust, rain, and carbon monoxide sensors.

John, [2] the importance of tackling the changing cybersecurity threat is growing along with the reliance on computer systems. This work uses an expanded version of the well-known Petri net framework to explore the complex domain of cyberattacks. Petri nets with players, strategies, and prices are the specific formalism used here, which provides a detailed depiction of cyberattack situations. The states of a cyberattack are represented in this formalism as marks, and the actions that take place during an attack are represented by transition firings inside the Petri net. This approach is novel in that it takes players, strategies, and costs into account. The model perceives attackers and defenders as rival players and makes a distinction between them.

ASMAA A. ELSAEID [3] Because intrusion detection has a significant impact on the dependability and quality of services these technologically sophisticated urban environments deliver, it is an important issue in the context of smart cities. Replay attacks are one of the most common risks that smart city infrastructure faces, and they pose a serious risk to the authentication procedures that are built into smart city networks. A successful replay assault may have a variety of negative effects, such as the compromising of sensitive data and physical harm to the infrastructure of smart cities, which could result in significant financial losses. In order to overcome this difficulty, new research has suggested deep learning-based intrusion detection systems and frameworks for smart cities. Replay attack detection accuracy can be improved by the use of deep learning models. Nevertheless, a noteworthy drawback of current suggestions is their neglect of the temporal dimension, which is an essential component in the dynamic and changing field of smart city operations. Our work offers a novel deep learning-based model designed specifically for replay attack detection in smart cities as a solution to this restriction.

Rong Fu [4] The intrinsic size and complexity of smart grids have increased dramatically as they become more automated and networked, opening up a bigger attack surface for possible cyber threats. The increasing interconnectedness of smart grids makes it more difficult to identify and quickly address cyberattacks. There may be dire repercussions if the power system vulnerabilities are not found in a timely manner and the necessary remedies are not put into place right away. This work addresses these issues by introducing a unique voltage control method that combines an event triggering mechanism with Petri nets to improve the resilience of smart grids against cyberattacks. The prompt identification and reaction to cyber threats in smart grids is a major issue that is addressed by the suggested voltage control technique. The impact of cyberattacks on the electricity system is captured in a complete model created using Petri nets, a flexible formalism for modeling system dynamics.

Bartosz Jasiul [5] presents a thorough approach to the development and verification of a formal modeling framework for cyber threats aimed at computer systems in response to the growing sophistication of these attacks. The principal aim is to exhibit that this approach is not only able to generate precise models that mimic the behavior of malware, but also functions as a useful instrument for identifying specific cyber-attacks and providing assistance in putting into place

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802063

efficient defenses. The presence of malware, or malicious software, is a major cybersecurity concern in the modern day. Malware is a major source of cyber threats that target end users and terminals. Using signature-based anti- virus software or matching digital signatures is the traditional method of detecting malware. But the advent of obfuscation techniques has made spyware nearly imperceptible using these conventional methods. As such, there is an increasing need to use more sophisticated techniques, such behavioral analysis, in addition to signature-based approaches. This article's suggested methodology models malware activity using colored Petri nets as the basis.

2.1 EXISTING SYSTEM

Against fraudulent assaults, network intrusion detection systems are essential for cyber security. From a feature standpoint, the network traffic can contain a range of items, including host information, malicious scripts, attack kind, attack reference, and so on. From a network perspective, compared to regular traffic, network traffic could contain an uneven quantity of malicious attacks. A particular attack can be difficult to pinpoint because of complicated features and problems with data imbalance. This research presented an Intrusion Detection System for Imbalanced Network Traffic (IDS-INT) that uses transformer-based transfer learning to overcome these problems. IDS-INT learns feature interactions in both imbalanced data and network feature representation by transformer- based transfer learning. Initially, comprehensive details regarding every kind of assault are acquired via descriptions of network interactions, encompassing details about network nodes, attack types, references, host information, and so forth. Second, using their semantic anchors, the transformer-based transfer learning strategy is designed to learn the detailed feature representation.

III. PROPOSED SYSTEM

The suggested system is a Frothy Disturbance Intrusion Detection System (FIDS) that is intended to meet the unique issues of protecting varied domains connected with the internet, particularly those with limited resource availability and memory and battery capacity. The system is built around a well-designed sensor network that serves as the backbone for deploying the FIDS. The system uses the Ad-hoc On-demand Distance Vector (AODV) routing protocol for efficient communication and includes a lightweight attack detection method that employs a supervised machine learning-based FIDS using the Multivariate correlation analysis algorithm. The system's modules include building the sensor network, producing AODV packets with an emphasis on energy efficiency, identifying permitted and unauthorized ports, and controlling data transfer while checking the correctness of received packets. Simulations demonstrate the proposed system's classification accuracy and detection time, demonstrating its potential to improve application security by efficiently addressing the special restrictions of intrusion detection in resource-constrained contexts.

A. CONSTRUCTING SENSOR NETWORK MODULE

This module creates and organizes the sensor network, which serves as the foundation for the Frothy Disturbance Intrusion Detection System (FIDS). It entails creating the topology, configuring nodes, and implementing communication protocols for the sensor network. The goal is to build a strong and efficient network infrastructure that will facilitate the implementation of the intrusion detection system.

B. AODV PACKET CREATION ENERGY CONSUMPTION MODULE

This module implements the Ad-hoc On-demand Distance Vector (AODV) routing protocol to facilitate communication between sensor network nodes. AODV packets are generated for routing information, and the module tackles energy consumption problems. Energy-efficient solutions are used to improve resource utilization, assuring the sensor nodes' longevity and sustainability.

C. FIND AUTHORIZED AND UN AUTHORIZED PORT

This module distinguishes between authorized and unauthorized ports in the sensor network. It is likely to include a method for monitoring and analyzing network traffic, as well as scanning communication ports for irregularities. Detecting illegal ports is critical for identifying potential security concerns, and this module adds to the system's total intrusion detection capacity.

D. DATA TRANSMISSION AND VERIFICATION RECEIVING

The Valid Packet

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802063

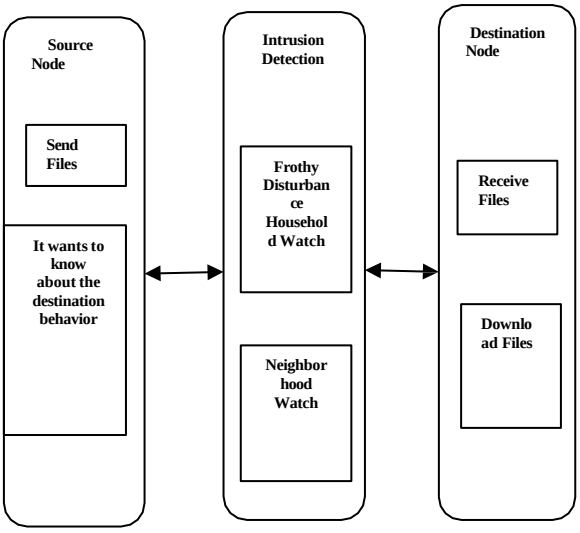

Figure.1. Flow diagram

The data transmission module controls information flow in the sensor network. It entails the transfer of AODV packets and other pertinent information. The verification process guarantees the integrity and authenticity of received packets. This module is expected to use the Multivariate correlation analysis technique indicated in the abstract for successful intrusion detection. Valid packets are processed further, whereas suspicious or unauthorized packets initiate appropriate security steps.

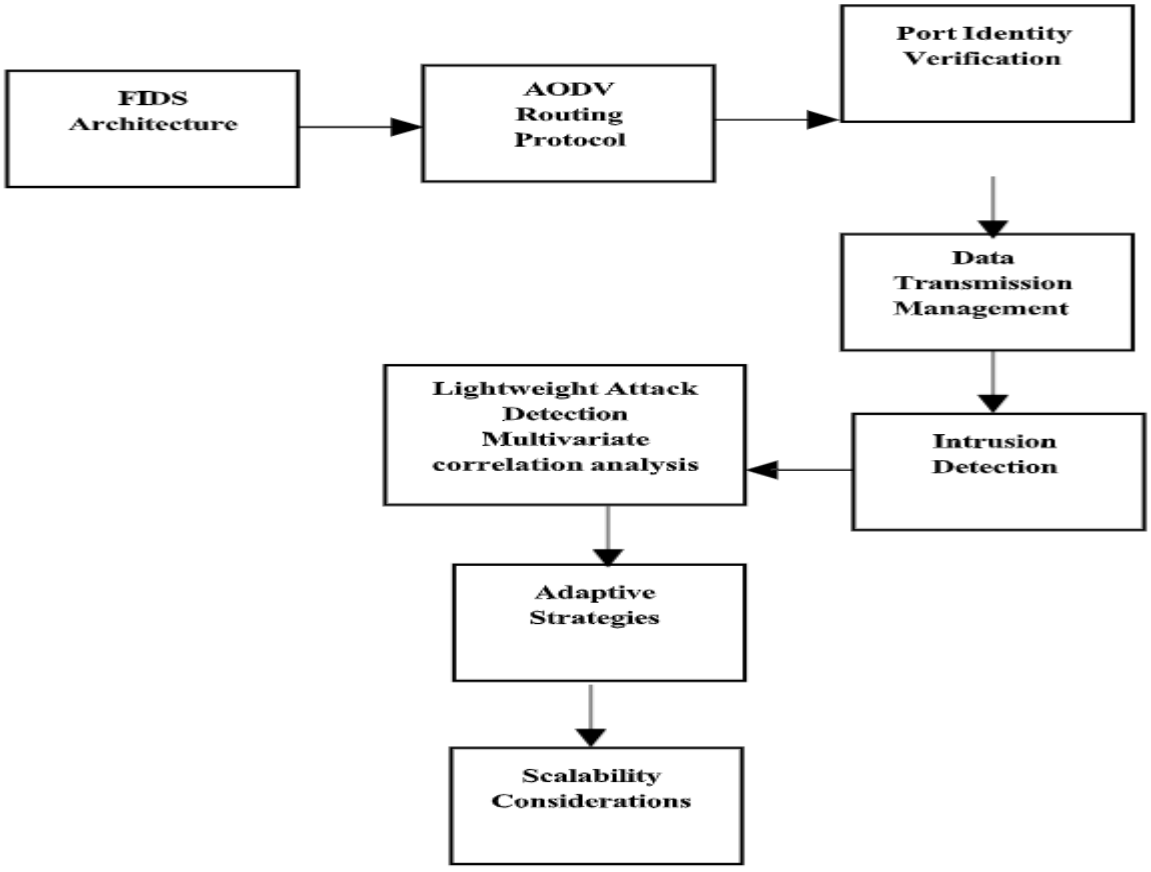

Figure.2. Block diagram

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802063

3.1ALGORITHM DETAILS

A. Multivariate Correlation Analysis

Triangle Area Map Generation module is applied to extract the correlations between two distinct features within each raw/original traffic record coming from the initial step or the traffic record normalized by the " Feature Normalization " module in this step. The occurrence of network intrusions cause changes to these correlations so that the changes can be used as indicators to identify the intrusive activities. All the extracted correlations, namely triangle areas stored in Triangle Area Maps (TAMs), are then used to replace the original basic features or the normalized features to represent the traffic records. This provides higher discriminative information to differentiate between legitimate and illegitimate traffic records.

EVALUATION METRICS

Precision

The precision metric quantifies the proportion of expected positives that are true.

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{F1-score} = \frac{2.\ \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$$

IV. RESULT ANALYSIS

In Multivariate correlation-based denial of service attack detection system based on triangle technique evaluates network traffic dataset for verification of the effectiveness and performance of proposed system The table that follows compares the accuracy of a suggested algorithm with an existing one for the Frothy Disturbance Intrusion Detection System (FIDS) with Support Vector Machine for the Internet of Things (IoT). The recently suggested approach shows a significant improvement with an accuracy of 88%, while the current algorithm only manages a recognition accuracy of 75%. This significant improvement in accuracy highlights the effectiveness of the suggested lightweight attack detection approach, which makes use of signature criteria, supervised machine learning, and anomaly- based detection. Given the resource-constrained IoT devices and different protocol stacks that are addressed in the passage, the suggested model's improved accuracy shows that it has the potential to identify and mitigate security assaults more effectively.

Recall

Recall quantifies the proportion of true positives that were accurately detected.

$$\text{Recall} = \frac{TP}{TP + FN}$$

Table.1. Comparison table

algorithm	accuracy
existing	75
proposed	88

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802063

Accuracy

Accuracy gauges how accurate the model is overall across all classes.

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN}$$

F1-score By balancing Precision and Recall, the F1-score provides a single statistic that takes false positives and false negatives into consideration.

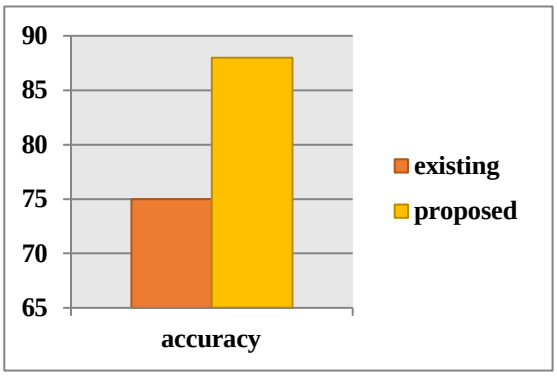

Figure.3. Comparison graph

V. CONCLUSION

To summarize, the created Frothy Disturbance Intrusion Detection System (FIDS) provides a comprehensive solution optimized for safeguarding varied domains integrated with the internet, particularly those confronting resource limits and limited memory and battery capacity. The suggested system efficiently fulfills the special requirements of intrusion detection in resource-constrained contexts by integrating a well-constructed sensor network with a lightweight attack detection method based on the Multivariate correlation analysis algorithm. The simulation results demonstrate the system's efficiency, with remarkable performance in terms of classification accuracy and detection time.

VI. FUTURE WORK

The Frothy Disturbance Intrusion Detection System (FIDS) may be extended and improved in the future. To begin, investigating the integration of alternative machine learning algorithms alongside the Multivariate correlation analysis could provide a comparison analysis to choose the most appropriate method for various scenarios. Furthermore, the system may benefit from scalability considerations to support larger and more complicated sensor networks. Further study could also focus on developing adaptive algorithms that dynamically modify intrusion detection parameters in response to the network's changing features and possible threats.

REFERENCES

1. K. Agarwal and T. Kumar, "Using FPGA and Petri Net to Model and Implement a Smart Home and Self-control Window," at the 2nd International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, 2018.
2. The article "Machine Learning Cyberattack and Defense Strategies" by S. Rajput and A. Arora was published in the International Journal of Computer Applications in 2013.
3. Replay attack detection in smart cities using deep learning, M. Mohamad and A. Selamat, International Conference on Computer, Communications, and Control Technology (I4CT), 2003. 2015 IEEE, pp. 227–231.
4. In the Proceedings of the first instructional conference on machine learning, vol. 242, Piscataway, NJ, 2003, pp. 133–142, J. Ramos et al.discuss a petri net-based voltage control technique under fake data injection attack.
5. Detection and Modeling of Cyber Attacks using Petri Nets, T. Kumaresan and C. Palanisamy, International Journal

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802063

of Bio-Inspired Computation, vol. 9, no. 3, pp. 142–156, 2017. Technologies
6. (NGCT), pp. 516–521, 2016.
7. H. Kaur and S. Ajay, "Efficient Intrusion Detection Algorithms for Smart Cities-Based Wireless Sensing Technologies. In Proceedings of the Joint Conference of the 47th Annual Meeting of the ACL and the 4th International Joint Conference on Natural Language Processing of the AFNLP: Volume 1- Volume 1,
8. K. Toutanova and C. Cherry, "Selection of Effective Machine Learning Algorithm and Bot-IoT Attacks Traffic Identification for Internet of Things In Smart City," page 7–9. 2009, pp. 486–494, Association for Computational Linguistics.
9. A Deep Learning-based IoT-oriented Infrastructure for Secure Smart City, T. N. Sainath,
10. O. Vinyals, A. Senior, and H. Sak, 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 4580–4584 (IEEE, 2015).
11. In the 2012 IEEE Spoken Language Technology Workshop (SLT), T. Mikolov and G. Zweig presented their paper, "Fog Computing for Sustainable Smart Cities in the IoT Era: Caching Techniques and Enabling Technologies - An Overview." 2012 IEEE, pp. 234–239.
12. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
13. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
14. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
15. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
16. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
17. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
18. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
19. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
20. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
21. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
22. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
23. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
24. "A hierarchical colored Petri net–based cyberattacks response strategy making approach for critical infrastructures," Rizky, W. M., Ristu, S., and Afrizal, D. Nov. 2016, Scientific Journal of Informatics, Vol. 3(2), pp. 41–50