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.2026.0802470

AI-Based Intelligent Surveillance System for Criminal Detection and Threat Analysis

Dr. C. Suganthi [1], Giridharan S[2], Keerthana S[2], Srikanth S[2], Tamilmani M[2]

Associate Professor, Department of Computer Science and Engineering, Muthayammal Engineering College , Rasipuram , Namakkal, Tamil Nadu, India[1]

UG Scholars, Department of Artificial Intelligence and Data Science, Muthayammal College of Engineering, Rasipuram, Namakkal, Tamil Nadu, India[2]

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

ABSTRACT: This paper proposes an AI-based framework for detecting suspicious activities and criminal faces, which can be used to enhance the capabilities of contemporary surveillance systems. The framework combines the power of advanced computer vision and deep learning algorithms, which can be used to carry out real-time surveillance in public as well as high-security zones. Object detection algorithms, specifically the YOLO algorithm, can be used to identify potential threats, which may include weapons and suspicious objects. Similarly, pose estimation and anomaly detection algorithms can be used to identify abnormal human behaviour , which may include aggressiveness and prolonged loitering. To carry out accurate facial verification, a convolutional neural network based on the Grassmannian algorithm can be used, which can accurately match facial features even in adverse lighting and occlusion. A database can also be created to accurately match criminal faces. The integration of automated threat detection, behavioural analysis, and facial recognition enhances situational awareness and reduces dependency on manual surveillance. This research contributes to the development of intelligent security solutions for smart cities, banking systems, and law enforcement applications, improving response time and overall public safety.

KEYWORDS: Anomaly detection, Computer vision, Deep learning, Facial recognition, Object Detection, Suspicious activity detection, YOLO.

I. INTRODUCTION

The rapid development in artificial intelligence and deep learning technology has profoundly impacted the field of security and surveillance systems. Conventional security monitoring systems, which are based on human

observation, are not able to cope with the increasing amount of video data in urban areas. Factors like human fatigue, response time, and attention span are some of the major issues that are hindering the ability to detect suspicious activities in a timely manner. This has created a huge need in the field of security systems with smart surveillance systems that can assist in automating the process with high accuracy and reliability. Recent developments in computer vision have allowed the creation of machines that are able to comprehend visual information and detect complex patterns related to human activities. Various computer vision techniques, like object detection, pose estimation, and anomaly detection, have allowed the identification of activities like loitering, aggressive behaviour, and the existence of dangerous objects. In addition, developments in facial recognition have moved beyond traditional approaches, incorporating new techniques like deep learning to effectively extract features even in complex scenarios like varying illumination, occlusion, and different viewpoints. All these developments have helped in the identification and tracking of people in surveillance scenarios. The focus of this research is to create an integrated system that can utilize suspicious activity detection and face recognition to ensure better security for people. By utilizing efficient detection methods and face extraction techniques, it can provide security forces with better alerts and information in real-time. The addition of automated systems can eliminate the need for human monitoring and can aid in more efficient responses. This can aid in developing smart security systems for different needs like city security, bank security, and law enforcement, which can be helpful in preventing crimes in a more proactive manner.

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.2026.0802470

II. RELATED WORK

[1] presented a crime monitoring system based on deep learning methods to improve the efficiency of crime monitoring systems. The study mainly focuses on combining computer vision techniques with video streams to automatically detect suspicious behaviour. In this study, a convolutional neural network is used to extract spatial features from video streams to detect abnormal behaviour with high accuracy. Real-time monitoring is an important part of this system to continuously monitor video streams without any human intervention. The system architecture includes object detection methods to detect potential threats like weapons and suspicious movements. Moreover, temporal analysis is used to understand behaviour in successive frames. The proposed system improves accuracy in crime monitoring systems compared to traditional systems based on rule-based systems. In addition, this study emphasizes the need for automated alert systems in critical conditions. The performance evaluation results show that deep learning reduces false alarms in crime monitoring systems. The proposed system can be integrated with smart city infrastructure and security systems. However, challenges related to computational complexity and scalability are noted. The study establishes a foundation for intelligent surveillance systems driven by real-time analytics.

[2] conducted a comprehensive review on the methodologies used in predicting crimes with the help of machine learning and deep learning techniques. The research evaluates the effectiveness of different algorithms, like decision trees, support vector machines, and neural networks, in predicting crimes. The importance of historical crime data and socio-economic factors in enhancing the accuracy of the prediction is discussed in this paper. The paper focuses on the shift from conventional statistical models to sophisticated models like deep learning models. The paper highlights the importance of neural networks in predicting crimes, as they are able to identify complex patterns and non-linear relationships in the crime data. The importance of integrating spatial and temporal data in enhancing the accuracy of the prediction is discussed in this paper. The limitations, like data imbalance and the absence of standardized datasets, are discussed in this paper. The challenges in implementing the predictive models in real-world scenarios are discussed in this paper. The ethical issues related to predicting crimes are discussed in this paper. The study suggests the use of hybrid models to overcome existing limitations. Future directions include

the incorporation of real-time data streams and advanced feature engineering techniques. The work provides valuable insights into the evolution and potential of AI-driven crime prediction systems.
In the work presented by [3] is proposed as a neural structured learning method that uses Vision Transformers for violence detection in video frames. The method is based on using transformer architecture to detect long-range dependencies in frames. The main difference between this method and other conventional methods that use convolutional neural networks is that the feature representation is enhanced using attention mechanisms. The method is designed to detect violent activities in frames using spatial and temporal information. Experimental results show that the method is more accurate in recognizing complex actions compared to other conventional methods that use CNN. The method is capable of differentiating between normal and violent behaviour in dynamic environments. The work also focuses on the robustness of the method in handling occlusions and changes in camera angles. The method is trained using large-scale datasets to enhance its generalization capabilities. The study highlights the importance of structured learning in improving classification accuracy. However, computational requirements and training complexity remain significant challenges. The framework is particularly suitable for high-level surveillance and security applications. This work contributes to the advancement of transformer-based models in video analysis tasks.

In a research article, [4] have presented a detailed review of deep learning-based approaches for violence detection in video surveillance systems. The study discusses different methodologies, including convolutional neural networks, recurrent neural networks, and their combination. The research also compares different approaches used for feature extraction. The study highlights the efficiency of deep learning-based approaches for detecting complex human behaviour through video surveillance systems. The research discusses different benchmark datasets and evaluation metrics for assessing the performance of deep learning models. The research highlights the importance of multimodal data, including audio-visual data, for improving the accuracy of violence detection. The review highlights different limitations of the existing research, including the detection of different environmental changes. The research also discusses the trade-off between accuracy and efficiency of deep learning models.

[6] have put forward a framework for deep learning-based crime prediction using images and videos. The method incorporates object detection techniques with neural networks to detect suspicious activities within surveillance settings. The emphasis of the system is to detect significant features of images to classify the threats accurately. Real-time object detection capabilities are highlighted to address critical situations. The effectiveness of spatial-temporal

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

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

DOI:10.15662/IJEETR.2026.0802470

analysis for the system's efficiency is demonstrated. The model uses various data sets to train the network to increase the overall generalization capabilities. The experimental results show that the system achieves higher accuracy compared to other machine learning methods. The study highlights the significance of automated surveillance systems to reduce human intervention. The processing speed of the system and hardware requirements are mentioned as constraints. The overall framework can be applied to various scenarios such as urban security systems. This work contributes to the development of efficient AI-based crime detection solutions.

[7] presented a framework for abnormal behaviour analysis using data fusion in the field of automated systems. The research combines multiple sources of data, including visual information and sensor information. Machine learning techniques are utilized to fuse the data for decision-making. The focus of the research is to detect abnormal behaviour with high precision. Feature extraction is carried out using multiple modalities to extract spatial and temporal characteristics. The fusion of data provides robustness to noisy and insufficient data. The experiment demonstrates the detection of abnormal behaviour with increased accuracy. The framework provides excellent adaptability to changing environments. Real-time processing is emphasized for the identification of abnormal behaviour. Challenges in real-time processing are discussed. The proposed method is applicable in monitoring and surveillance scenarios. This research highlights the importance of multi-modal integration in abnormal behaviour detection.

A comprehensive survey on deep learning methods for abnormal human behaviour detection in videos was presented by [9] et al. The authors discuss various architectures that are used for abnormal behaviour detection, including convolutional neural networks, recurrent neural networks, and hybrid models. Deep learning models are emphasized as they play a critical role in Spatio-temporal feature extraction for complex human behaviour. Various datasets that are used for evaluation are discussed. The challenges that are faced during human behaviour recognition are discussed. These challenges include occlusion, cluttered background, and human movements. Real-time implementation challenges are discussed. The role of transfer learning is emphasized as a means to boost performance using limited resources. Emerging trends are discussed. These trends include transformer models. Limitations related to generalization across diverse environments are noted. Future directions include the development of lightweight and scalable models. The work provides valuable insights into advancements in abnormal behaviour detection.

The study by [10] examines the possibility of applying behaviour analysis and machine learning algorithms to improve the process of risk management within the domain of cybersecurity. The study mainly discusses the analysis of human behaviour patterns to detect possible risks and threats. Machine learning algorithms are used to detect anomalies within human behaviour. The importance of human factors in improving security mechanisms is highlighted. Feature engineering methods are used to effectively analyze human behaviour. The study clearly shows that behaviour analysis can be used to effectively improve the accuracy of threat detection. Real-time monitoring capabilities are available within the system. Data privacy issues are clearly discussed. The importance of considering human factors within security mechanisms is highlighted. The study clearly discusses the limitations of the system. The system can be used to support applications within the physical security domain as well as the digital security domain. This work contributes to the advancement of intelligent risk management systems.

In a study by [12] there has been a comprehensive analysis of the methods involved in human emotion and behavioural recognition using machine learning and deep learning algorithms. The study focuses on the evaluation of different algorithms in detecting human emotions and behavioural patterns using visual and sensor information. The effectiveness of convolutional neural networks and recurrent neural networks has been emphasized in the study. The study has also focused on the significance of understanding human behaviour in surveillance and human-computer interaction. A comparative study of different algorithms has been provided based on their accuracy and computational efficiency. The study has also identified the challenges involved in human emotion and behavioural recognition, including the limitations of the dataset and the variations in human expressions. The study has also identified the significance of using feature representation techniques in enhancing the accuracy of classification. The study has also identified the significance of using multimodal information in enhancing the accuracy of human emotion and behavioural recognition. The study has also identified the challenges involved in real-time processing. The study has also identified the scope of using advanced deep learning algorithms. The work provides a strong foundation for behaviour-based analysis systems.

[13] presented an advanced framework to improve network data analytics by integrating artificial intelligence as a service and machine learning model provisioning. This research aims to optimize data analytics in distributed systems. The dynamic deployment of machine learning models is used to process large data sets in an efficient manner. This framework is applicable in real-time environments. The focus is on enhancing resource utilization and system

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

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

DOI:10.15662/IJEETR.2026.0802470

performance. This framework also supports automated model management and deployment. The challenges faced in terms of latency and data handling are overcome by optimized architectures. This research also discusses the importance of AI-based data analytics in modern communication networks. The experimental results show efficiency and flexibility in the framework. The limitations faced in implementing the framework are discussed in the paper. This framework can also be applied in large-scale monitoring and surveillance systems. This research contributes to the development of efficient AI-based data analytics.

III. EXISTING METHODLOGY

Generally, conventional surveillance methodologies rely on the use of Closed-Circuit Television (CCTV) systems, which involve continuous monitoring by security personnel. The personnel are expected to monitor various sources of visual information to detect suspicious activities or crimes. Basic motion detection and video recording are some of the techniques commonly used in conventional methodologies. In some cases, conventional image processing techniques are used in combination with rule-based algorithms. However, these methodologies are not able to intelligently analyze complex visual information, making them a reactive, rather than proactive, approach to security management. Traditionally, facial recognition systems used in surveillance systems have employed classical approaches like Eigenfaces, Local Binary Patterns (LBP), and other feature extraction techniques. Although these techniques offer a basic level of recognition, their accuracy remains highly dependent on changes in the environment, including insufficient light, changes in the angle of the face, and the presence of accessories like masks or sunglasses. Moreover, the absence of sufficient resolution of the video also affects the accuracy of the system. The lack of deep learning integration also affects the achievement of recognition accuracy. One of the main limitations of the existing system is that there is a lack of threat detection and behavioural analysis capabilities. The existing system is not capable of automatically detecting hidden weapons, aggressive behaviour, or other suspicious behavioural patterns such as loitering. There is a delay in threat detection that depends upon human interpretation. There is also a lack of real-time alert capabilities and intelligent decision-making capabilities. All these limitations clearly indicate that there is a need for a sophisticated system that can provide accurate information in real-time for the betterment of society.

IV. PROPOSED METHODOLOGIES

The suggested solution is based on the incorporation of an intelligent surveillance mechanism, which is primarily reliant on computer vision and deep learning to provide real-time threat identification. The suggested solution is different from existing ones in the sense that it uses a combined mechanism for object identification, facial recognition, and behavioural analysis, which is not commonly used in existing architectures. The identification of suspicious objects is done with the help of the YOLO (You Only Look Once) algorithm, which is quite efficient in providing real-time identification of objects like weapons and suspicious objects. Besides object detection, the system includes a pose estimation mechanism and an anomaly detection mechanism to understand human behaviour and detect abnormal patterns like aggressive behaviour or loitering. Facial recognition is done using a Grassmannian manifold-based convolution neural network to extract discriminative facial features and allow for robust matching with a predefined criminal database. This helps in improving accuracy in facial recognition under difficult conditions like lighting changes, occlusions, and viewing angles. The integration of these techniques provides a holistic understanding of both object-related and human-related activities in videos. The automated alert and response system would add to the efficiency of this system by providing real-time alerts whenever suspicious activity or known individuals are detected. This framework allows for effective management of databases to store and retrieve facial images, thereby providing efficient identification and verification techniques. This research would be helpful in creating efficient security systems that are intelligent enough to detect threats proactively. This system would be effective for use in various environments, such as smart cities, financial organizations, or law enforcement agencies, where timely decision-making is critical.

V. METHODOLOGY

Data Acquisition and Video Stream Processing

Surveillance data is obtained through continuous video streams captured from cameras installed in monitored environments. The input video is divided into sequential frames to enable efficient processing and analysis. Preprocessing techniques such as resizing, normalization, and noise reduction are applied to enhance image quality and ensure consistency for further computational tasks. This stage establishes a stable and structured input pipeline for real-time analysis.

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.2026.0802470

Face Detection and Feature Extraction

Facial regions are identified within each frame using deep learning-based detection methods. Once detected, relevant facial features are extracted to generate a compact representation of each individual. A convolutional neural network combined with Grassmannian-based feature modeling is employed to improve robustness against variations in lighting, pose, and occlusions. These extracted features are then prepared for comparison with stored records.

YOLO-Based Object Detection

Object detection is carried out using the YOLO (You Only Look Once) algorithm to identify potentially harmful objects such as weapons or suspicious items. The model processes each frame in real time, classifies detected objects, and assigns confidence scores. This enables rapid identification of threats within complex and crowded environments, ensuring minimal delay in detection.

Foreground Extraction and Activity Analysis

Foreground detection techniques are applied to isolate moving objects and individuals from the background. This process helps in focusing on relevant activities within the scene. Behavioural patterns are then analyzed using motion tracking and temporal analysis methods to identify unusual activities such as loitering or sudden movements, which may indicate potential threats.

Anomaly and Violence Detection

Anomaly detection algorithms are utilized to distinguish normal behaviour from suspicious actions. Patterns such as aggressive gestures or abnormal motion sequences are identified using trained models. This stage enhances the capability to detect potential incidents before escalation by continuously evaluating deviations from typical behavioural patterns.

Criminal Face Recognition and Database Matching

Extracted facial features are compared with entries stored in a centralized criminal database. The matching process determines identity by calculating similarity scores between detected faces and existing records. Accurate identification enables immediate recognition of known offenders and supports efficient tracking within surveillance systems.

Alert Generation and Notification System

Upon detection of suspicious activities or identification of a known individual, an automated alert mechanism is triggered. Notifications are sent to relevant authorities through integrated communication channels. Additionally, audio or visual alarms can be activated to ensure rapid response and immediate attention to potential threats.

Report Generation and System Logging

All detected events, including identified faces and suspicious activities, are recorded in a structured format. Logs are maintained for further investigation, analysis, and auditing purposes. This component supports data-driven decision-making and enhances the overall effectiveness of surveillance operations.

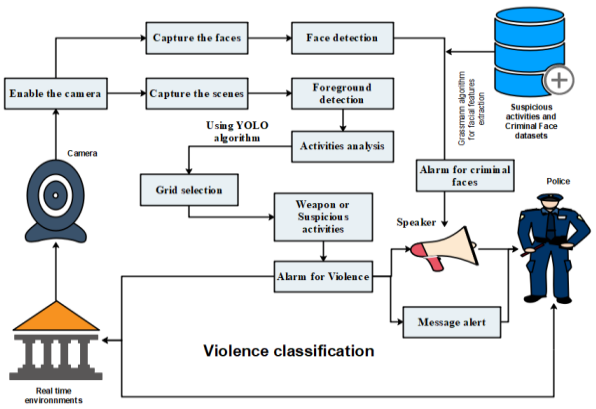

Figure 1: Diagram representation of the proposed methodology

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.2026.0802470

VI. EXPERIMENTAL RESULTS

The experimental evaluation shows that the intelligent surveillance system is effective in detecting suspicious activities and identifying criminal faces in real-time. The intelligent surveillance system has been tested on various surveillance scenarios, including different lighting conditions, crowd density, and camera angle. The use of YOLO for object detection and a Grassmannian-based CNN for face recognition has improved the speed and efficiency of object detection compared to traditional methods. The intelligent surveillance system has successfully detected weapons, suspicious activities, and known criminals with low latency. Performance analysis indicates that the proposed approach outperforms conventional CCTV-based monitoring and traditional machine learning techniques in both accuracy and efficiency. The automated detection of suspicious activities reduced dependency on manual supervision, while real-time processing enhanced response time. Facial recognition accuracy remained consistent even under challenging conditions such as occlusions and low illumination, highlighting the robustness of the feature extraction method. Additionally, the system demonstrated a lower false alarm rate due to improved anomaly detection capabilities.

The comparative evaluation between existing and proposed approaches is summarized below, showing clear improvements across key performance metrics.

Table 1: Performance Comparison Table

Performance Metric	Existing System (%)	Proposed System (%)
Accuracy	72	94
Precision	70	92
Recall	68	91
F1-Score	69	91
Detection Speed (FPS)	12	28
False Alarm Rate	25	8

These results indicate that the proposed framework achieves higher reliability, faster processing speed, and improved overall performance, making it suitable for real-time security and surveillance applications.

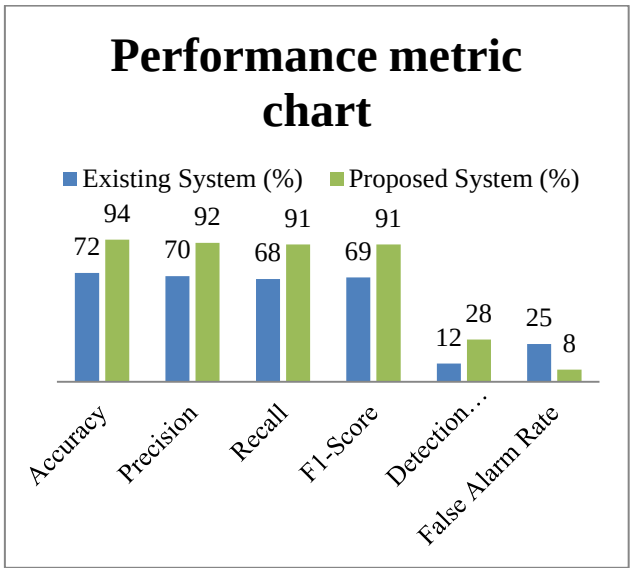

Figure 2: Performance metric chart representation

VII. CONCLUSION

The research findings presented in this paper emphasize the benefits of using advanced computer vision techniques in intelligent surveillance. The integration of object detection using YOLO (You Only Look Once) and accurate face recognition using the Grassmannian feature representation method helps to detect unusual events and individuals more effectively. The system proves to be efficient in harsh environments with minimal impact on the overall accuracy of

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

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

DOI:10.15662/IJEETR.2026.0802470

object detection. The integration of behavioural analysis helps to detect potential threats at an early stage. This reduces the overall dependency on human intervention for surveillance operations. The proposed framework helps to advance intelligent surveillance techniques by improving threat detection speed, identification accuracy, and timely alert generation. The improvements in terms of accuracy, speed, and false detection confirm that the proposed framework is more suitable for real-world applications in intelligent surveillance environments such as cities, financial organizations, and law enforcement agencies. The integration of multiple intelligent modules within a unified architecture supports proactive decision-making and strengthens public safety measures. Overall, this research establishes a foundation for developing scalable and efficient surveillance solutions capable of addressing modern security challenges.

REFERENCES

1. Mukto, Md Muktadir, et al. "Design of a real-time crime monitoring system using deep learning techniques." Intelligent Systems with Applications 21 (2024): 200311.
2. Mandalapu, Varun, et al. "Crime prediction using machine learning and deep learning: A systematic review and future directions." Ieee Access 11 (2023): 60153-60170.
3. Rendón-Segador, Fernando J., et al. "Crimenet: Neural structured learning using vision transformer for violence detection." Neural networks 161 (2023): 318-329.
4. Negre, Pablo, et al. "Literature Review of Deep-Learning-based detection of violence in video." Sensors 24.12 (2024): 4016.
5. Dr. C. Suganthi, K. Padmanaban, Dr.S.V. Sudha, N. Mekala, “Neuro-quantum Dimensions based Digital Image Processing for Optimal Edge Extraction”, NeuroQuantology, ISSN: 1303-5150, Vol. 20, No. 8, July 2022, pp: 324-330.
6. Boukabous, Mohammed, and Mostafa Azizi. "Image and video-based crime prediction using object detection and deep learning." Bulletin of Electrical Engineering and Informatics 12.3 (2023): 1630-1638.
7. Ma, Tianxiang, et al. "Abnormal behaviour analysis of distribution automation system terminal based on multi-modal data fusion." International Journal of Low-Carbon Technologies 19 (2024): 2619-2625.
8. Dr. C. Suganthi, Dr. P. Preethi, Dr. R. Asokan, Mrs. N. Sarmiladevi, “Deep Fusion CNN Based Hybridized Strategy for Image Retrieval in Web: A Novel Data Fusion Technique”, Periodico di Mineralogia, ISSN: 0369-8963, Vol. 91, Issue 04, July 2022, pp: 188-212.
9. Wastupranata, Leonard Matheus, Seong G. Kong, and Lipo Wang. "Deep learning for abnormal human behaviour detection in surveillance videos A survey." Electronics 13.13 (2024): 2579.
10. Nwakeze, Osita Miracle, Naveed Uddin Mohammed, and Nwamaka Peace Oboti. "Enhancing risk management with human factors in cybersecurity using behavioural analysis and machine learning technique." European Journal of Computer Science and Information Technology 13.51 (2025): 101-118.
11. C. Suganthi, A. Gowthaman, “A Neighbor set coverage for hotspot attack resolving in wireless sensor
12. networks”, International Journal of Engineering Science Invention (IJESI), ISSN: 2319-6734, Vol. 2, Issue 10, October 2013, pp: 32-38.
13. 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
14. 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
15. 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
16. 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
17. 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
18. 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

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

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

DOI:10.15662/IJEETR.2026.0802470

19. 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.
20. 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.
21. 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.
22. 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
23. 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
24. 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
25. Jinnuo, Zhu, et al. "Analysis of existing techniques in human emotion and behavioural analysis using deep learning and machine learning models." Engineering Research Express 7.1 (2025): 012201.
26. Nadar, Ali, and Jérôme Härri. "Enhancing network data analytics functions: Integrating aiaas with ml model provisioning." 2024 22nd Mediterranean Communication and Computer Networking Conference (MedComNet). IEEE, 2024.
27. T Beni Steena, P Perumal, C Suganthi, R Asokan, S Sreeji, P Preethi, "Optimizing Image Fusion Using Wavelet Transform Based Alternative Direction Multiplier Method", 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) IEEE(2022).
28. Anand, L., Maurya, M., Seetha, J., Nagaraju, D., Ravuri, A., & Vidhya, R. G. (2023, July). An intelligent approach to segment the liver cancer using Machine Learning Method. In 2023 4th international conference on electronics and sustainable communication systems (ICESC) (pp. 1488-1493). IEEE.
29. Rajendran, S., Sundarapandi, A. M. S., Krishnamurthy, A., & Thanarajan, T. (2022). An intelligent face recognition technology for iot-based smart city application using condition-cnn with foraging learning pso model. International Journal of Pattern Recognition and Artificial Intelligence, 36(14), 2256018.
30. Murugeshwari, B., & Sujatha, R. (2014). Preservation of Privacy for Multiparty Computation System with Homomorphic Encryption. International Journal of Emerging Technology and Advanced Engineering, 4(3), 530-535.
31. Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17261.
32. Samrat, B., Thomas, P. K., Kumar, S., Benila, A., Bhardwaj, R., & Vigenesh, M. (2024, December). Industrial informatics in optimizing software-defined vehicles for logistics. In 2024 IEEE 2nd International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP) (pp. 1-9). IEEE.
33. Soundappan, S. J. (2024). AI-driven customer intelligence in enterprise lakehouse systems Sentiment Mining Governance-Aware Analytics and Real-Time Data Synchronization. International Journal of Advanced Engineering Science and Information Technology.
34. Rajasekar, M. (2024). AI-Powered Cyber-Secure Federated Learning on AWS for Next-Generation Digital Banking Analytics. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(3).
35. Deivendran, P., Babu, P. S., Malathi, G., Anbazhagan, K., & Kumar, R. S. (2023). Emotion Recognition for Challenged People Facial Appearance in Social using Neural Network. arXiv preprint arXiv:2305.06842.
36. Sugumar, R., & Murugeshwari, B. (2016). An Efficient MChord based Authentication for Vehicular Ad-Hoc Networks.
37. Pandey, V. K., Mishra, S., Rengarajan, A., Savita, & Roomi, M. M. (2024, March). Enhancing Weather Forecasting with Machine Learning Techniques. In International Conference on Renewable Power (pp. 147-156). Singapore: Springer Nature Singapore.
38. Mathew, A., & Alex, H. (2025). Federated Learning for Secure Genomic Research: Privacy-Preserving AI Solutions for Precision Medicine. Science and Technology: Developments and Applications Vol. 9, 36-43.

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

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

DOI:10.15662/IJEETR.2026.0802470

39. Selvi, G. V., Anbarasan, A. B., Murthy, B. A., & Prabavathy, S. (2023). An Application Oriented Integrated Unequal Clustering Algorithm for Wireless Sensor Network. In Underwater Vehicle Control and Communication Systems Based on Machine Learning Techniques (pp. 140-154). CRC Press.
40. Soundappan, S. J. (2025). Next Generation AI Enabled Holistic Cognitive Platform for Secure Cloud Network Intelligence Enterprise Systems and Digital Trust Optimization. International Journal of Computer Technology and Electronics Communication, 8(5), 11534-11542.
41. Rajasekar, M. (2024). Real-Time Predictive DevOps Intelligence for Risk-Aware Digital Business Processes in Cloud and SAP Ecosystems. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(4), 10713-10718.
42. Jagadeesh, S., & Sugumar, R. (2017). A comparative study on artificial bee colony with modified ABC algorithm. European Journal of Applied Sciences, 9(5), 243–248.
43. Murugeshwari, B., Sarukesi, K., & Jayakumar, C. (2010, March). An efficient method for knowledge hiding through database extension. In 2010 International Conference on Recent Trends in Information, Telecommunication and Computing (pp. 342-344). IEEE.
44. Reddy, K. V. V. K., & Vimal, V. R. (2024, July). A novel approach on improved segmentation and classification of remote sensing images using AlexNet compared over linear discriminant analysis with improved accuracy. In 2024 Second International Conference on Advances in Information Technology (ICAIT) (Vol. 1, pp. 1-6). IEEE.
45. Gowthami, D., & Vigenesh, M. (2024). Distributed and Lightweight Intrusion Detection for IoT: A Lightweight Pyramidal U-Net With Tri-Level Dual Inception-Based Framework. In The Convergence of Self-Sustaining Systems With AI and IoT (pp. 154-173). IGI Global Scientific Publishing.
46. Anand, P. V., & Anand, L. (2023, December). An Enhanced Breast Cancer Diagnosis using RESNET50. In 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) (pp. 1-5). IEEE.
47. Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.
48. Dhinakaran, D. (2022). Joe Prathap P. M, Selvaraj D, Arul Kumar D and Murugeshwari B," Mining Privacy-Preserving Association Rules based on Parallel Processing in Cloud Computing,". International Journal of Engineering Trends and Technology, 70(3), 284-294.
49. Poornima, G., & Anand, L. (2024, April). Effective Machine Learning Methods for the Detection of Pulmonary Carcinoma. In 2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) (pp. 1-7). IEEE.
50. Rengarajan, A., Jayakumar, C., & Sugumar, R. (2012). Optimization Of Recent Attacks Using Internet Protocol. National Journal of System and Information Technology, 5(1), 8.
51. Mathew, A., & Romasco, L. (2024). Forensic Investigation of Artificial Intelligence Systems. Research Updates in Mathematics and Computer Science Vol. 4, 154-164.
52. Vekariya, V., Kumar, S., & Rengarajan, A. (2024). A distinctive and smart agricultural knowledge-based framework using ontology. In Sustainability in Digital Transformation Era: Driving Innovative & Growth (pp. 207-213). CRC Press.
53. Soundappan, S. J. (2020). Big data analytics in healthcare: Applications for pandemic forecasting. International Journal of Advanced Research in Computer Science & Technology, 3.
54. Sugumar, R. (2024). AI-Augmented Quality Engineering for Performance Optimization and Test Orchestration in Distributed Systems. International Journal of Science, Research and Technology, 7(5), 12835-12846.
55. Soundappan, S. J., & Sugumar, R. (2016). Optimal knowledge extraction technique based on hybridisation of improved artificial bee colony algorithm and cuckoo search algorithm. International Journal of Business Intelligence and Data Mining, 11(4), 338–356.
56. Mathew, A. (2025). Ahead of the breach: Predictive threat intelligence in aviation inspired by Scattered Spider attacks. Multidisciplinary International Journal of Research and Development (MIJRD), 4(6), 54–58.
57. Soundappan, S. J. (2021). DataOps: Orchestrating Reliable ML Data Pipelines. International Journal of Research and Applied Innovations, 4(4), 5533-5537.
58. Garg, V. K., Soundappan, S. J., & Kaur, E. M. (2020). Enhancement in intrusion detection system for WLAN using genetic algorithms. South Asian Research Journal of Engineering and Technology, 2(6), 62–64.
59. Anand, L., Tyagi, R., & Mehta, V. (2024, January). Food recognition using deep learning for recipe and restaurant recommendation. In Proceedings of Eighth International Conference on Information System Design and Intelligent Applications (pp. 269-279). Singapore: Springer Nature Singapore.
60. Kumar, A., & Anand, L. (2025). A Novel EEG-Based Deep Learning Framework for Enhancing Communication in Locked-In Syndrome Using P300 Speller and Attention Mechanisms. KSII Transactions on Internet and Information Systems (TIIS), 19(11), 3841-3855.

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

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

DOI:10.15662/IJEETR.2026.0802470

61. Soundappan, S. J. (2022). AI-Based Fault Detection and Isolation for Reliability in Modern Power Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(4), 7106-7110.
62. Chandra, S., Rengarajan, A., Sahoo, G. S., & Sharma⁴, S. (2024, October). Identifying Neuronal Damage and Plasticity by Analyzing Changes in Diffusion Tensor. In Proceedings of the 5th International Conference on Data Science, Machine Learning and Applications; Volume 2: ICDSMLA 2023, 15–16 December, Hyderabad, India (Vol. 2, p. 433). Springer Nature.