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.2026.0802378

Deft-IP: Decoy Enhanced Framework for Threat Protection in Intellectual Property

K.Susila Rani[1], Dr.M.Tamilselvi[2]

M.E., Department of Computer Science and Engineering – Roever Engineering College, Perambalur, Tamil Nadu, India[1]

Associate Professor, Department of CSE, Roever Engineering College, Perambalur, Tamil Nadu, India[2]

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

ABSTRACT: Intellectual Property (IP) represents a critical asset for modern organizations, encompassing sensitive information such as proprietary designs, research data, and strategic knowledge. With the rapid advancement of cyber technologies, IP repositories have become prime targets for sophisticated attacks, particularly automated data extraction methods that utilize machine learning techniques for document classification and topic modeling. Traditional security mechanisms, while effective at restricting access, often fail to prevent intelligent adversaries from analyzing and inferring valuable information once access is obtained.

To address this challenge, this paper proposes DEFT-IP (Decoy Enhanced Framework for Threat Protection in Intellectual Property), an intelligent and proactive defense system designed to safeguard sensitive documents. The framework employs a Variational Autoencoder (VAE) to monitor user behavior and detect anomalies indicative of potential threats. Upon identifying suspicious activity, the system dynamically generates decoy documents by manipulating content through keyword shuffling, topic alteration, and controlled data modification.

The proposed system integrates advanced Natural Language Processing (NLP) techniques, including TF-IDF, K-Means clustering, and Latent Dirichlet Allocation (LDA), to create semantically plausible yet misleading data. This approach disrupts automated analysis tools used by attackers while preserving seamless access for legitimate users. Experimental outcomes demonstrate that DEFT-IP significantly enhances the confidentiality, robustness, and resilience of intellectual property systems against emerging cyber threats, offering a novel direction for intelligent data protection.

KEYWORDS: Intellectual Property (IP), Cyber security, Decoy-Based Defense, Variational Auto encoder (VAE), Natural Language Processing (NLP), TF-IDF, K-Means Clustering, Latent Dirichlet Allocation (LDA), Anomaly Detection, Data Protection

I. INTRODUCTION

In the contemporary digital era, Intellectual Property (IP) has emerged as one of the most valuable assets for organizations, encompassing proprietary research, innovative designs, trade secrets, and strategic knowledge. The increasing reliance on digital storage and collaborative platforms has significantly improved accessibility and productivity; however, it has also exposed sensitive information to a wide range of cyber threats. Among these, automated intellectual property theft—driven by advanced data mining and machine learning techniques—poses a critical challenge to traditional security frameworks.

Conventional security mechanisms such as encryption and access control, while essential, are often insufficient against sophisticated adversaries who exploit automated document classification and topic modeling techniques to extract meaningful insights from large repositories of data. These attacks are particularly concerning because they can operate silently, bypassing detection while systematically identifying and exfiltrating valuable information.

To address these limitations, this work introduces DEFT-IP (Decoy Enhanced Framework for Threat Protection in Intellectual Property), a novel and intelligent defense mechanism designed to safeguard sensitive documents by actively disrupting adversarial analysis. Unlike passive security approaches, DEFT-IP adopts a proactive strategy that combines anomaly detection with deception techniques to both identify and mislead potential attackers.The proposed framework utilizes a Variational Autoencoder (VAE) to monitor user access patterns and detect anomalies indicative of malicious

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

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

DOI:10.15662/IJEETR.2026.0802378

behavior. Upon identifying suspicious activity, the system dynamically generates decoy documents that resemble legitimate data but contain strategically modified content. These decoys are designed to interfere with automated extraction processes by altering keywords, restructuring topics, and injecting misleading information.

To enhance the effectiveness of deception, DEFT-IP integrates Natural Language Processing (NLP) techniques, including Term Frequency–Inverse Document Frequency (TF-IDF), K-Means clustering, and Latent Dirichlet Allocation (LDA). These methods enable the system to manipulate document semantics in a way that confuses adversarial models while preserving the integrity and accessibility of original documents for authorized users.Furthermore, the framework incorporates a secure access architecture that ensures legitimate users can retrieve authentic information without disruption. By combining anomaly detection, intelligent decoy generation, and secure access control, DEFT-IP represents a significant advancement over traditional IP protection strategies.Overall, this research contributes to the field of cybersecurity by introducing a resilient and adaptive approach to intellectual property protection, capable of countering emerging threats posed by automated and intelligent attack systems.

II. LITERATURE SURVEY

Decoy-based cybersecurity has emerged as an effective approach to mitigate insider threats and unauthorized data access. One of the foundational works in this domain is the study by Voris et al., which introduced the concept of generating decoy documents using automated translation techniques. The authors proposed that translating sensitive documents into different languages can produce realistic yet misleading versions that retain structural characteristics while distorting semantic meaning. This approach significantly reduces content similarity and increases the difficulty for automated systems to distinguish between real and fake data. The study also emphasized key design principles such as believability, detectability, and variability to ensure effective deception. However, the method faced limitations related to translation inconsistencies and lack of large-scale real-world validation.

Building upon the concept of deception, Taofeek et al. proposed a cognitive deception model aimed at preventing data exfiltration in enterprise environments. Their approach dynamically generates fake documents based on user behavior and contextual information. By integrating behavioral analytics and natural language generation, the system produces decoys that closely resemble genuine data. Experimental results demonstrated that such deception techniques significantly delay attackers and reduce the likelihood of successful data theft. Despite its effectiveness, the approach introduces computational overhead and challenges in maintaining scalability across large systems.

In another significant contribution, Park et al. developed a secure cyber deception architecture incorporating dynamic decoy injection mechanisms. The system consists of monitoring, deception, and response layers, where suspicious user activities trigger the insertion of decoy data into accessible environments. This real-time injection strategy increases the probability of attacker interaction with deceptive content while enabling efficient tracking and analysis of malicious behavior. The study highlights the effectiveness of integrating behavioral monitoring with adaptive deception, though it requires careful design to avoid interference with legitimate users.

Further research by Ferguson-Walter et al. explored the psychological aspects of cyber deception, emphasizing how attacker perception and decision-making influence the effectiveness of decoy systems. The study demonstrated that both technical and psychologically appealing decoys significantly increase attacker cognitive load, delay malicious actions, and improve detection capabilities. The findings suggest that combining behavioral insights with technical mechanisms leads to more robust and adaptive defense strategies. However, the effectiveness of such approaches depends on continuous adaptation and variability in decoy design.

More recently, Zambianco et al. introduced a proactive decoy selection framework based on the MITRE ATT&CK model. Their approach leverages predictive analytics to determine optimal decoy placement based on anticipated attacker behavior. By dynamically selecting high-impact decoys, the system improves detection rates and resource efficiency compared to static deployment methods. The inclusion of feedback mechanisms allows the system to learn from attacker interactions and refine its strategy over time, making it more adaptive and intelligent.

These studies collectively highlight the growing importance of deception-based security mechanisms in modern cybersecurity. While existing approaches demonstrate significant improvements in threat detection and mitigation, many rely on static or partially adaptive techniques. The proposed DEFT-IP framework addresses these limitations by integrating anomaly detection using Variational Autoencoders with advanced natural language processing techniques such as TF-IDF, K-Means clustering, and Latent Dirichlet Allocation. This combination enables dynamic, intelligent,

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

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

DOI:10.15662/IJEETR.2026.0802378

and context-aware decoy generation, providing a more robust and proactive solution for protecting intellectual property against sophisticated cyber threats.

III. RESEARCH METHODOLOGY

The proposed DEFT-IP framework integrates anomaly detection, natural language processing, and deception strategies to protect intellectual property. The system identifies adversarial behavior and responds proactively by generating misleading content, ensuring both detection and disruption of unauthorized data extraction.The framework employs secure authentication and role-based access control, while continuously monitoring user activities such as login behavior and document access patterns. A Variational Autoencoder (VAE) is used to model normal behavior and detect anomalies based on deviations.

Upon detection, a deception mechanism generates decoy documents using keyword manipulation and topic alteration. These documents are further processed using NLP techniques such as TF-IDF, K-Means clustering, and Latent Dirichlet Allocation (LDA), ensuring misleading analytical outputs. Legitimate users receive original content, while adversaries are served altered data, and administrators are notified through real-time alerts.

A.Algorithms and Techniques: The DEFT-IP framework utilizes a combination of machine learning and natural language processing techniques to detect and mitigate adversarial activities. A Variational Autoencoder (VAE) is employed as an unsupervised model to learn normal user behavior patterns through encoding and decoding processes. It detects anomalies by measuring reconstruction error, where higher deviations indicate suspicious activity. The objective function of VAE is defined as:

$$L=Eq(z|x)[\log p(x|z)]-DKL(q(z|x)\|p(z)) \quad (1)$$

TF-IDF is used to evaluate the importance of terms within documents, enabling effective keyword manipulation for deception. It is defined as:

$$TF\text{-}IDF(t,d)=TF(t,d)\times IDF(t)$$

$$IDF(t)=\log(Ndf(t))IDF(t) = \log \left(\frac{N}{df(t)}\right)IDF(t)=\log(df(t)N) \quad (2)$$

K-Means clustering is used to group documents based on similarity in feature space. The objective function minimizes the distance between data points and their respective cluster centroids:

$$J=i=1\sum kx\in Ci\sum\|x-\mu i\|2 \quad (3)$$

Latent Dirichlet Allocation (LDA) is used for topic modeling, where documents are represented as mixtures of topics and topics as distributions over words. The probability distribution is expressed as:

$$P(w)=z\sum P(w|z)P(z|d) \quad (4)$$

These techniques collectively enable the system to detect anomalies, manipulate document features, and generate misleading outputs that effectively disrupt adversarial analysis.

B. System Workflow and Security Mechanism: The DEFT-IP framework operates through a structured workflow that begins with secure user authentication and role-based access control to ensure authorized access to intellectual property. User activities, including login patterns and document interactions, are continuously monitored and recorded to establish behavioral profiles. A Variational Autoencoder (VAE) analyzes this data to detect anomalies by identifying deviations from normal patterns. Upon detecting suspicious behavior, a deception mechanism is activated, allowing the system to mislead adversaries without restricting access. Decoy documents are generated through manipulation techniques such as keyword alteration and topic modification, which distort the semantic meaning of the content. These manipulated documents are further processed using Natural Language Processing techniques, including TF-IDF, K-Means clustering, and Latent Dirichlet Allocation (LDA), to produce misleading analytical outputs. Finally, legitimate users receive original documents, while adversaries are served altered content, and real-time alerts are sent to administrators for monitoring and response.

C. Decoy Generation Strategy: The decoy generation strategy is a core component of the DEFT-IP framework, designed to mislead adversaries through controlled document manipulation. This approach includes techniques such as keyword shuffling, keyword injection, content reduction, and topic alteration. Keyword shuffling disrupts the structural flow of information, while keyword injection introduces misleading terms that distort analytical significance. Content reduction removes critical elements, resulting in incomplete interpretations, and topic alteration replaces domain-

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.2026.0802378

specific terms to change the perceived context. Together, these techniques ensure that automated analysis tools generate inaccurate results, effectively preventing meaningful information extraction.

IV. ARCHITECTURE

The overall architecture of the proposed DEFT-IP framework is illustrated in Fig. 1, which presents a multi-layered design integrating user interaction, anomaly detection, and deception mechanisms for protecting intellectual property. The system begins with the user interface layer, where administrators and authorized users access the platform based on role-based access control.

User activities are continuously monitored and analyzed by the behavior monitoring module, and the collected data is processed by the Variational Autoencoder (VAE)-based anomaly detection module to identify abnormal patterns. Upon detecting suspicious behavior, the system activates the document manipulation module, which generates decoy documents using techniques such as keyword shuffling, injection, and topic alteration.

The manipulated documents are further processed using Natural Language Processing techniques, including TF-IDF, K-Means clustering, and Latent Dirichlet Allocation (LDA), to produce misleading analytical outputs. Simultaneously, alerts are generated to notify administrators of potential threats. Legitimate users receive original documents, while adversaries are served altered content, ensuring both security and usability.

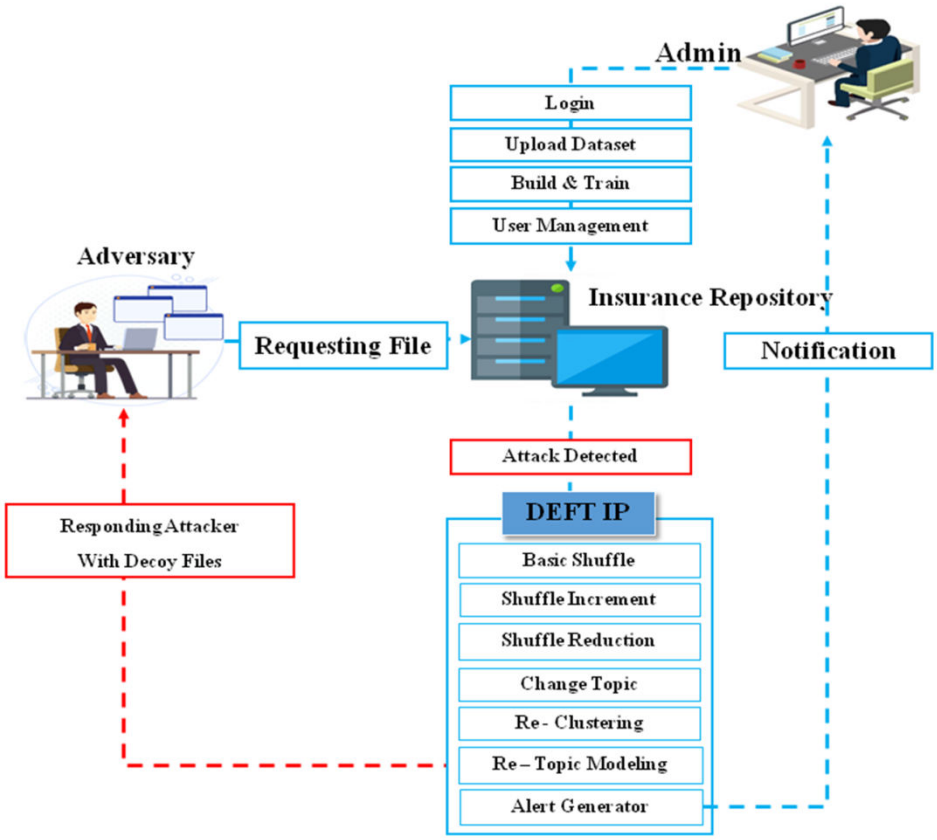


FIG 1.OVERALL ARCHITECTURE OF THE PROPOSED DEFT-IP

V. RESULTS AND DISCUSSION

The performance of the proposed DEFT-IP framework was evaluated based on its ability to detect anomalous user behavior and effectively disrupt automated intellectual property (IP) extraction techniques. The system was implemented using Python-based machine learning and Natural Language Processing (NLP) libraries and tested on a structured document repository containing domain-specific data. The evaluation focuses on anomaly detection accuracy, decoy effectiveness, system efficiency, and overall security improvement. The overall framework and operational workflow are illustrated in Fig. 2 and Fig. 3.

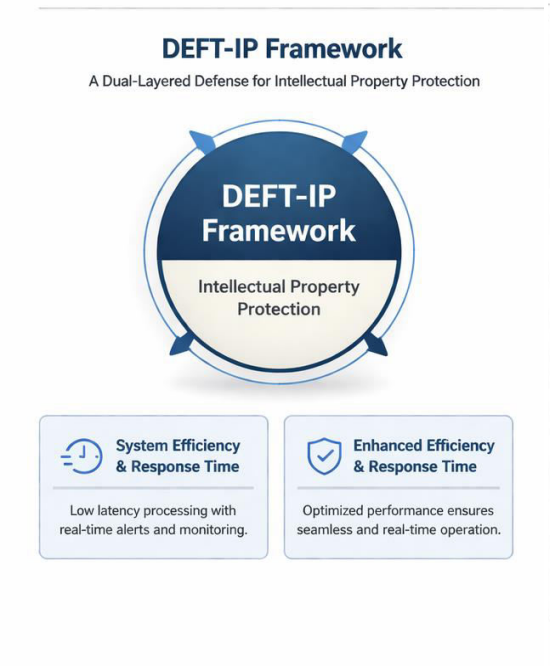
International Journal of Engineering & Extended Technologies Research (IJEETR)

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

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

DOI:10.15662/IJEETR.2026.0802378

The Variational Autoencoder (VAE) model was trained on normal user activity patterns, including document access frequency, session duration, and navigation behavior. Experimental results indicate that the model successfully identifies abnormal access patterns such as bulk document retrieval, irregular login timings, and access to unrelated document categories. The reconstruction error metric effectively distinguishes legitimate users from potential adversaries, enabling timely activation of defensive mechanisms. As shown in Fig. 2, the model achieves high accuracy, precision, recall, and F1-score, demonstrating the robustness of the anomaly detection mechanism.



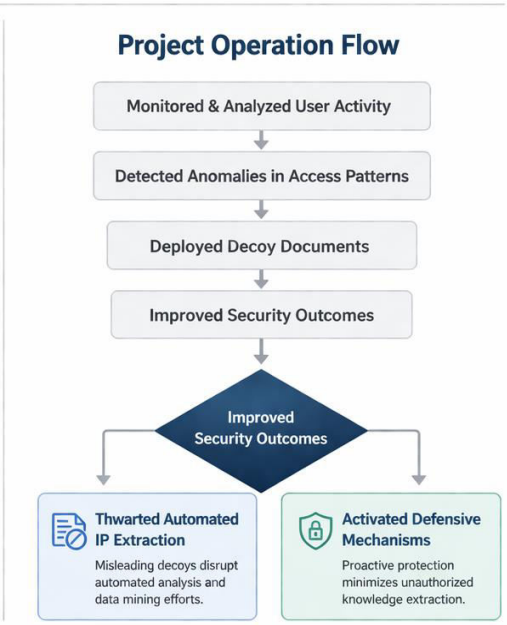
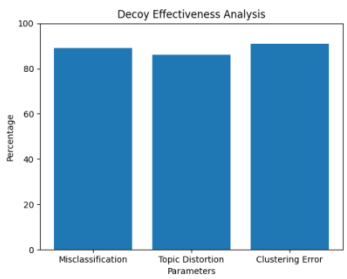


FIG 2. DEFT-IP FRAMEWORK **FIG 3. PROJECT OPERATION FLOW**

The decoy generation module demonstrates strong effectiveness in misleading automated data extraction techniques. Documents manipulated using keyword shuffling, keyword injection, content reduction, and topic alteration retain structural similarity while altering semantic meaning. Consequently, topic modeling using Latent Dirichlet Allocation (LDA) produces inaccurate topic distributions, and clustering algorithms such as K-Means generate misleading document groupings. As illustrated in Fig. 3, the high misclassification rate and distorted clustering outputs confirm that adversarial analysis is effectively disrupted.

The system response time was also evaluated to ensure real-time performance. The results indicate that operations such as authentication, anomaly detection, decoy generation, and alert notification are performed with low latency. As depicted in Fig. 5, the system maintains efficient processing speed even while executing complex machine learning and NLP tasks, ensuring that security mechanisms operate without negatively affecting system performance or user experience.



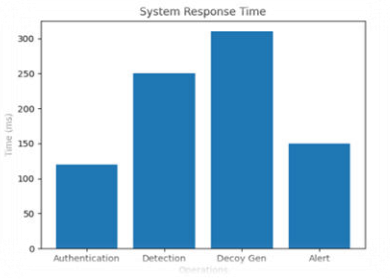


FIG 4. DECOY EFFECTIVE ANALYSIS **FIG 5. SYSTEM RESPONSE TIME**

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

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

DOI:10.15662/IJEETR.2026.0802378

The integration of anomaly detection with deception mechanisms significantly enhances overall system security. Unlike traditional approaches that focus solely on detection or prevention, the DEFT-IP framework actively misleads attackers, reducing of successful data exfiltration. The system also maintains a clear separation between legitimate and adversarial users, ensuring that genuine users receive original documents without disruption. The effectiveness of the deception strategy is further supported by the analysis shown in Fig. 4.

Overall, the results demonstrate that the DEFT-IP framework achieves high detection accuracy, effectively disrupts automated analysis techniques, and maintains efficient system performance. The combination of anomaly detection, NLP-based processing, and deception strategies provides a comprehensive and proactive security solution, making it highly suitable for protecting intellectual property in modern digital environments.

VI. CONCLUSION

This paper presented DEFT-IP, a proactive framework for protecting intellectual property against advanced cyber threats. By combining Variational Autoencoder (VAE)-based anomaly detection with decoy-driven document manipulation, the system effectively identifies suspicious behavior and misleads adversarial analysis techniques. The integration of NLP methods such as TF-IDF, K-Means, and LDA further enhances the system's ability to disrupt automated data extraction. Experimental results demonstrate improved detection accuracy, strong decoy effectiveness, and efficient performance. Overall, DEFT-IP provides a robust and intelligent approach for securing sensitive digital assets against both external and insider threats.

VII. FUTURE WORK

1. The future scope of the project is expansive, with potential for continual improvement and adaptation to evolving technological landscapes.
2. Integration with Blockchain Technology:Use blockchain to create a tamper-proof log of all access and changes to IP documents, ensuring better transparency and traceability.
3. Multi-Factor Authentication (MFA):Introduce multi-factor authentication to provide an additional layer of security for accessing the IP repository, reducing the risk of unauthorized access.
4. Cross-Platform Integration**:** Enable integration with various platforms (e.g., mobile devices) to allow secure access and management of documents across different devices and environments.

REFERENCES

1. Fariana and S. Jinan, "The urgency of intellectual property rights in the digital era from the perspective of Sharia economic law in Indonesia," Int. J. Res. Bus. Soc. Sci., vol. 12, no. 8, pp. 552–556, 2023.
2. P. Kumar, "Intellectual Property Rights (IPR): Nurturing Creativity Fostering Innovation," vol. 2, no. 2, pp. 32–38, 2024.
3. F. Indra and F. Santiago, "Intellectual Property Rights in Legal Perspective in Indonesia," in Proc. First Multidisciplinary Int. Conf., 2022.
4. X. Sun, X. Zhou, Q. Wang, P. Tang, E. L. C. Law, and S. Cobb, "Understanding attitudes towards intellectual property from the perspective of design professionals," Electron. Commer. Res., vol. 21, no. 2, pp. 521–543, 2021.
5. C. Novelli, F. Casolari, P. Hacker, G. Spedicato, and L. Floridi, "Generative AI in EU law: Liability, privacy, intellectual property and cybersecurity," 2024.
6. T. Chakraborty, S. Jajodia, J. Katz, A. Picariello, G. Sperli, and V. Subrahmanian, "A fake online repository generation engine for cyber deception," IEEE Trans. Dependable Secure Comput., vol. 18, no. 2, pp. 518–533, Mar./Apr. 2021.
7. World Intellectual Property Organization, "What is Intellectual Property?," 2020. [Online]. Available: https://www.wipo.int/about-ip/en/
8. 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
9. 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

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

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

DOI:10.15662/IJEETR.2026.0802378

10. 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
11. 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
12. 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
13. 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
14. 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.
15. 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.
16. 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.
17. 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
18. 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
19. 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
20. S. M. H. Bamakan, N. Nezhadsistani, O. Bodaghi, and Q. Qu, "Patents and intellectual property assets as non-fungible tokens: Key technologies and challenges," Sci. Rep., vol. 12, no. 1, p. 2178, 2022.
21. R. Guo, "Research on the protection of enterprise digital intellectual property rights," Sci. Law J., vol. 3, no. 2, pp. 153–159, 2024.
22. C. Novelli, F. Casolari, P. Hacker, G. Spedicato, and L. Floridi, "Generative AI in EU law: Liability, privacy, intellectual property and cybersecurity," 2024.
23. Gopinathan, V. R. (2024). Real-Time Fault-Tolerant Multi-Cloud Database Architectures for High Availability Applications. International Journal of Future Innovative Science and Technology (IJFIST), 7(4), 13148.
24. Chandra, S., Rengarajan, A., Sahoo, G. S., & Sharma, S. (2023, December). Identifying Neuronal Damage and Plasticity by Analyzing Changes in Diffusion Tensor Imaging. In International Conference on Data Science, Machine Learning and Applications (pp. 433-438). Singapore: Springer Nature Singapore.
25. Sugumar, R. (2025). Federated AI in Offline-First Mobile Health Architectures for Privacy-Preserving Clinical Intelligence. International Journal of Science, Research and Technology, 8(4), 14589-14600.
26. Murugeshwari, B., Rajalakshmi, S., & Sudharson, K. (2023). Hybrid Approach for Privacy Enhancement in Data Mining Using Arbitrariness and Perturbation. Computer Systems Science & Engineering, 44(3).
27. 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.
28. 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.
29. Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.
30. 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.
31. Akila, R. (2024). A deep reinforcement learning approach for optimizing inventory management in the agri-food supply chain. J. Electrical Systems, 20(4s), 2238-2247.

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

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

DOI:10.15662/IJEETR.2026.0802378

32. Mahendran, M., Anbazhagan, K., Pavithran, G., Nivas, A., & Pandey, S. D. (2022). Earthquake Damage Prediction using Machine Learning. Grenze International Journal of Engineering & Technology (GIJET), 8(1).
33. Gopinathan, V. R. (2025). Enterprise AI Frameworks for Financial Data Engineering Behavioural Analytics and Intelligent Cloud Solutions. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(4), 12499-12506.
34. Kondalsamy, P., & Kaliappan, K. (2025). An Optimal Prediction of Leaf Disease Based on Hybrid Deep Learnings and Metaheuristic Technique. Traitement du Signal, 42(1), 363.
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. (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.
37. 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.
38. Gopinathan, V. R. (2025). Software engineering practices for AI-driven systems: From development to deployment (MLOps perspective). International Journal of Science, Research and Technology, 8(1), 13493-13500.
39. Mathew, A. R. (2022). Threats and protection on E-sim: a prospective study. Novel Perspectives of Engineering Research, 8, 76-81.
40. Naveena, S., & Kavitha, K. (2025). Gossypium herbaceum: Folium disease identification and classification using Efficient Net-Coordinate Convolutional Neural Network (EcoNet). Engineering Applications of Artificial Intelligence, 152, 110701.
41. Rengarajan, A., Mishra, A., Kulhar, K. S., Shrivastava, V. P., & Alawneh, Y. J. J. (2024, March). Role of Deep Reinforcement Learning in Mitigating Cyber Security Issues: A Review. In International Conference on Renewable Power (pp. 37-48). Singapore: Springer Nature Singapore.
42. Achari, A. P. S. K., & Sugumar, R. (2024, November). Performance analysis and determination of accuracy using machine learning techniques for naive bayes and random forest. In AIP Conference Proceedings (Vol. 3193, No. 1, p. 020199). AIP Publishing LLC.
43. Mathew, A., & Alex, H. (2022). Detect & protect-medical device cybersecurity. Curr. Overview Sci. Technol. Res, 1, 60-68.
44. Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep Learning-Driven Visual Analytics Framework for Next-Generation Environmental Monitoring. Journal of Applied Science and Technology Trends, 114-122.
45. Anbazhagan, K. (2024). Trustworthy and Adaptive AI Systems for Enterprise Analytics Cybersecurity and Decision Optimization Using API-First and Cloud-Native Architectures. International Journal of Technology, Management and Humanities, 10(03), 65-74.
46. Mathew, A. (2021). Deep reinforcement learning for cybersecurity applications. Int J Comput Sci Mob Compu, 10(12), 32-38.
47. 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.
48. Karthika, K., Anusha, K., Kavitha, K., Harshadha, R., Dharshini, D. S., & Sundhar, N. A. (2025, April). Frequency Reconfigurable Antenna using Advanced Materials: A Study. In 2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-6). IEEE.
49. Thavamani, C., & Rengarajan, A. (2024). Clustering related behaviour of users by the use of partitioning and parallel transaction reduction algorithm. International Journal of Advanced Intelligence Paradigms, 29(2-3), 122-132.
50. 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.
51. 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.
52. SakthiPreetha, A., Kavitha, K., Karthika, K., & Manohari, R. G. (2025, April). A Novel Metasurface-Embedded Antenna for WBAN Communications. In 2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-4). IEEE.

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

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

DOI:10.15662/IJEETR.2026.0802378

53. Murugeshwari, B., Selvaraj, D., Sudharson, K., & Radhika, S. (2023). Data Mining with Privacy Protection Using Precise Elliptical Curve Cryptography. Intelligent Automation & Soft Computing, 35(1).
54. Gopinathan, V. R. (2025). Software engineering practices for AI-driven systems: From development to deployment (MLOps perspective). International Journal of Science, Research and Technology, 8(1), 13493-13500.
55. Anbazhagan, K., Kumar, R., Thilagavathy, R., & Anuradha, D. (2024, March). Shortest Job First with Gateway-based Resource Management Strategy for Fog Enabled Cloud Computing. In 2024 4th International Conference on Data Engineering and Communication Systems (ICDECS) (pp. 1-6). IEEE.
56. Kannadhasan, S., Vasuki, S., Kavitha, K., Karthikeyan, P., & Usha, S. G. A. (Eds.). (2025, April). Preface: Role of Artificial Intelligence and IoT in Engineering, Technology & Science [ICRAETS 2024]. In AIP Conference Proceedings (Vol. 3258, No. 1, p. 010001). AIP Publishing LLC.
57. Dhinakaran, D., Prathap, P. J., Selvaraj, D., Kumar, D. A., & Murugeshwari, B. (2022). Mining privacy-preserving association rules based on parallel processing in cloud computing. International Journal of Engineering Trends and Technology, 70(3), 284-294.