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.2026.0802355

Cybersecurity Defense & Advanced Threat Detection System

Preeson Akash B, Ragavan R, Srinivasa Bala S, Tamil Selvan V

Department of Computer Science and Engineering, R P Sarathy Institute of Technology,

Salem, Tamil Nadu, India

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

ABSTRACT: In the contemporary digital era, the rapid expansion of internet technologies, cloud computing, and interconnected systems has significantly increased the risk and complexity of cyber threats. Organizations and individuals rely heavily on digital platforms for communication, data storage, financial transactions, and critical operations, making cybersecurity a fundamental requirement. However, traditional security mechanisms such as firewalls, antivirus software, and rule-based detection systems are no longer sufficient to combat modern cyberattacks. Advanced threats such as ransomware, zero-day exploits, phishing campaigns, and Advanced Persistent Threats (APTs) are becoming more sophisticated, stealthy, and difficult to detect using conventional approaches.

This project focuses on the design and development of a comprehensive Cybersecurity Defense and Advanced Threat Detection system aimed at enhancing the protection of digital assets and network infrastructures. The proposed system integrates multiple layers of security mechanisms, combining both preventive and detective strategies to ensure a robust defense framework. It emphasizes the importance of proactive threat detection, real-time monitoring, and intelligent response to mitigate potential risks before they cause significant damage.

The core objective of this system is to identify both known and unknown cyber threats using advanced analytical techniques. To achieve this, the system incorporates machine learning algorithms that can learn from historical data and detect anomalies in network traffic and user behavior. Behavioral analysis plays a crucial role in identifying suspicious activities by establishing a baseline of normal operations and detecting deviations from expected patterns. Additionally, signature-based detection methods are used to identify known threats by comparing incoming data with a database of previously identified attack signatures.

In conclusion, this project demonstrates the significance of integrating advanced technologies such as machine learning, behavioral analysis, and threat intelligence in modern cybersecurity systems. The Cybersecurity Defense and Advanced Threat Detection system provides a scalable, efficient, and intelligent solution to protect against evolving cyber threats. It enhances the overall security posture by ensuring the confidentiality, integrity, and availability of data while enabling organizations to respond effectively to potential cyber incidents. This approach represents a significant step forward in addressing the growing challenges of cybersecurity in an increasingly connected and digital world.

KEYWORDS: Cybersecurity, Advanced Threat Detection, Machine Learning, Intrusion Detection System, Anomaly Detection, Threat Intelligence, Network Security, Data Protection.

I. INTRODUCTION

In the modern digital era, cybersecurity has become a crucial aspect of protecting information systems, networks, and data from unauthorized access and cyber threats. With the rapid growth of internet usage, cloud computing, and interconnected devices, the risk of cyberattacks has increased significantly. Traditional security methods such as firewalls and antivirus software are no longer sufficient to defend against advanced and evolving threats like ransomware, phishing attacks, zero-day exploits, and Advanced Persistent Threats (APTs).

To address these challenges, Cybersecurity Defense and Advanced Threat Detection systems have emerged as powerful solutions that enhance security through intelligent and proactive approaches. These systems utilize advanced technologies such as machine learning, behavioral analysis, and threat intelligence to detect both known and unknown threats in real time. Unlike conventional methods, they focus on identifying unusual patterns and anomalies in network traffic and system behavior, enabling early detection of potential attacks.

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

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

DOI:10.15662/IJEETR.2026.0802355

This project aims to develop an effective cybersecurity framework that integrates multiple layers of protection, including network security, endpoint security, and data security. By implementing automated monitoring and detection mechanisms, the system improves response time and reduces the risk of data breaches. Overall, the proposed solution provides a robust and scalable approach to safeguarding digital assets and ensuring the confidentiality, integrity, and availability of information in an increasingly connected world.

II. LITERATURE REVIEW

Cybersecurity has become an important research area due to the increasing number of cyber threats and attacks. Many researchers have focused on developing systems that can detect and prevent these threats effectively. Earlier studies mainly relied on traditional security methods such as firewalls and antivirus software, which work based on known threat signatures. However, these methods are not effective against new and unknown attacks. Recent research has introduced advanced techniques such as machine learning and artificial intelligence for threat detection. These methods help in identifying unusual patterns in network traffic and user behavior. Machine learning models can learn from past data and improve their detection accuracy over time. Researchers have shown that anomaly-based detection systems are more effective in detecting zero-day attacks compared to traditional methods.

Several studies have also focused on Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). IDS monitors network activity and alerts when suspicious behavior is detected, while IPS can take action to block attacks automatically. Modern systems combine IDS and IPS with real-time monitoring and threat intelligence to provide better security.

In addition, behavioral analysis has been widely used to detect insider threats and advanced persistent threats. By analyzing user activities, these systems can identify abnormal behavior that may indicate a security breach. Cloud-based security solutions have also been developed to handle large-scale data and provide scalable protection.

Overall, the literature shows that combining traditional security methods with advanced technologies such as machine learning, behavioral analysis, and threat intelligence provides a more effective approach to cybersecurity. These studies highlight the need for intelligent and automated systems to handle modern cyber threats, which forms the basis of this project.

III. PROPOSED SYSTEM

A. System Overview

The proposed system introduces a Cybersecurity Defense and Advanced Threat Detection framework designed to protect systems and networks from modern cyber threats. Unlike traditional security systems that rely only on signature-based detection, this system uses multiple techniques to improve accuracy and efficiency.

The system continuously monitors network traffic, system activities, and user behavior in real time. It uses a multi-layer detection approach where each layer analyzes different threat indicators and generates a risk score. These scores are combined to make the final decision.

This approach combines rule-based detection, machine learning, anomaly detection, and threat intelligence to identify both known and unknown cyber threats.

B. Rule-Based Threat Detection

This module acts as the first layer of security. It uses predefined rules based on known attack patterns and security policies.

Typical rules include:

- Multiple failed login attempts
- Access from unusual IP addresses
- Unauthorized access to sensitive files
- Suspicious port scanning activities

This module helps in quickly detecting common and known threats while reducing the load on advanced detection systems.

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.2026.0802355

C. Supervised Machine Learning Model

This module uses machine learning algorithms such as Random Forest to classify activities as normal or malicious.
The model is trained using labeled datasets containing both normal and attack data.
Key advantages include:

- High detection accuracy
- Ability to handle large data
- Reduced false positives

The model produces a probability score indicating the likelihood of a cyberattack.

D. Unsupervised Anomaly Detection

This module detects unknown or new types of attacks using anomaly detection techniques such as Isolation Forest.
It identifies unusual patterns that deviate from normal system behavior without needing labeled data.
Since many cyberattacks are previously unseen, this method is useful for detecting zero-day attacks and advanced threats.

E. Behavioral Analysis

This module monitors user and system behavior over time to detect suspicious activities.
Behavioral features include:

- Login patterns
- File access behavior
- Network usage patterns
- Device usage
- Time-based activity

If any behavior deviates from normal patterns, it increases the risk score. This helps in detecting insider threats and advanced persistent threats.

F. Threat Intelligence Integration

This module uses external threat intelligence data to improve detection.
It includes:

- Blacklisted IP addresses
- Known malware signatures
- Latest attack trends

This helps the system stay updated and detect newly emerging threats more effectively.

G. Risk Score Aggregation

Each module generates a risk score, which is combined to calculate the final threat level.
Final Risk Score = Rule Score + ML Score + Behavioral Score

Based on the final score, the system classifies threats as follows:

Risk Level	Decision
Low	Allow Access
Medium	Alert / Monitor
High	Block / Isolate

This multi-layered approach ensures accurate threat detection and minimizes false positives while improving overall cybersecurity.

IV. SYSTEM ARCHITECTURE

The system architecture is designed as a multi-layered framework that collects, processes, and analyzes data to detect cyber threats in real time. It combines different modules such as data collection, preprocessing, detection engines, and response systems to provide complete security.

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

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

DOI:10.15662/IJEETR.2026.0802355

Architecture Components:

a) Data Collection Layer

This layer gathers data from different sources:

- Network traffic
- System logs
- User activities
- Application data

This data is used for monitoring and analysis.

b) Data Preprocessing Layer

In this layer:

- Noise and unwanted data are removed
- Important features are extracted
- Data is formatted for analysis

This improves detection accuracy.

c) Detection Layer

This is the core part of the system and includes multiple modules:

- **Rule-Based Detection**

Detects known threats using predefined rules

- **Machine Learning Model**

Classifies normal and malicious activities

- **Anomaly Detection**

Identifies unknown or unusual behavior

- **Behavioral Analysis**

Monitors user patterns to detect suspicious actions

d) Threat Intelligence Layer

This layer provides updated information about:

- New cyber threats
- Malware signatures
- Blacklisted IPs

It improves detection of new attacks.

e) Decision & Response Layer

This layer:

- Combines risk scores from all modules
- Generates alerts
- Blocks malicious activities
- Isolates affected systems

f) User Interface Layer

Provides:

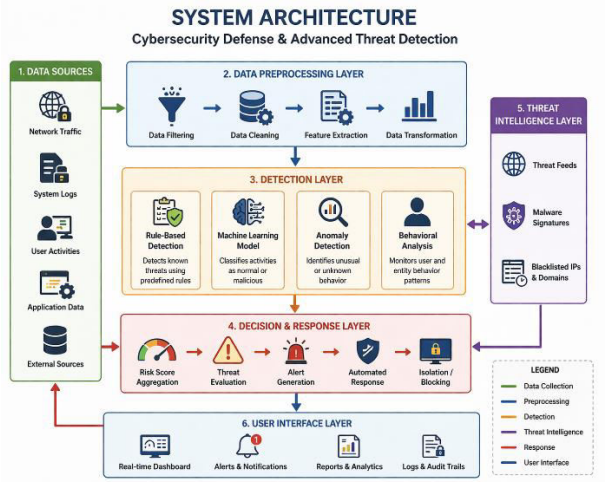
- Alerts and notifications
- Reports and logs
- Monitoring dashboard

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.2026.0802355



System Architecture

V. IMPLEMENTATION

Tools and Technologies Used

The system can be implemented using the following tools:

Programming Language:

• Python

Libraries:

• NumPy, Pandas – Data processing
• Scikit-learn – Machine learning models
• Matplotlib / Seaborn – Data visualization

Other Tools:

• Wireshark – Network data collection
• Jupyter Notebook / VS Code – Development environment

Implementation Steps

Step 1: Data Collection

- Collect data from network traffic, system logs, and user activities
- Use datasets (e.g., intrusion detection datasets) or live traffic tools

Step 2: Data Preprocessing

- Remove missing or irrelevant data
- Convert data into suitable format
- Normalize and clean data
- Extract important features

Step 3: Feature Extraction

- Select key attributes such as IP address, port number, login attempts, etc.
- Reduce unnecessary data to improve performance

Step 4: Model Development

a) Rule-Based Detection

- Define rules (e.g., multiple login failures, unusual IP access)

b) Machine Learning Model

- Train model (Random Forest / Decision Tree)
- Classify normal vs malicious activity

c) Anomaly Detection

- Use Isolation Forest to detect unusual patterns

Step 5: Behavioral Analysis

- Track user activity patterns

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

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

DOI:10.15662/IJEETR.2026.0802355

- Compare current activity with normal behavior
- Detect deviations

Step 6: Threat Detection and Scoring

- Combine outputs from all modules
- Assign risk scores
- Classify threat levels

Step 7: Alert and Response System

- Generate alerts for suspicious activity
- Block malicious IP addresses
- Isolate affected systems

Step 8: Visualization and Reporting

- Display results using graphs and dashboards
- Generate reports for analysis

VI. RESULTS AND DISCUSSION

1) Results of Threat Detection

a) Rule-Based Detection Results

The rule-based module successfully identified known threats such as:

- Multiple failed login attempts
- Unauthorized access attempts
- Suspicious IP addresses

This module provided quick detection with low processing time. However, it was limited to detecting only predefined attack patterns.

b) Machine Learning Model Results

The machine learning model (Random Forest) showed high accuracy in classifying normal and malicious activities.

Observed Results:

- High detection accuracy
- Good performance on structured data
- Reduced false positives compared to rule-based systems

The model was effective in detecting known and slightly modified attack patterns.

c) Anomaly Detection Results

The anomaly detection module (Isolation Forest) successfully identified unusual and unknown behaviors.

Observed Results:

- Detected zero-day attacks and unknown threats
- Identified rare and abnormal patterns
- Slight increase in false positives

This module is useful for detecting new types of cyberattacks.

d) Behavioral Analysis Results

Behavioral analysis helped in detecting insider threats and unusual user activities.

Observed Results:

- Detected deviations in user behavior
- Improved detection accuracy when combined with other modules
- Reduced false alarms by understanding normal behavior patterns

2) Performance Evaluation

The system performance was evaluated based on the following factors:

a) Accuracy

The combined system achieved high accuracy due to the integration of multiple detection techniques.

b) Detection Speed

Real-time monitoring enabled fast detection and response to threats.

c) False Positives

The hybrid approach reduced false positives compared to single-method systems.

d) Scalability

The system can handle large datasets and can be scaled for real-world applications.

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

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

DOI:10.15662/IJEETR.2026.0802355

4. Discussion

The results show that combining multiple detection techniques significantly improves cybersecurity performance. Each module plays a specific role:

- Rule-based detection provides fast identification of known threats
- Machine learning improves classification accuracy
- Anomaly detection identifies unknown attacks
- Behavioral analysis detects insider threats

The integration of these modules creates a strong and reliable defense system.

However, some challenges were observed:

- Anomaly detection may produce false positives
- Machine learning requires large datasets for training
- High computational resources are needed for real-time analysis

Despite these challenges, the overall system performance is effective and suitable for modern cybersecurity requirements.

VII. CONCLUSION

In the modern digital world, cybersecurity is very important due to the increasing number of cyber threats. Traditional security methods are not enough to handle advanced attacks such as malware, phishing, and zero-day threats. This project presented a Cybersecurity Defense and Advanced Threat Detection system that uses multiple techniques to improve security.

The system combines rule-based detection, machine learning, anomaly detection, and behavioral analysis to detect both known and unknown threats. It provides real-time monitoring and quick response to reduce damage caused by cyberattacks. The results show that this multi-layered approach improves accuracy and reduces false positives compared to traditional systems.

Overall, the proposed system offers an effective and reliable solution for protecting digital systems and data. It can be further improved and used in real-world applications to enhance cybersecurity and ensure safe and secure digital environments.

VIII. FUTURE WORK

The proposed Cybersecurity Defense and Advanced Threat Detection system can be further improved in several ways to enhance its performance and efficiency. In the future, more advanced machine learning and deep learning algorithms can be used to improve detection accuracy and reduce false positives. Techniques such as neural networks and artificial intelligence can help in identifying complex and hidden cyber threats more effectively.

The system can also be extended to support real-time deployment in cloud environments and large-scale networks. Integration with cloud security platforms and Internet of Things (IoT) devices will help in providing better protection in modern digital infrastructures. Additionally, incorporating automated response mechanisms using artificial intelligence can further reduce human intervention and improve response time.

Another area of improvement is the use of big data technologies to handle large volumes of security data efficiently. The system can also be enhanced by continuously updating threat intelligence to detect newly emerging cyber threats. Overall, future enhancements will make the system more intelligent, scalable, and adaptable, providing stronger protection against evolving cybersecurity challenges.

REFERENCES

1. W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed., Pearson, 2017.
2. V. K. Jain and B. B. Gupta, “An anomaly detection approach for intrusion detection system using machine learning,” *Procedia Computer Science*, vol. 132, pp. 141–150, 2018.
3. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.
4. S. Axelsson, “Intrusion detection systems: A survey and taxonomy,” *Technical Report*, Chalmers University, 2000.
5. M. Roesch, “Snort: Lightweight intrusion detection for networks,” in *Proc. USENIX LISA Conference*, 1999.
6. T. M. Mitchell, *Machine Learning*, McGraw-Hill, 1997.

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

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

DOI:10.15662/IJEETR.2026.0802355

7. 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
8. 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
9. 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
10. 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
11. 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
12. 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
13. 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.
14. 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.
15. 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.
16. 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
17. 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
18. 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
19. N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in *Proc. Military Communications and Information Systems Conference*, 2015.
20. S. Garfinkel and G. Spafford, *Practical UNIX and Internet Security*, 3rd ed., O'Reilly Media, 2003.
21. Cisco Systems, "Cisco Annual Cybersecurity Report," 2020.
22. K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, 2007.
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.

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

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

DOI:10.15662/IJEETR.2026.0802355

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.
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.

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

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

DOI:10.15662/IJEETR.2026.0802355

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.
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.