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.2026.0802399

Intelligent Cyber Threat Detection System using Machine Learning

Saranya A, Mrs. Anu Uthayam P., M. Tech., Uma M, Mrs. Sathya S., M.E., Thanzim P, Mrs. Vasugi R., M.Tech

Student, Department of Information Technology,Er. Perumal Manimekalai College of Engineering, Hosur, Anna University, Krishnagiri, Tamil Nadu, India

Assistant Professor, Department of Information Technology, Er. Perumal Manimekalai College of Engineering, Hosur, Anna University, Krishnagiri, Tamil Nadu, India

Student, Department of Information Technology, Er. Perumal Manimekalai College of Engineering, Hosur, Anna University, Krishnagiri, Tamil Nadu, India

Assistant Professor, Department of Information Technology, Er. Perumal Manimekalai College of Engineering, Hosur, Anna University, , Tamil Nadu, India

Student, Department of Information Technology, Er. Perumal Manimekalai College of Engineering, Hosur, Anna University, Krishnagiri, Tamil Nadu, India

Assistant Professor, Department of Information Technology, Sai Ram College of Engineering, Anekal, Bangalore, India

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

ABSTRACT: As internet technologies and digital communication expand, cybersecurity risks are rising quickly. Malware, phishing, and Distributed Denial of Service (DDoS) attacks are just a few of the cyberattacks that people and organisations are more susceptible to. These assaults have the potential to compromise private data, interfere with network services, and seriously harm operations and finances. It is challenging to successfully identify new or unknown threats because traditional security systems primarily rely on predefined rules and signature-based detection techniques.

In order to recognise anomalous network activity and automatically identify possible cyberattacks, this paper suggests an Intelligent Cyber Threat Detection System that uses machine learning. The system uses machine learning algorithms to analyse network traffic data and categorise it as either malicious or normal. The detection model is tested and trained using the CICIDS2017 dataset. The system can recognise suspicious activity and offer early cyber threat detection by identifying patterns in past network data. In order to improve overall network security, the suggested method seeks to enhance cybersecurity monitoring and assist organisations in promptly responding to possible attacks.

KEYWORDS: Cybersecurity, Machine Learning, Intrusion Detection System, Network Security, Threat Detection.

I. INTRODUCTION

Cyberattacks are now a major threat to people, companies, and organisations due to the quick development of digital technologies and internet connectivity. Attackers now have more ways to take advantage of weaknesses in computer systems and networks due to the growing use of online services, cloud computing, and digital

communication. To obtain unauthorised access to systems, steal confidential information, or interfere with network services, cybercriminals employ a variety of strategies, including phishing, malware, ransomware, and Distributed Denial of Service (DDoS) attacks. Serious repercussions from these attacks could include monetary losses, data breaches, harm to one's reputation, and interruptions to business operations. To defend networks against online threats, conventional cybersecurity techniques like firewalls, antivirus programs, and signature-based intrusion detection systems (IDS) are frequently employed. To identify malicious activity, these systems rely on pre-established rules and recognised

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

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

DOI:10.15662/IJEETR.2026.0802399

attack signatures. But contemporary cyberattacks are growing increasingly complex and ever-changing. Because of this, conventional security systems frequently fail to identify novel or unidentified threats, also referred to as zero-day attacks. Because of this constraint, more sophisticated and flexible security solutions must be created.

One way to improve cyber security systems is by using a machine learning (ML) technique. A large amount of data from network traffic can be analyzed by a machine learning model, which will be able to identify patterns of both normal and malicious behavior. It is better at detecting potential cyber threats and anomalies by learning from previous data compared to other techniques.

In this paper, an "Intelligent Cyber Threat Detection System using Machine Learning" is proposed, which can enhance network security. In this system, network traffic data is analyzed, and activities are classified as "Normal" or "Malicious" using machine learning techniques. For training and testing, the "CICIDS2017" dataset, which includes real-world network data, is used. This system is expected to enhance cybersecurity by detecting cyber attacks at an early stage, enabling organizations to take appropriate actions against potential cyber threats.

II. PROBLEM STATEMENT

Today's networks are generating a huge amount of traffic data, which makes it hard for security experts to monitor the traffic data manually in order to detect cyber attacks.

It is believed that as cyber attacks are becoming sophisticated, there is a need for the development of intelligent systems that can automatically analyze the data in the network in order to detect unusual activities.

It is believed that the absence of automated systems for detecting cyber attacks can result in the destruction of the network infrastructure.

It is with this reason that this project aims at developing an Intelligent Cyber Threat Detection System using Machine Learning in order to detect cyber attacks in the network.

III. EXISTING SYSTEM

Currently, available cybersecurity systems utilize conventional security solutions to ensure computer networks' security against cyber threats. Conventional security solutions include firewalls, signature-based Intrusion Detection Systems, antivirus software, and manual monitoring by security experts. Firewalls provide a boundary between trusted networks, which operate internally, and external networks, which are not trusted. Firewalls filter incoming and outgoing network traffic according to defined rules. Intrusion Detection Systems, on the other hand, monitor activities taking place within a network.

Signature detection is a common method that has been widely used in many traditional security systems. Signature detection identifies cyber attacks through a comparison of network activities to known patterns of cyber attacks, which are stored in a database as a signature. However, this method is limited in that it performs poorly in identifying new cyber attacks that are unknown to it.

In addition, there is a need for organizations to employ security analysts to monitor network logs and identify potential threats. This is a time-consuming process and requires a lot of human resources, especially in cases where a large amount of network traffic is generated daily. This increases the chances of human error in the process.

Another limitation associated with the traditional system is the rate of false alarms. In some cases, the system may identify normal network activities as potential threats. This may increase the rate of false alarms.

Because of such limitations, it has been seen that traditional cybersecurity systems are not always effective in detecting new cyber threats. Hence, it has become necessary to use intelligent systems like machine learning-based threat detection systems to improve cybersecurity monitoring.

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

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

DOI:10.15662/IJEETR.2026.0802399

IV. PROPOSED SYSTEM

The proposed system is focused on developing an "Intelligent Cyber Threat Detection System using Machine Learning" for the automated detection of malicious activities in the network. This system is different from traditional cyber threat detection systems that follow rule-based approaches for threat detection.

In this system, the data is collected in the form of network traffic using a cybersecurity dataset. The CICIDS2017 dataset is chosen for this system as it contains normal as well as multiple types of cyber attack data. Prior to the training of the model, the data collected in the previous step is subjected to a data preprocessing step. In this step, unnecessary data is eliminated, data with missing values is managed, and the data is cleaned in order to enhance the quality of the data.

Subsequent to the data preprocessing step, machine learning algorithms are employed in the training of the threat detection model. The trained model is capable of learning from the data collected in the past, allowing the model to classify the data as either normal or malicious. When new data regarding the network is fed into the system, the trained model is capable of detecting the suspicious activity based on the patterns learned from the data collected in the past.

In order for the system to be easily monitored, a web-based dashboard is developed using the Flask framework. The dashboard displays the detection result and offers a simple interface for the user to view potential threats. With the proposed system's automated detection feature, the accuracy and efficiency of the system are improved.

V. SYSTEM ARCHITECTURE

The system architecture of the proposed Intelligent Cyber Threat Detection System is composed of different components that collaborate with each other to identify cyber attacks in the network traffic data. The system architecture is composed of data collection, data preprocessing, training of the machine learning model, detection of the threat, and visualization of the results.

Firstly, the network traffic data is collected using the CICIDS2017 dataset. This dataset contains normal network traffic as well as various kinds of cyber attacks. This data is used for the training and testing of the machine learning model.

After collecting the data, the data preprocessing phase is performed. Here, the data is cleaned by eliminating any missing or irrelevant values. Important features are also chosen for this phase. This step is important for the quality and accuracy of the machine learning model.

After the preprocessing stage, the processed dataset is used for training the machine learning model. The machine learning model learns the patterns from the dataset and is able to distinguish between normal network traffic and malicious activities. After the training is done with the dataset, the machine learning model is ready for prediction of potential cyber attacks.

The machine learning model receives the network traffic data as an input. The machine learning model performs the task of threat detection by analyzing the data and identifying whether the data is normal or malicious.

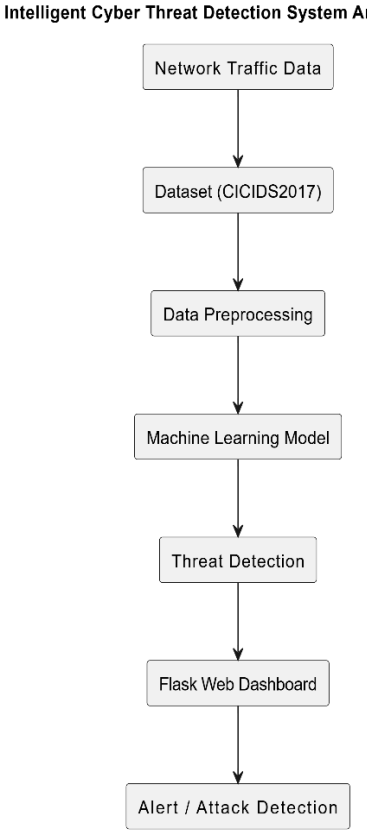
Finally, the detection results are presented in a web-based dashboard implemented using Flask. The dashboard provides users with a way to monitor network activities and view detected threats in a simple and user-friendly manner.The proposed architecture allows for automating a variety of security-related tasks, such as threat detection and incident response.

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.2026.0802399



VI. METHODOLOGY

The proposed Intelligent Cyber Threat Detection System utilizes machine learning algorithms in the detection of cyber threats in the network. The methodology used in the proposed Intelligent Cyber Threat Detection System involves several steps, including data collection, data preprocessing, training, threat detection, and visualization using a web interface. The step-by-step working process of the proposed Intelligent Cyber Threat Detection System is as shown in Fig. 2.

A. Dataset Collection

The system uses a dataset called CICIDS2017, which is a popular dataset in cybersecurity-related tasks. The dataset contains various records of network traffic that include both normal and malicious activities such as DDoS attacks, brute-force attacks, and infiltration attacks. The dataset contains various features that are helpful in recognizing abnormal patterns in network traffic.

B. Data Preprocessing

Data preprocessing is a significant step to process the data for machine learning. During this step, unnecessary data is removed from the dataset. Here, cleaning and preparation of data take place to enhance the performance of the machine learning model. Feature selection and normalization may also take place during this step.

C. Model Training

After this preprocessing stage, the cleaned data is used for training the machine learning model. The dataset is split into training data and testing data. In this research, the classification problem is addressed by using the Random Forest and Logistic Regression algorithms. The machine learning models are trained by learning the characteristics of normal and malicious network traffic. Then the performance of the trained model is checked by using the testing data.

D. Threat Detection

Once the model is trained, it is used to analyze new network traffic data. Based on the patterns learned, the network traffic is classified as normal or malicious. If there is any suspicious activity, it is classified as a cyber threat.

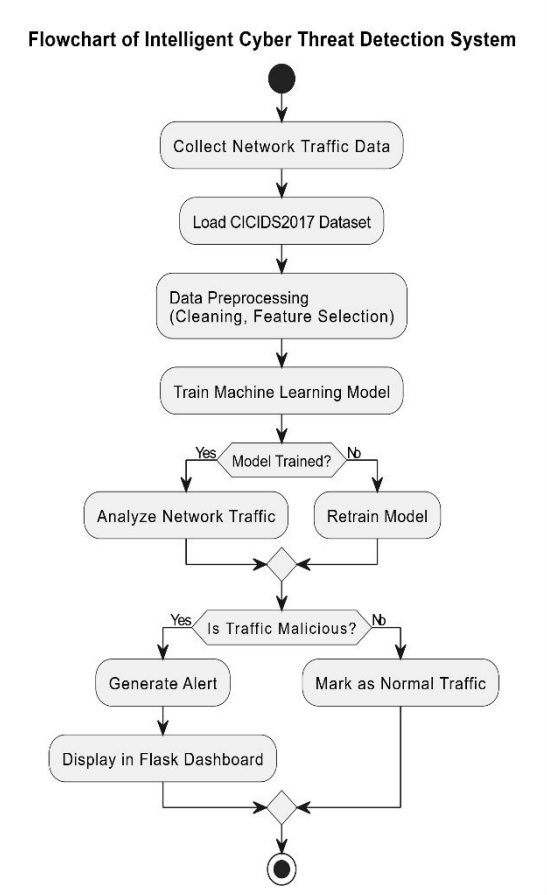
International Journal of Engineering & Extended Technologies Research (IJEETR)

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

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

DOI:10.15662/IJEETR.2026.0802399

E. Visualization and Monitoring The threats identified are shown through a web interface using Flask. This interface is useful for monitoring the activities taking place in the network and for identifying any attack. Alerts may also be sent to notify users about possible cyber threats.



VII. RESULTS AND DISCUSSION

The proposed Intelligent Cyber Threat Detection System was aimed at detecting malicious network activities using machine learning approaches. The Intelligent Cyber Threat Detection System was tested using the CICIDS2017 data set, which comprises both normal and attack traffic.

Once the data set is preprocessed and the machine learning algorithm is trained, the system is able to classify the network traffic as normal and malicious. The system is able to show effective results in the detection of common attacks like DDoS and brute force attacks.

The results show that the detection of cyber attacks is greatly improved through the usage of the machine learning-based system. The system reduces the manual efforts in the detection of attacks.

The web-based dashboard, which was created using the Flask library, is a simple yet efficient interface for monitoring the traffic on the network as well as the threats that are detected.

However, the system has a few limitations as well. The accuracy of the model depends on the data set used as well as the features chosen for the model.

Overall, the proposed system demonstrates the potential of machine learning in improving cybersecurity monitoring and threat detection.

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

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

DOI:10.15662/IJEETR.2026.0802399

VIII. CONCLUSION

In this paper, an Intelligent Cyber Threat Detection System based on the concept of machine learning has been proposed. The system processes the network traffic data and classifies it as normal and malicious activity.

The use of machine learning helps in the detection of known as well as unknown cyber attacks more efficiently compared to other security systems. The incorporation of the web-based dashboard feature enhances the usability of the system.

The proposed system minimizes human intervention and maximizes the efficiency of cybersecurity operations. For future enhancement of this system, it can be improved to achieve greater accuracy through the implementation of efficient machine learning algorithms and real-time data processing.

REFERENCES

1. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” in Proc. International Conference on Information Systems Security and Privacy (ICISSP), 2018, pp. 108–116.
2. D. P. Kingma and M. Welling, “Auto-encoding variational Bayes,” 2013, arXiv:1312.6114.
3. T. M. Mitchell, Machine Learning. New York, NY, USA: McGraw-Hill, 1997.
4. W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Pearson, 2017.
5. 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
6. 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
7. 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
8. 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
9. 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
10. 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
11. 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.
12. 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.
13. 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.
14. 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
15. 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
16. 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

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

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

DOI:10.15662/IJEETR.2026.0802399

17. S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Technical Report, Chalmers University of Technology, 2000.
18. M. Roesch, "Snort: Lightweight intrusion detection for networks," in Proc. 13th USENIX Conference on System Administration (LISA), 1999, pp. 229–238.
19. J. Zhang, M. Zulkernine, and A. Haque, "Random-forests-based network intrusion detection systems," IEEE Transactions on Systems, Man, and Cybernetics, vol. 38, no. 5, pp. 649–659, 2008.
20. Y. Lecun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, pp. 436–444, 2015.
A. H. Lashkari et al., "Characterization of Tor traffic using time based features," in Proc. ICISSP, 2017.
21. S. García, M. Grill, J. Stiborek, and A. Zunino, "An empirical comparison of botnet detection methods," Computers & Security, vol. 45, pp. 100–123, 2014.
22. 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.
23. 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.
24. 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.
25. 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).
26. 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.
27. 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.
28. Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.
29. 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.
30. 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.
31. 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).
32. 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.
33. 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.
34. 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.
35. 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.
36. 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.
37. 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.
38. Mathew, A. R. (2022). Threats and protection on E-sim: a prospective study. Novel Perspectives of Engineering Research, 8, 76-81.
39. 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.
40. 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.

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

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

DOI:10.15662/IJEETR.2026.0802399

41. 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.
42. Mathew, A., & Alex, H. (2022). Detect & protect-medical device cybersecurity. Curr. Overview Sci. Technol. Res, 1, 60-68.
43. 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.
44. 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.
45. Mathew, A. (2021). Deep reinforcement learning for cybersecurity applications. Int J Comput Sci Mob Compu, 10(12), 32-38.
46. 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.
47. 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.
48. 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.
49. 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.
50. 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.
51. 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.
52. 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).
53. 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.
54. 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.
55. 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.
56. 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.