International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-June-2026, ISSN (Online): 2395-566X

Enhancing Cybersecurity Through Machine Learning and Explainable AI-Based Intrusion Detection

Prakash Gahora[1], Bhanu Pratap Singh[2]
[1]M. Tech Scholar, 2HOD
[1,2]Department Computer Science and Engineering
[1,2]Aditya college of technology and science, Satna

Abstract — The rapid growth of digital communication, cloud computing, Internet of Things (IoT), and smart infrastructures has significantly increased cybersecurity threats and network vulnerabilities. Traditional intrusion detection systems (IDS) often struggle to detect sophisticated and evolving cyber-attacks due to their dependence on static rule-based mechanisms. To address these limitations, Machine Learning (ML) and Explainable Artificial Intelligence (XAI) have emerged as promising solutions for intelligent and adaptive intrusion detection. This research explores the integration of ML and XAI techniques in intrusion detection systems to improve attack detection accuracy, transparency, and real-time threat response. The study reviews various machine learning approaches, including supervised learning, deep learning, reinforcement learning, and federated learning methods used in modern IDS frameworks. Additionally, the role of explainable AI in enhancing trust, interpretability, and decision-making within cybersecurity systems is examined. The proposed approach emphasizes intelligent threat detection, reduced false alarm rates, and improved adaptability in IoT, industrial, and distributed computing environments. The findings indicate that AI-driven IDS frameworks provide efficient and scalable cybersecurity solutions capable of addressing emerging cyber threats while ensuring transparency and reliability in security operations.

Keywords— Machine Learning, Explainable Artificial Intelligence, Intrusion Detection System, Cybersecurity, Deep Learning, Network Security, IoT Security, Federated Learning, Threat Detection, Artificial Intelligence.

I. INTRODUCTION

The increasing dependence on digital technologies, cloud platforms, Internet of Things (IoT) devices, and smart communication networks has transformed modern society while simultaneously introducing significant cybersecurity challenges. Cyber-attacks such as malware, phishing, denial-of-service (DoS), ransomware, and unauthorized access have become more sophisticated and difficult to detect using traditional security mechanisms. As a result, intrusion detection systems (IDS) have become an essential component of network security infrastructures for identifying malicious activities and protecting critical digital resources.

Traditional IDS approaches primarily rely on signature-based and rule-based techniques to identify known attack patterns. Although these systems are effective against previously identified threats, they often fail to detect zero-day attacks, advanced persistent threats, and evolving intrusion techniques. Furthermore, conventional IDS models generate high false positive rates and lack adaptability to dynamic network environments. These limitations have encouraged researchers to integrate Artificial Intelligence (AI) and Machine Learning (ML) technologies into cybersecurity systems.

Machine learning-based intrusion detection systems can automatically analyze large volumes of network traffic data, identify hidden attack patterns, and continuously improve detection performance through training and learning mechanisms. Advanced deep learning techniques such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and reinforcement learning have demonstrated promising results in detecting complex and unknown cyber threats. Additionally, federated learning and edge intelligence approaches are being explored to improve privacy preservation and distributed attack detection in IoT and smart environments.

Despite these advancements, AI-driven intrusion detection systems often operate as black-box models, making their decisions difficult to interpret for cybersecurity professionals. Explainable Artificial Intelligence (XAI) addresses this issue by providing transparent explanations for detection outcomes, enabling security analysts to understand model behavior and improve trust in automated cybersecurity systems. XAI techniques enhance accountability, interpretability, and real-time threat response, which are critical for modern cybersecurity operations.

This research focuses on enhancing cybersecurity through machine learning and explainable AI-based intrusion detection

systems. The study examines recent advancements in AI-driven IDS models, highlights their applications in IoT and industrial environments, and explores the role of explainable AI in improving transparency and decision-making in cybersecurity systems.

II. LITERATURE REVIEW

1. Artificial Intelligence and Machine Learning-Based Intrusion Detection Systems

Recent studies have highlighted the growing importance of Artificial Intelligence (AI) and Machine Learning (ML) in enhancing intrusion detection systems (IDS). Traditional signature-based IDS approaches often fail to detect sophisticated and zero-day attacks, leading researchers to integrate AI-driven techniques for intelligent threat detection. Labib et al. (2026) emphasized that integrated AI significantly improves network security by enabling adaptive learning, automated threat analysis, and faster intrusion detection. Similarly, Mukil et al. (2026) demonstrated that machine learning models such as Decision Trees, Random Forest, and Support Vector Machines improve classification accuracy and reduce false alarm rates in IDS environments.

Deep learning approaches have also gained considerable attention due to their capability to process complex network traffic patterns. Purbia (2026) proposed the IA-IDS framework using Convolutional Neural Networks (CNN), Bidirectional Long Short-Term Memory (BiLSTM), and attention mechanisms to secure IoT networks, achieving enhanced detection accuracy for cyber threats. Priyadharshini et al. (2026) further improved intrusion detection performance through multimodal deep representation learning combined with dimensionality reduction techniques. These approaches effectively handled high-dimensional IoT traffic data while improving computational efficiency.

Comparative and optimization studies have also contributed to the advancement of ML-based IDS. Vu et al. (2026) compared multiple machine learning algorithms using the KDD99 and BKIDS2025 datasets and found that optimized feature selection and model tuning significantly improve IDS performance. Nayak et al. (2026) reviewed several machine and deep learning techniques for intrusion detection and concluded that hybrid deep learning models outperform conventional ML algorithms in identifying complex attack patterns. Collectively, these studies demonstrate that AI and ML technologies provide robust, scalable, and intelligent solutions for modern intrusion detection systems.

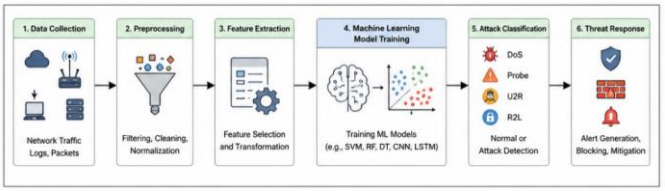

Figure 1: Architecture of AI and Machine Learning-Based Intrusion Detection System

This figure 1 illustrates the general architecture of an AI and ML-based intrusion detection system, including data collection, preprocessing, feature extraction, machine learning model training, attack classification, and threat response mechanisms. The figure highlights how AI techniques improve detection accuracy and automate cybersecurity operations.

2. Deep Learning, Reinforcement Learning, and Explainable AI in IDS

The emergence of deep learning and reinforcement learning has transformed intrusion detection by enabling systems to learn dynamic attack behaviors and adapt to changing network conditions. Yang et al. (2026) conducted a comprehensive survey on deep reinforcement learning-based IDS and reported that reinforcement learning techniques enhance autonomous decision-making and adaptive threat mitigation in cybersecurity systems. These methods allow IDS frameworks to continuously learn from network environments and improve attack detection over time.

Explainable Artificial Intelligence (XAI) has also become a critical research area in intrusion detection due to concerns regarding the transparency and trustworthiness of AI-driven security systems. Kumar (2026) emphasized that XAI techniques improve user confidence by providing interpretable explanations for IDS decisions, enabling security analysts to better understand detected threats and system behavior. The study highlighted that explainable models support real-time threat response while maintaining detection accuracy.

In industrial and critical infrastructure environments, intelligent IDS frameworks are increasingly being adopted to enhance cybersecurity resilience. Shafique et al. (2026) introduced X-SecureNet, an AI-driven intelligent framework specifically designed for smart industrial infrastructures. The framework integrates advanced security mechanisms with intelligent intrusion detection capabilities to secure Industry 4.0 environments. Similarly, Verma et al. (2026) proposed a real-time intelligent intrusion detection framework for robotic system cybersecurity, demonstrating the effectiveness of AI-

enabled IDS in protecting autonomous and robotic systems from cyber-attacks.

Bibliometric and trend analysis studies further indicate the increasing focus on lightweight, interpretable, and efficient IDS models. Pramudya et al. (2026) observed a growing research trend toward interpretable and lightweight intrusion detection systems capable of operating efficiently in resource-constrained environments. These findings indicate that future IDS research is moving toward adaptive, explainable, and real-time intelligent security systems.

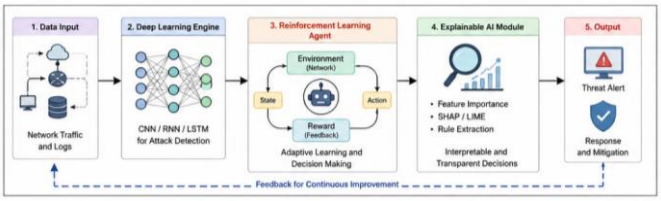

Figure 2: Deep Learning and Explainable AI Framework for Intrusion Detection

This figure 2 presents a conceptual framework integrating deep learning, reinforcement learning, and explainable AI within intrusion detection systems. It demonstrates how deep neural networks identify complex attack patterns, reinforcement learning adapts to dynamic threats, and explainable AI provides transparent decision-making for cybersecurity analysts.

3. Intrusion Detection for IoT, Wireless Networks, and Emerging Computing Environments

The rapid growth of Internet of Things (IoT), wireless sensor networks, fog computing, and smart city infrastructures has introduced new cybersecurity challenges, necessitating advanced intrusion detection mechanisms. Heidari and Jabraeil Jamali (2023) provided a comprehensive review of IoT intrusion detection systems and identified challenges such as resource constraints, scalability, and heterogeneous device communication. Their study also highlighted future directions involving lightweight AI-driven IDS architectures for IoT environments.

Several researchers have proposed specialized IDS frameworks for IoT and distributed environments. Nourildean et al. (2026) developed an ensemble machine learning-based IDS to improve IoT network security against cyber-attacks, demonstrating improved detection performance and robustness. Kushwaha et al. (2026) introduced an energy-aware federated learning approach using latent feature encoding for IoT intrusion detection. Their framework enhanced privacy preservation and reduced energy consumption while maintaining high detection accuracy, making it suitable for decentralized IoT networks.

Wireless and fog computing environments have also become major research areas in IDS development. Angurala et al. (2026) proposed enhanced intrusion detection techniques for wireless sensor networks to improve network security and attack resilience. Tamuka et al. (2026) reviewed intrusion detection advancements in fog computing and identified several unresolved challenges, including latency, data privacy, and distributed attack management. These studies indicate the growing importance of adaptive and lightweight IDS frameworks in distributed computing environments.

In addition, smart city and human-centered security applications are receiving increasing attention. Alnuaim (2026) explored intrusion detection and security attack mitigation in smart cities through the integration of human-computer interaction techniques. The study emphasized the importance of intelligent and user-centric cybersecurity systems for protecting urban digital infrastructures. Kalpani and Rodrigo (2026) further reviewed AI-driven intrusion detection approaches for Industry 4.0 and highlighted emerging trends such as federated learning, edge intelligence, and explainable AI for industrial cybersecurity applications. Together, these studies reveal that intrusion detection research is rapidly evolving to address the security demands of modern interconnected systems and emerging digital ecosystems.

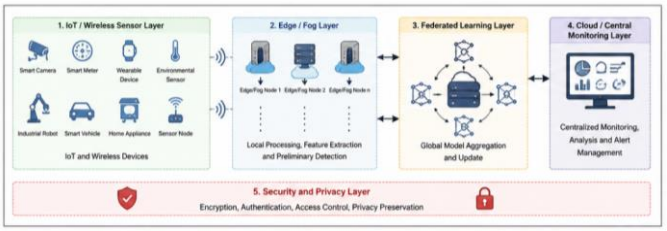

Figure 3: IoT and Fog Computing-Based Intrusion Detection Environment

This figure 3 depicts an intrusion detection framework designed for IoT, wireless sensor networks, and fog computing environments. It includes interconnected smart devices, edge/fog nodes, federated learning components, and centralized monitoring systems used to detect and mitigate cyber threats in distributed and resource-constrained environments.

Recent studies by U. Singh and co-authors have focused extensively on artificial intelligence, deep learning, machine learning, computer vision, cybersecurity, and healthcare

applications. Nagar and Singh (2025) proposed an AI-powered secure soccer penalty detection and performance recommendation system, while Shakyawar and Singh (2024) developed a deep learning model for facial expression recognition in crowds. Prajapati et al. (2023) and Patel and Singh (2023) worked on gender and age recognition using deep learning techniques. Gupta et al. (2023) and Baghel et al. (2022) focused on human face mask recognition using ResNet and OpenCV-based deep learning approaches. Vishwakarma et al. (2023) introduced an EfficientNetB3-based brain tumor segmentation and detection framework, whereas Singh and Songare (2022) developed a GoogLeNet-based monkeypox detection model. Research by Ranjan et al. (2022) explored cancer prediction using Random Forest and deep learning techniques. In recommendation systems, Singh et al. (2023) proposed a job recommendation model using machine learning and deep learning, while Taiwade et al. (2022) implemented a hierarchical K-means clustering approach for friend recommendation systems. Ray and Singh (2023) applied Hybrid Task Cascade Region-Based CNN for cricket score analysis. In cybersecurity and networking, Waskle et al. (2020) proposed an intrusion detection system using PCA with Random Forest, and Nihale et al. (2020) developed an LSTM-based network traffic prediction model. Additionally, Saxena et al. (2020) presented a CNN-based glaucoma detection system, while Bamne et al. (2020) explored transfer learning-based object detection using convolutional neural networks. Rajput et al. (2023) also conducted a comparative study of cloud providers including Azure, Amazon, and Oracle based on service availability and pricing.

III. RESEARCH GAP

Although significant progress has been made in machine learning and AI-based intrusion detection systems, several research gaps still exist in current cybersecurity solutions. Most traditional IDS models focus primarily on improving detection accuracy while neglecting interpretability and transparency. Deep learning models such as CNNs, LSTMs, and reinforcement learning algorithms often function as black-box systems, making it difficult for cybersecurity analysts to understand the reasoning behind intrusion detection decisions. This lack of explainability reduces trust and limits the practical deployment of AI-driven IDS in critical applications.

Another major research gap is the challenge of deploying intrusion detection systems in resource-constrained environments such as IoT devices, wireless sensor networks, and fog computing infrastructures. Many advanced deep learning models require high computational power, memory, and energy consumption, which limits their applicability in distributed and low-resource environments. Lightweight and energy-efficient IDS models are still under development and require further optimization.

In addition, existing intrusion detection systems often struggle to adapt to evolving cyber threats and zero-day attacks in real time. Static training datasets and centralized learning approaches reduce system adaptability and scalability in dynamic network environments. While federated learning and adaptive reinforcement learning techniques have shown promising results, their integration with explainable AI and real-time detection frameworks remains limited.

Furthermore, there is insufficient research on combining explainable AI with federated and deep learning-based intrusion detection systems to achieve both high accuracy and transparent decision-making. Most current studies evaluate IDS performance using benchmark datasets rather than real-world heterogeneous environments, creating a gap between theoretical models and practical cybersecurity applications. Therefore, further research is needed to develop adaptive, explainable, lightweight, and real-time intelligent intrusion detection systems capable of securing modern interconnected networks and emerging smart infrastructures.

IV. CONCLUSION

This study examined the role of machine learning and explainable artificial intelligence in enhancing modern intrusion detection systems for cybersecurity applications. The analysis revealed that AI-driven IDS frameworks significantly improve attack detection accuracy, threat classification, and automated response capabilities compared to traditional signature-based security systems. Machine learning and deep learning techniques enable IDS models to identify complex attack patterns, detect unknown threats, and adapt to dynamic network environments.

The study also highlighted the importance of Explainable AI in improving transparency, trust, and interpretability in cybersecurity systems. XAI techniques provide meaningful explanations for intrusion detection decisions, helping security analysts better understand system behavior and respond effectively to cyber threats. Furthermore, the integration of federated learning, reinforcement learning, and lightweight deep learning models demonstrates strong potential for securing IoT devices, industrial systems, wireless sensor networks, and fog computing environments.

Despite these advancements, several challenges remain, including high computational requirements, scalability

limitations, lack of interpretability in complex models, and difficulties in real-time deployment within resource-constrained environments. Overall, the research concludes that combining machine learning with explainable AI offers a powerful and intelligent approach for building reliable, adaptive, and transparent intrusion detection systems capable of addressing evolving cybersecurity threats.

Future Work

Future research can focus on developing lightweight and energy-efficient intrusion detection models suitable for IoT, edge computing, and wireless sensor network environments. Advanced optimization techniques can be applied to reduce computational complexity while maintaining high detection accuracy and low false positive rates.

Another important direction is the integration of Explainable AI with federated learning and reinforcement learning frameworks to create transparent and privacy-preserving intrusion detection systems. Real-time adaptive IDS models capable of continuously learning from evolving cyber threats should also be explored to improve system scalability and robustness.

Future studies may additionally investigate hybrid AI models combining deep learning, blockchain technology, and edge intelligence to strengthen cybersecurity in smart cities, Industry 4.0 infrastructures, and cloud-fog computing systems. The use of real-world datasets and practical deployment scenarios can further enhance the reliability and applicability of AI-driven intrusion detection systems in modern cybersecurity environments.

REFERENCES

1. Labib, S. S., Abdelsamad, R. S., Mahmoud, M. T., Khalil, M. M., & Abdelfatah, M. A. (2026). Transforming Network Security: The Role of Integrated AI in Intrusion Detection Systems. Advanced Sciences and Technology Journal, 3(1), 1-14.
2. Yang, W., Acuto, A., Zhou, Y., & Wojtczak, D. (2026). A survey for deep reinforcement learning based network intrusion detection. Applied AI Letters, 7(2), e70026.
3. Kumar, S. (2026). Explainable AI for Intrusion Detection Systems: Enhancing Trust, Transparency, and Real-Time Threat Response. International Journal of AI, BigData, Computational and Management Studies, 7(2), 115-123.
4. Shafique, A., Wu, G., Saeed, M. S., & Javeed, D. (2026). X-SecureNet: A Security-Driven Intelligent Framework for Intrusion Detection in Smart Industrial Infrastructures. Cluster Computing, 29(3), 168.
5. Purbia, R. (2026). IA-IDS: an intelligent adaptive intrusion detection system for IoT security using CNN, BiLSTM, and attention mechanism. Peer-to-Peer Networking and Applications, 19(1), 32.
6. Mukil, S., Patel, N. D., Lamkuche, H. S., Alazaidah, R., & Taqatqa, S. (2026). Intrusion detection system using machine learning models. In Business Resilience and Business Innovation for Sustainability: The Double-Edged Role of Artificial Intelligence and Other Disruptive Technologies (pp. 2125-2139). Cham: Springer Nature Switzerland.
7. Vu, T. A., Quoc, N. K., & Cao-Van, K. (2026). Optimizing Machine Learning-based Intrusion Detection Systems: A Comparative Study on KDD99 and BKIDS2025 Datasets. Vietnam Journal of Computer Science, 1-30.
8. Kushwaha, V. K., Verma, D. K., Yadav, S. P., & Gupta, H. (2026). Energy-Aware Federated Learning for IoT Intrusion Detection Using Latent Feature Encoding. IEEE Access.
9. Kushwaha, V. K., Verma, D. K., Yadav, S. P., & Gupta, H. (2026). Energy-Aware Federated Learning for IoT Intrusion Detection Using Latent Feature Encoding. IEEE Access.
10. Kushwaha, V. K., Verma, D. K., Yadav, S. P., & Gupta, H. (2026). Energy-Aware Federated Learning for IoT Intrusion Detection Using Latent Feature Encoding. IEEE Access.
11. Pramudya, E., Maharrani, R. H., Abdussalam, A., & Ghozi, W. (2026). Trends in Interpretable and Lightweight Intrusion Detection Systems: A Bibliometric Analysis of Network Traffic Anomaly Detection. Infotekmesin, 17(1), 1-8.
12. Verma, N., Kumar, N., Almuzaini, K. K., Sinha, A., & Abid Hussain, S. (2026). A real-time intelligent intrusion detection framework for robotic system cybersecurity. Peer-to-Peer Networking and Applications, 19(1), 30.
13. Nayak, V., Pawar, S., & Kumar, B. S. (2026). A review of machine and deep learning techniques for network intrusion detection. International Journal of Communication Networks and Distributed Systems, 32(2), 136-182.
14. Kalpani, N., & Rodrigo, N. (2026). Securing industry 4.0: a systematic review of AI-driven intrusion detection approaches and emerging trends. Journal of Reliable Intelligent Environments, 12(1), 1.
15. Alnuaim, A. (2026). Intrusion Detection and Security Attacks Mitigation in Smart Cities with Integration of Human-Computer Interaction. Computers, Materials, & Continua, 86(1), 1.
16. Angurala, M., Krishnan, S. B., Kshirsagar, P. R., & Maram, B. (2026). Advancing wireless sensor network security

through enhanced intrusion detection techniques. Wireless Networks, 1-17.
17. Nourildean, S. W., Mefteh, W., & Frihida, A. M. (2026). Intrusion detection system-based ensemble machine learning to improve IoT network against cyber attacks. The Journal of Supercomputing, 82(6), 370.
18. Priyadharshini, K., Arulprakash, M., Jeya, R., Muthevi, A. K., Sahu, M., Mohanty, S., & Singh, R. (2026). Harnessing multimodal deep representation with dimensionality reducing approach for enhanced intrusion detection system in internet of things networks. Scientific Reports.
19. Priyadharshini, K., Arulprakash, M., Jeya, R., Muthevi, A. K., Sahu, M., Mohanty, S., & Singh, R. (2026). Harnessing multimodal deep representation with dimensionality reducing approach for enhanced intrusion detection system in internet of things networks. Scientific Reports.
20. Tamuka, N., Mathonsi, T. E., Olwal, T. O., Maswikaneng, S., Muchenje, T., & Tshilongamulenzhe, T. M. (2026). Intrusion Detection in Fog Computing: A Systematic Review of Security Advances and Challenges. Computers, 15(3), 169.
21. Abo-Alian, A., Prince AbdelHalim, A., & Badr, N. (2026). Enhancing early detection and accuracy in image-based network intrusion detection systems. Cybersecurity, 9(1), 51.
22. Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: a comprehensive review and future directions. Cluster Computing, 26(6), 3753-3780.
23. K. Nagar, U. Singh, "ProSoccerTrainer: A secure AI-powered Penalty Detection and Performance Recommendation System," in 2025 5th Intelligent Cybersecurity Conference (ICSC), 2025, pp. 248–255.
24. P. Shakyawar, U. Singh, "Facial Expression Recognition Using Deep Learning Model on Crowd," in 2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET), 2024, pp. 1–6.
25. A. Prajapati, N. Patel, U. Singh, "Gender Recognition using Deep Learning Methodology," in 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), 2023, pp. 798–804.
26. A. Gupta, P. Tripathi, B. P. Singh, U. Singh, "Human Face Mask Recognition using ResNet 152 Model," in 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), 2023, pp. 1503–1510.
27. D. Singh, N. Patel, U. Singh, "Method for Job Recommendation based on Machine Learning and Deep Learning Model," in 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), 2023, pp. 875–883.
28. M. Vishwakarma, P. Tripathi, B. P. Singh, U. Singh, "Segmentation and Detection of Brain Tumors using EfficientNetB3 Model," in 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), 2023, pp. 1463–1470.
29. S. Ray, U. Singh, "Hybrid Task Cascade Region-Based Convolutional Neural Network is Used to Analyse Cricket Scores," in 2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), 2023, pp. 19–26.
30. A. Rajput, P. Gupta, P. Ghodeshwar, S. Varma, K. K. Sharma, U. Singh, "Study of Cloud Providers (Azure, Amazon, and Oracle) According To Service Availability and Price," in 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN), 2023, pp. 1177–1188.
31. M. Patel, U. Singh, "Age and Gender Recognition using Deep Learning Technique," in 2023 3rd International Conference on Smart Data Intelligence (ICSMDI), 2023, pp. 238–245.
32. U. Singh, L. S. Songare, "Analysis and Detection of Monkeypox using the GoogLeNet Model," in 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), 2022, pp. 1000–1008.
33. A. Taiwade, N. Gupta, R. Tiwari, S. Kumar, U. Singh, "Hierarchical K-Means Clustering Method for Friend Recommendation System," in 2022 International Conference on Inventive Computation Technologies (ICICT), 2022, pp. 89–95.
34. R. Baghel, P. Pahadiya, U. Singh, "Human Face Mask Identification using Deep Learning with OpenCV Techniques," in 2022 7th International Conference on Communication and Electronics Systems (ICCES), 2022, pp. 1051–1057.
35. M. Ranjan, A. Shukla, K. Soni, S. Varma, M. Kuliha, U. Singh, "Cancer Prediction Using Random Forest and Deep Learning Techniques," in 2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT), 2022, pp. 227–231.
36. S. Waskle, L. Parashar, U. Singh, "Intrusion Detection System Using PCA with Random Forest Approach," in 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020, pp. 803–808.
37. S. Nihale, S. Sharma, L. Parashar, U. Singh, "Network Traffic Prediction Using Long Short-Term Memory," in 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020, pp. 338–343.
38. A. Saxena, A. Vyas, L. Parashar, U. Singh, "A Glaucoma Detection using Convolutional Neural Network," in 2020

International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020, pp. 815–820.

39. B. Bamne, N. Shrivastava, L. Parashar, U. Singh, “Transfer learning-based Object Detection by using Convolutional Neural Networks,” in 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020, pp. 328–332.