STM JOURNALS

International Journal of
Wireless Security and Networks

ISSN: 2584-0703
Volume 3, Issue 2, 2025
July–December
DOI (Journal): 10.37591/IJWSN

https://journals.stmjournals.com/ijwsn

Review IJWSN

# Enhancing LAN Security Using Machine Learning

Kazi Kutubuddin Sayyad Liyakat*

***Abstract***

*The modern Local Area Network (LAN) is a critical component of any organization's infrastructure, facilitating communication, resource sharing, and access to the wider internet. However, this connectivity also brings inherent security risks. Traditional security measures, relying on signature-based detection and rule-based systems, are increasingly struggling to keep pace with the evolving sophistication of cyberattacks. This is where Machine Learning (ML) offers a powerful alternative, enabling proactive threat detection and enhanced security posture within the LAN environment. This study explores the application of machine learning-ML techniques to bolster LAN security, drawing insights and conclusions from recent research in the field. Traditional security systems often fail to address the complexities of modern cyber threats. Signature-based intrusion detection systems (IDSs) are limited to detecting known attacks, making them susceptible to zero-day vulnerabilities and polymorphic malware. Rule-based firewalls require constant updates and fine-tuning, which are time-consuming and disposed to errors. Moreover, these systems are often reactive, detecting threats only after they have already breached the network perimeter. Machine learning offers a proactive and adaptive approach to LAN security. By examining network traffic patterns, user actions, and system logs, machine learning algorithms can detect unusual behavior that differs from regular activity. This enables the identification of suspicious actions, including those that do not align with known attack signatures. Additionally, ML models can keep learning and adjusting to the changing threat environment, enhancing their precision and efficiency as time progresses.*

**Keywords:** LAN, security, machine learning, anomaly detection, cyberattacks

## INTRODUCTION

Local Area Networks (LANs) are essential to the IT infrastructure of many organizations, enabling devices to communicate and share resources seamlessly. However, as data traffic grows and cyber threats become more advanced, securing LANs has become a vital issue. While traditional security approaches are somewhat effective, they often fail to keep up with the fast-evolving tactics employed by cybercriminals. ML offers a revolutionary approach to bolster LAN security, providing advanced analytics and predictive capabilities that can bolster defenses against internal and external threats [1–4].

### LAN Threats

Before diving into applications of ML in LAN security, it is essential to comprehend the various threats that LANs face:

#### *Unauthorized Access*

Attackers often exploit weak passwords or configuration flaws to gain unauthorized access to network resources [5].

#### *Malware and Ransomware*

Malicious software can be introduced into LANs through various channels, causing significant threats to network integrity and data confidentiality [6].

***Author for Correspondence**
Kazi Kutubuddin Sayyad Liyakat
E-mail: drkkazi@gmail.com

Professor and Head, Department of Electronics and Telecommunication Engineering, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India

Received Date: February 15, 2025
Accepted Date: July 17, 2025
Published Date: September 09, 2025

**Citation:** Kazi Kutubuddin Sayyad Liyakat. Enhancing LAN Security Using Machine Learning. International Journal of Wireless Security and Networks. 2025; 3(2): 7–16p.

 

***Phishing Attacks***

Phishing remains a common tactic for breaching network security, whereby users are deceived into revealing sensitive information [7].

***Insider Threats***

Employees or authorized users can pose a substantial risk either maliciously or inadvertently, by misconfiguring systems or exposing sensitive data [8].

**Machine Learning Solutions to Threats**

Machine learning provides innovative solutions that are capable of addressing these threats through the following methods:

***Anomaly Detection***

ML algorithms can examine network traffic and establish a baseline of normal activity through techniques such as clustering and classification. ML-based systems can detect potential security incidents in real-time by recognizing deviations from the established baseline.

For instance, an unusual spike in data transfer from a specific device could indicate a malware infection or data exfiltration attempt [9].

***User Behavior Analytics (UBA)***

As insider threats can be particularly challenging to identify, UBA utilizes machine learning to monitor user behavior patterns across the network. By employing models that learn individual user habits, such as typical login times, accessed files, and activity frequency, anomalies can be detected quickly. If a user suddenly accesses sensitive data at an odd hour or from an unfamiliar device, alerts can be generated for further investigation [10].

***Automated Threat Intelligence***

ML can collect and examine vast quantities of threat intelligence data from varied sources, correlating this information to predict potential vulnerabilities within a LAN. This process enables security teams to receive actionable insights, improving their preparedness for known threats and enabling proactive defense strategies [11].

***Phishing Detection***

Machine learning models can be used to examine emails and messages for indicators of phishing attempts. By examining keywords, sender histories, and email structures, ML algorithms can categorize emails as suspicious, potentially reducing the chances of successful phishing attacks [12].

***Network Segmentation and Access Control***

By employing ML algorithms to build intelligent segmentation strategies, organizations can more effectively isolate critical infrastructure and sensitive data. Machine learning can assist in developing access control policies that adapt based on user behavior and threat landscapes, ensuring that employees only have access to necessary systems and data [13].

**LAN security challenges**

Although machine learning holds great potential for improving LAN security, several challenges need to be overcome:

- *Data Quality:* High-quality, labeled datasets are essential for machine learning models to function effectively. Organizations may struggle to gather adequate historical data or expertise to label anomalies accurately [14].
- *Model Accuracy:* Overfitting or underfitting models can result in false positives or negatives, leading to alert fatigue among security personnel or undetected breaches.

 

- *Complexity and Resource Requirements:* Implementing ML-based solutions often demands considerable computational resources and expertise, posing challenges for smaller organizations [15].
- *Adapting to Evolving Threats:* Cyber threats continually evolve, and ML models need to be retrained and updated frequently to remain effective.

The integration of machine learning technologies into LAN security represents a forward-thinking approach to combating the developing scenery of cyber threats. By leveraging ML's ability to analyze data and identify patterns, administrations can improve their security postures and respond to incidents more effectively [16].

As machine learning continues to advance, its applications in LAN security will undoubtedly expand, making it an essential facet of modern cybersecurity strategies. Organizations must recognize the importance of adopting these technologies while also addressing implementation challenges, ultimately fostering a more resilient security framework. By combining the analytical power of machine learning with best practices in cybersecurity, organizations can fortify their LANs against both current threats and the unknown challenges of the future.

## ANOMALY DETECTION WITH MACHINE LEARNING

In today's linked world, safeguarding LANs is critical for organizations and individuals. As cyberattacks become more advanced, traditional security measures like firewalls and antivirus software are no longer sufficient. A proactive strategy is essential, and ML is growing as an effective method for spotting anomalies that may suggest hostile activity within a LAN [17, 18].

Traditional security methods typically operate on predefined rules and signature databases. They are effective against known threats, but often struggle to identify novel attacks or subtle indicators of compromise. This is where anomaly detection comes in. By learning the normal behavior patterns of devices and users on network, ML models can identify deviations from the norm that could signal a security breach. These anomalies could range from uncommon network traffic patterns and unauthorized access attempts to compromised devices behaving erratically.

Several ML techniques are employed for anomaly detection in LAN environments:

- *Supervised Learning:* This method involves training a model using labeled data, where network traffic is categorized as either normal or malicious. While effective for identifying known attack patterns, it requires substantial quantity of considered data, which may be difficult and slow to acquire. Common algorithms used include Support Vector Machines (SVMs) and Decision Trees [19].
- *Unsupervised Learning:* This approach detects anomalies without the need for predefined labels. The model understands the natural structure of the network traffic data and identifies instances that significantly differ from the learned patterns. Algorithms such as K-Means clustering, Autoencoders, and One-Class SVM are well-suited for this task [20].
- *Time Series Analysis:* This method examines network traffic data over a period to detect abnormal increases or decreases in activity. Models like ARIMA (Autoregressive_Integrated_Moving_Average) and LSTM (Long_Short-Term_Memory) networks will be used to predict forthcoming network behavior and detect deviations from these predictions [21–24].

Advantages of Utilizing Machine Learning for Anomaly Detection in LANs:

- *Prompt Threat Identification:* Detecting anomalies enables early action, helping to prevent potential harm before it grows.
- *Identification of Zero-Day Attacks:* Because anomaly detection targets deviations from typical behavior, it can uncover new attacks that are not yet present in signature databases.

 

- *Improved Network Visibility:* The analysis performed by ML models provides valuable insights into network traffic patterns and user behavior, improving overall network visibility and security awareness.
- *Reduced False Positives:* By learning the specific nuances of the network environment, ML models can decrease the number of false positives, letting security sides to emphasize on sincere threats.
- *Automation and Scalability:* ML-powered anomaly detection solutions can automate the process of threat detection and scale to accommodate the growing demands of modern networks.

## IMPLEMENTING ANOMALY DETECTION IN LAN

Implementing ML-based anomaly detection demands thorough planning and execution:

- *Data Collection:* Collect detailed network traffic data, such as packet captures, system logs, and user activity logs.
- *Data Preprocessing:* Cleanse and convert the gathered data into a format compatible with ML algorithms. This step may include eliminating noise, addressing missing data, and performing feature engineering.
- *Model Selection and Training:* Select a suitable ML algorithm based on the specific traits of the network environment and the data at hand. Train the model on a representative dataset to learn normal behavior patterns [25].
- *Evaluation and Tuning:* Evaluate the enactment of the ideal using appropriate metrics like precision, recall, and F1-score. Tune parameters to optimize its accuracy and reduce false positives [26].
- *Deployment and Monitoring:* Implement the trained model in a live environment and continuously track its performance. Periodically retrain the model to accommodate changes in network behavior and emerging threats [27].

### Challenges and Considerations

- *Data Privacy:* Handling sensitive network traffic data requires careful attention to data privacy regulations. Anonymization and pseudonymization methods can be employed to safeguard user privacy [28].
- *Computational Resources:* Training and implementing ML models can take large computational resources, especially for large and complex networks [29].
- *Model Interpretability:* Understanding why a particular anomaly was flagged can be challenging, especially with complex ML models. Techniques in Explainable AI (XAI) can enhance the interpretability of models.
- *Adversarial Attacks:* ML models may be vulnerable to argumentative attacks, where assailants deliberately craft inputs to evade detection. Robustness techniques can be used to mitigate these vulnerabilities.

Machine learning provides an effective method for enhancing LAN security by detecting anomalies. By learning usual network behavior and identifying deviations, ML models can detect threats that customary security measures may miss. While challenges exist, the benefits of early threat detection, improved network visibility, and automated security outweigh the complexities. As cyberthreats endure to evolve, integrating ML-powered anomaly detection into LAN security strategies will become increasingly critical for protecting valuable data and maintaining a secure network environment [30].

## MACHINE LEARNING POWERS USER BEHAVIOR ANALYTICS IN LAN

In today's interconnected era, network security spreads far beyond perimeter firewalls. A significant threat lurks within: insider threats. These threats, whether malicious or accidental, originate from authorized users within the Local Area Network (LAN), making them notoriously difficult to detect. Fortunately, a powerful weapon has emerged in the fight against rogue actors and negligent employees: User Behavior Analytics (UBA) powered by Machine Learning (ML).

 

UBA uses ML algorithms to analyze user activity patterns in a LAN, establishing baselines of "normal" behavior. Any deviations from these baselines trigger notifications, drawing attention to potentially suspicious actions that traditional security methods could overlook. This proactive method allows administrations to identify and mitigate risks before they accelerate into significant security incidents.

Traditional rule-based security systems scuffle to keep hop with the complexity and vitality of modern LAN environments. Here is why ML-powered UBA is a game-changer:

- *Scalability:* A ML algorithm can efficiently process vast quantities of data generated by user activity, including login attempts, file access, application usage, network traffic, and more. The ability to scale is essential for handling the growing complexity and size of modern business LANs.
- *Anomaly Detection:* ML excels at identifying subtle deviations from established behavioral norms. It can detect unusual login times, access to sensitive data outside of normal work hours, or sudden spikes in data downloads, even if these actions do not trigger pre-defined security rules.
- *Behavioral Profiling:* ML algorithms create comprehensive behavioral profiles for individual users and groups. These profiles consider various factors, allowing for more accurate identification of anomalies that are specific to each user's role and responsibilities.
- *Reduced False Positives:* Outdated security systems frequently generate bulk of false positives, irresistible security teams. ML-based UBA learns from past data and adapts to evolving user behavior, meaningfully reducing the number of false alerts and letting security personnel to emphasize on sincere threats.
- *Adaptability:* The threat landscape is constantly evolving. ML-powered UBA continuously learns from new data, adapting to changing user behavior patterns and emergent threats, safeguarding that the security system remains operative over time.

The implementation of ML-powered UBA in a LAN typically includes the subsequent steps:

**Data Collection**

Collecting data from numerous sources within the LAN, including:

- *Security Logs:* Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS).
- *Active Directory Logs:* Login attempts, user group memberships, password changes.
- *Application Logs:* Application usage, data access patterns.
- *Network Traffic Data:* Monitoring network activity for unusual communication patterns.

**Data Processing and Feature Engineering**

Normalizing, cleaning, and transforming the collected data into setup suitable for ML analysis. Feature causing includes generating new topographies from the raw data that are relevant for anomaly detection.

**Model Training**

Training ML algorithms on historical user behavior data to establish baseline profiles. Common ML algorithms used include:

- *Clustering Algorithms (e.g., K-Means):* Grouping users with similar behavior patterns.
- *Anomaly Detection Algorithms (e.g., Isolation Forest):* Identifying outliers in user activity.
- *Supervised Learning Algorithms (e.g., Support Vector Machines):* Classifying user activity as normal or anomalous based on labeled data.

**Anomaly Detection and Alerting**

Continuously monitoring user activity and comparing it against the established baselines. When significant deviations are detected, alerts are generated and sent to security personnel for investigation.

 

**Continuous Learning and Improvement**

Retraining the ML models periodically with new data to familiarize to evolving user behavior and emergent threats.

**Benefits of Implementing ML-Powered UBA in Your LAN**

- *Early Detection of Insider Threats:* Identify malicious insiders and compromised accounts before they effect important damage.
- *Improved Security Posture:* Strengthen overall security stance by proactively classifying and mitigating risks.
- *Reduced Data Breaches:* Prevent data breaches by detecting unusual data access patterns and exfiltration attempts.
- *Improved Compliance:* Ensure adherence to regulatory standards for data security and privacy.
- *Optimized Security Operations:* Decrease the liability on security sides by automating anomaly detection and prioritizing alerts.

Although ML-driven UBA provides considerable advantages, its successful implementation demands thorough planning and thoughtful consideration.

- *Data Quality:* The accuracy of UBA relies heavily on quality of the data collected. Ensure data is clean, consistent, and accurate.
- *Privacy Concerns:* Gathering and examining handler behavior data raises privacy concerns. Adopt suitable privacy safeguards and guarantee adherence to applicable regulations.
- *Model Training Data:* Adequate and representative training data is crucial for building accurate ML models.
- *Expertise:* Implementing and managing ML-powered UBA requires specialized expertise in data science, security, and network administration.

In the face of increasingly sophisticated insider threats, ML-powered UBA is becoming an indispensable tool for securing LAN environments. By leveraging the power of ML to analyze user behavior, organizations can proactively identify and mitigate risks, protecting their valuable data and assets from malicious or negligent insiders. While challenges exist, the remunerations of applying this technology far outweigh the hurdles, making it a crucial investment for any organization committed to robust security.

## FORTIFYING THE FOUNDATION: HOW MACHINE LEARNING IS REVOLUTIONIZING LAN SECURITY DESIGN

Local Area Networks (LANs) serve as the foundation of contemporary organizations, linking devices and enabling smooth communication and data exchange. However, this connectivity also presents a significant vulnerability, making LANs prime targets for cyberattacks. Outdated security measures, while valuable, often fight to keep hop with the developing threat landscape. This is where Machine Learning (ML) comes into play, providing an effective method to automate threat identification, forecast vulnerabilities, and proactively strengthen LAN security architecture.

This study outlines how incorporating ML can revolutionize your LAN security design process, offering a more intelligent, adaptive, and resilient network defense.

Before diving into integration of ML, it is crucial to understand limitations of traditional approaches:

- *Reactive Security:* Traditional methods largely rely on reacting to known threats, leaving the network vulnerable to novel attacks.
- *Signature-Based Detection:* Virus scanners and intrusion detection systems often depend on predefined signatures, making them ineffective against zero-day exploits.
- *Manual Configuration:* Manual configuration of security policies and rules is time-consuming, error-prone, and difficult to scale.

 

- *Limited Contextual Awareness:* Traditional systems lack the ability to correlate data points and understand the overall security stance of network.

**Leveraging Machine Learning for LAN Security: A Design-Focused Approach**

ML offers active and adaptive method to LAN security design. Here are key design steps incorporating ML techniques:

***Data Collection and Feature Engineering: The Foundation of Intelligence***

- *Goal:* Gather relevant data representing network behavior and extract meaningful features for ML models.
- *ML Techniques:* Data mining, feature selection, dimensionality reduction.
- *Implementation:*
  - *Log Analysis:* Gather logs from firewalls, intrusion detection systems (IDS), servers, and client maneuvers.
  - *Network Traffic Analysis:* Examine network packets using software such as Wireshark and Suricata.
  - *Endpoint Monitoring:* Collect data on application usage, process behavior, and system configurations on endpoint devices.
  - *Feature Extraction:* Derive features such as packet size, source/destination IP addresses, port numbers, protocol types, and user agent details.

***Anomaly Detection: Recognizing Suspicious Behavior***

- *Objective:* Detect anomalies in network activity that may signal a potential malicious attack.
- *ML Techniques:* Anomaly detection algorithms (e.g. One-Class SVM, Autoencoders).
- *Implementation:*
  - *Network Traffic Anomaly Detection:* Identify unusual traffic patterns, such as spikes in data transfer, connections to suspicious IP addresses, or unusual protocol usage.
  - *User Behavior Anomaly Detection:* Detect unusual user activity, such as logging in from unfamiliar locations, accessing sensitive data outside of working hours, or sudden changes in file access patterns.
  - *Endpoint Anomaly Detection:* Identify unusual process behavior, such as unauthorized software installations, suspicious system calls, or excessive resource consumption.

***Intrusion Detection and Prevention: Real-time Threat Mitigation***

- *Goal:* Identify and prevent malicious intrusions into the LAN.
- *ML Techniques:* Supervised learning algorithms (e.g., Decision Trees, Random Forests, SVM, DL).
- *Implementation:*
  - *Training:* Train ML models on labeled datasets of known attacks and benign network traffic.
  - *Real-time Detection:* Deploy models to examine network traffic in real-time and recognize possible threats.
  - *Prevention:* Automatically block suspicious traffic, quarantine infected devices, and alert security personnel.

***Vulnerability Evaluation and Prioritization: Preventive Risk Management***

- *Goal:* Identify and prioritize vulnerabilities in the LAN infrastructure.
- *ML Techniques:* Natural Language Processing (NLP), Machine Learning-based vulnerability scanners.
- *Implementation:*
  - *Vulnerability Scanning:* Use ML-powered vulnerability scanners to automatically identify security flaws in software and hardware.

 

- *Vulnerability Prioritization:* Use NLP techniques to analyze vulnerability descriptions and prioritize remediation struggles centered on severity and possible impact.
- *Predictive Vulnerability Analysis:* Leverage ML to predict possible vulnerabilities founded on historical data and emerging threat trends.

***Security Policy Optimization: Adaptive and Intelligent Protection***

- *Goal:* Dynamically regulate security strategies founded on real-time network circumstances and threat intellect.
- *ML Techniques:* Reinforcement Learning, Genetic Algorithms.
- *Implementation:*
  - *Automated Policy Enforcement:* Automatically enforce security policies based on detected threats and user behavior.
  - *Dynamic Access Control:* Dynamically adjust access control rules based on user role, device type, and location.
  - *Adaptive Firewall Rules:* Modify firewall rules automatically based on network traffic trends and threat intelligence.

***Threat Intelligence and Correlation: Building a Holistic View***

- *Goal:* Aggregate and correlate threat intellect from numerous sources to increase a complete understanding of threat background.
- *ML Techniques:* Knowledge Graphs, Natural Language Processing (NLP), ML-based threat intelligence platforms.
- *Implementation:*
  - *Threat Intelligence Aggregation:* Gather threat intelligence from public feeds, commercial providers, and internal security systems.
  - *Threat Intelligence Correlation:* Use ML to correlate threat intelligence data with network activity and identify potential attacks.
  - *Threat Hunting:* Leverage threat intelligence to actively seek out threats that might have evaded conventional security defenses.

While ML offers significant advantages, its implementation necessitates cautious deliberation:

- *Data Quality:* The effectiveness of ML models relies on the quality and comprehensiveness of the training data.
- *Model Explainability:* Understanding how ML simulations make results is vital for debugging and ensuring trust.
- *Computational Demands:* Training and implementing ML models can require significant computational power.
- *Adversarial Threats:* ML models may be susceptible to adversarial attacks that can alter their functioning.
- *Privacy Issues:* Gathering and analyzing network data presents privacy concerns that need to be managed.

Incorporating Machine Learning into LAN security design represents a shift from reactive to proactive defense strategies. By automating threat detection, predicting vulnerabilities, and dynamically adapting security policies, ML empowers organizations to build more resilient and intelligent networks. Although there are challenges, the advantages of using ML to improve LAN security are clear. By embracing these design steps, organizations can fortify their foundations and protect their critical data and systems from the ever-evolving threat scenery. The future of LAN security is undoubtedly intelligent, adaptive, and driven by the power of ML.

 

## CONCLUSION

The application of ML to LAN security offers a significant improvement over traditional security approaches. By leveraging the power of data examination and pattern recognition, ML can provide proactive threat detection, improved accuracy, and automated response capabilities. As cyber threats endure to evolve, machine learning will become an increasingly essential tool for securing Local Area Networks and protecting organizations from cyberattacks. Further study and advancement in this area are warranted to refine ML algorithms, optimize deployment strategies, and address potential challenges like data privacy and model explainability. The future of LAN security lies in the intelligent application of machine learning to create a more secure and resilient network environment.

## REFERENCES

1. Khadake S, Kawade S, Moholkar S, Pawar M. A review of 6G technologies and its advantages over 5G technology. In: Techno-Societal 2016, International Conference on Advanced Technologies for Societal Applications. Cham: Springer International Publishing; 2022 Dec 9; 1043–1051.
2. Patil VJ, Khadake SB, Tamboli DA, Mallad HM, Takpere SM, Sawant VA. Review of AI in power electronics and drive systems. In 2024 IEEE 3rd International conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC). 2024 Feb 23; 94–99.
3. Dudgikar AB, Ingalgi AA, Jamadar AG, Swami OR, Khadake SB, Moholkar SV. Intelligent battery swapping system for electric vehicles with charging stations locator on IoT and cloud platform. Int J Adv Res Sci Commun Technol. 2023 Jan; 3(1): 204–8.
4. Khadake SB, Patil VJ. Prototype design & development of solar based electric vehicle. In 2023 IEEE 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON). 2023 Dec 29; 1–7.
5. Patil VJ, Khadake SB, Tamboli DA, Mallad HM, Takpere SM, Sawant VA. A comprehensive analysis of artificial intelligence integration in electrical engineering. In 2024 IEEE 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI). 2024 Jan 18; 484–491.
6. Khadake SB, Dolli SP, Rathod KS, Waghmare MO, Deshpande MA. An overview of intelligent traffic control system using PLC and use of current data of vehicle travels. VESCOMM-2016. 2016 Feb 12; 1–4.
7. Magar SS, Sugandhi AS, Pawar SH, Khadake SB, Mallad HM. Harnessing Wind Vibration, a Novel Approach towards Electric Energy Generation-Review. Int J Adv Res Sci Commun Technol. 2024 Oct; 4(2): 73–82.
8. Sarkar A. Design of automatic hand sanitizer with temperature sensing. Int J Innov Sci Res Technol. 2020; 5(5): 1269–75.
9. Landage SS, Chavan SR, Kokate PA, Lohar SP, Pawar MK, Khadake SB. Solar outdoor air purifier with air quality monitoring system. Synergies of Innovation: Proceedings of NCSTEM. 2024 Sep; 2023: 260–6.
10. Shabnam S, Latha HN. Design and implementation of saliency detection model in h. 264 standard. Int J Sci Res. 2014; 3(6): 2014–20.
11. Deng Z. Survey on various approaches of saliency detection. In 2019 IEEE International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI). 2019 Nov 8; 358–363.
12. Bhosale PS, Kokare PD, Potdar DS, Waghmode SD, Sawant VA, Khadake SB. DTMF Based Irrigation Water Pump Control System. Synergies of Innovation: Proceedings of NCSTEM. 2023; 267–73.
13. Korake P, Murade H, Doke R, Narale V, Khadake SB, Chavan AS. Automatic Load Sharing of Distribution Transformer using PLC. Synergies of Innovation: Proceedings of NCSTEM. 2024 Sep; 253–9.
14. Xiong R. Overview of battery and its management. In: Battery Management Algorithm for Electric Vehicles. Singapore: Springer Singapore; 2019 Sep 24; 1–24.
15. Gavaskar S, Sumithra A, Saranya A. Health portal-an android smarter healthcare application. Int J Res Eng Technol. 2013 Sep; 9(2): 291–295.

 

16. Javaid M, Haleem A, Singh RP, Suman R. Enhancing smart farming through the applications of Agriculture 4.0 technologies. Int J Intell Netw. 2022 Jan 1; 3: 150–64.
17. Muniappan A, Thiagarajan C, Kumar GA, Joseph Raj X, Irene J, Niranjan N. Conversion of Conventional Vehicle Into Solar Powered Electric Vehicle—A Realistic Approach. Int J Innov Res Sci Eng Technol. 2014; 3(9): 16232–7.
18. Randive AB, Gaikwad SK, Khadake SB, HM M. Biodiesel: a renewable source of fuel. Int J Adv Res Sci Commun Technol. 2024 Dec; 4(3): 225–40.
19. Veena C, Sridevi M, Liyakat KK, Saha B, Reddy SR, Shirisha N. HEECCNB: An efficient IoT-cloud architecture for secure patient data transmission and accurate disease prediction in healthcare systems. In 2023 IEEE Seventh International Conference on Image Information Processing (ICIIP). 2023 Nov 22; 407–410.
20. Kazi KS. Computer-aided diagnosis in ophthalmology: A technical review of deep learning applications. Transformative Approaches to Patient Literacy and Healthcare Innovation. Cham: Springer; 2024; 112–35.
21. Dhanke J, Rathee N, Vinmathi MS, Janu Priya S, Abidin S, Tesfamariam M. [Retracted] Smart Health Monitoring System with Wireless Networks to Detect Kidney Diseases. Comput Intell Neurosci. 2022; 2022(1): 3564482.
22. Kumar M, Sul SS, Lakhara JS, Kashid PJ, Bhinge SR, Waghmode AS, Khadake SB. Small Wind Electric System Energy Saver. Int J Adv Res Sci Commun Technol. 2025 May; 5(5): 447–466.
23. Reddy BM. Amalgamation of internet of things and machine learning for smart healthcare applications–a review. Int J Comp Eng Sci Res. 2023 Jun; 5(1): 08–36.
24. Baseer KK, Sivakumar K, Veeraiah D, Chhabra G, Lakineni PK, Pasha MJ, Gandikota R, Harikrishnan G. Healthcare diagnostics with an adaptive deep learning model integrated with the Internet of medical Things (IoMT) for predicting heart disease. Biomed Signal Process Control. 2024 Jun 1; 92: 105988.
25. Odnala S, Shanthy R, Bharathi B, Pandey C, Rachapalli A, Liyakat KK. Artificial Intelligence and Cloud-Enabled E-Vehicle Design with Wireless Sensor Integration. Available at SSRN 5107242. 2024 Nov 15.
26. Neeraja P, Kumar RG, Kumar MS, Liyakat KK, Vani MS. DL-based somnolence detection for improved driver safety and alertness monitoring. In 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT). 2024 Feb 9; 5: 589–594.
27. Nerkar PM, Dhaware BU, Liyakat KS. Predictive data analytics framework based on heart healthcare system (HHS) using machine learning. J Adv Zool. 2023; 44(2): 3673–3686.
28. Bhadula S, Sharma S. IoT-based skin monitoring system. Int J Recent Technol Eng. 2020 Jan; 8(5): 4258–64.
29. Fang K, Wang W, Woźniak M, Zhang Q, Yu K, Chen J, Tolba A, Zhang L. Guest Editorial AI-Empowered Internet of Things for Data-Driven Psychophysiological Computing and Patient Monitoring. IEEE J Biomed Health Inform. 2024 May 6; 28(5): 2496–9.
30. Abdelghani W, Zayani CA, Amous I, Sèdes F. Trust evaluation model for attack detection in social internet of things. In International conference on risks and security of internet and systems. Cham: Springer International Publishing; 2018 Oct 16; 48–64.

 