e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

ANOMALY DETECTION IN IOT: MACHINE LEARNING APPROACHES

Manasa Batthula*1

*1Department Of Computer Science And Engineering, Vaagdevi Engineering College, India.

DOI: https://www.doi.org/10.56726/IRJMETS71702

ABSTRACT

The pervasive nature of the Internet of Things devices has revolutionized various sectors, enabling data-driven decision-making and automation. However, the massive influx of data from these devices also presents significant challenges, particularly in identifying anomalous behaviors that may indicate system failures, security breaches, or other critical issues. This research paper delves into the application of machine learning techniques for anomaly detection in IoT ecosystems, exploring various algorithms, methodologies, and their effectiveness in addressing the unique characteristics of IoT data. The paper also aims to explore the challenges and limitations of these techniques.

I. INTRODUCTION

The Internet of Things transforms different industries through its ability to gather enormous amounts of data from linked devices and sensors. The connectivity between IoT devices introduces substantial security weaknesses that position these systems as prime targets for cyberattacks together with anomalies[1]. Sophisticated analytical techniques must handle the aggressive data volume growth from IoT devices that serve every industrial sector, including healthcare and manufacturing, to achieve system reliability and security[2]. The identification of irregular patterns within the norm has become essential to protect IoT ecosystems from attacks and operational breakdowns[3]. The large amount of elaborate data produced by IoT systems makes anomaly detection challenging. Machine learning applied to IoT infrastructure shows great potential for building advanced and effective anomaly detection systems that both detect risks ahead of time and minimize their impact[4].

The quick advancement of the fourth industrial revolution through the Industrial Internet of Things and smart and sustainable manufacturing systems produces enormous quantities of data daily[5]. Current IIoT infrastructures need efficient anomaly detection systems due to this situation.

II. LITERATURE REVIEW

Sectors across the board have experienced a revolution through IoT because the system collects immense data from linked devices and sensors[6]. The connected nature of IoT devices exposes them to major security threats, which makes them particularly susceptible to cyberattacks and anomalies. Industrial expansion of IoT equipment between healthcare and manufacturing sectors has created vast increases in generated data that need complex analytical methods to maintain system dependability and security levels[7]. IoT ecosystems require anomaly detection for threat protection and operational stability because of the complex nature of their generated data[7]. The combination of machine learning methods with IoT systems brings hope to create powerful security systems that detect anomalies and then protect IoT systems from potential threats ahead of time[8].

Every day, the fast development of the fourth industrial revolution produces extensive amounts of data, including IoT data from manufacturing systems alongside smart, sustainable production[9]. IIoT systems require immediate implementation of effective anomaly detection protocols because of escalating data generation.

III. METHODOLOGY

3.1. Data Acquisition and Preprocessing

The initial step in any machine learning-based anomaly detection system is the acquisition and preprocessing of relevant data.

The process of data collection involves obtaining information from IoT devices in combination with network traffic and sensors in the system. The acquired data typically contains surplus data that negatively affects machine learning model effectiveness[10]. The conversion of raw data requires data preprocessing to make it

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

usable for analysis purposes. The data preprocessing techniques involve data cleaning and the combination of different datasets and implementing transformation and a reduction process to enhance data quality by addressing missing values and duplicate entries while fixing inconsistencies[11].

The preprocessed data becomes more suitable for classification by retaining its essential features through feature extraction methods before selecting the most important features for computational efficiency and better predictive power[12]. The removal of redundant data, together with improved clarity during representation, helps preprocessing systems improve detection neutrality.

3.2. Machine Learning Model Selection:

Anomaly detection within IoT utilizes many machine learning approaches where the optimal algorithms depend both on data characteristics and application specifications[13]. The supervised learning algorithm Support Vector Machines enables training through labeled datasets consisting of normal and anomalous points, enabling it to detect new instances as normal or anomalous[14].

The K-Means clustering method, together with autoencoders, operates under unsupervised learning to detect anomalies because they can work effectively without needing labeled data, and therefore, it is appropriate for challenging setups[15]. Supervised learning requires labeled data that could be challenging to obtain from IoT systems but results in high accuracy after practical training[16].

Unsupervised learning provides value to unlabeled data, although its detection accuracy might be lower and requires additional adjustment[17]. The hybrid approach in semi-supervised learning systems utilizes supervised and unsupervised methods to process labeled and unlabeled data so that detection performance increases.

Machine Learning Model	Reason for Selection
Support Vector Machines	SVMs enable training through labeled datasets consisting of normal and anomalous points, allowing them to effectively detect new instances as normal or anomalous.
K-Means Clustering	K-means clustering, along with autoencoders, operate under unsupervised learning to detect anomalies. They can work effectively without needing labeled data, making them appropriate for challenging setups where labeled data is difficult to obtain.
Autoencoder	Autoencoders, along with K-Means clustering, operate under unsupervised learning to detect anomalies. They can work effectively without needing labeled data, making them appropriate for challenging setups where labeled data is difficult to obtain.
Semi-Supervised Learning	Semi-supervised learning systems utilize a hybrid approach, combining supervised and unsupervised methods to process labeled and unlabeled data. This approach can increase detection performance by leveraging both labeled and unlabeled data sources.

3.3. Model Training and Evaluation:

Training begins after selecting a proper machine learning model, where researchers feed representative datasets to train them in learning typical behavioral patterns. A split of the data into separate training and testing sections enables model training on the training set followed by testing set performance evaluation[18]. Anomaly detection models can be evaluated using precision and recall and the F1-score alongside the area under the receiver operating characteristic curve[19, 20].

Anomaly detection system efficiency stems from proper training and validation of the model. During training, the model adjusts its parameters through optimization methods until the actual values are close to the predicted ones[21,22]. Performance evaluation of models involves using accuracy in combination with precision and recall as well as F1-score metrics. These performance measurement tools provide evidence about anomaly detection capabilities alongside the ability to reduce both incorrect positive and negative results.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

IV. RESULTS

4.1. Performance Metrics and Analysis

Evaluation of the proposed anomaly detection system happens through precision-recall F1-score and area under the receiver operating characteristic curve metrics[23,24]. The precision performance metric rates the fraction of proper anomaly detections from flagged incidents, yet Recall rates proper anomaly detections compared to the total actual anomalies. A systematic measure of overall system performance emerges through the F1-score calculation based on precision and recall combined with their harmonic mean[25,26].

AUC-ROC evaluates the relationship between positive predictive values and negative detections from different boundary settings to determine optimal capabilities[27,28]. Model evaluation measures better performance through a higher AUC value. Machine learning operations and security domains use false positives and false negatives as indicators of model anomaly detection precision. The F-measure operates as an appraisal metric, but it needs modification to evaluate unbalanced datasets.

Model performance metrics that take time series patterns into account should be used in anomaly detection analyses since standard metrics often reward methods that only detect long anomalies by ignoring temporal relevance. The use of cross-validation scores enables assessment of how well the model will perform with new data.

4.2. Comparative Analysis

The proposed anomaly detection system needs performance evaluation through comparison against existing anomaly detection techniques. The proposed detection method must provide better results than existing approaches when measuring precision, recall, F1-score, and AUC-ROC, thus proving its capability to detect anomalies in IoT environments[29,30].

The Random Forest model demonstrates a high ability in anomaly detection through its effective performance and accuracy alongside precision and recall and F1-score measurements[31]. Anomaly detection assessment standards depend on the purposes but necessitate early anomaly identification to prevent the negative aftermath from anomalies. Research involving anomaly detection systems should utilize diverse anomaly types and multiple benchmark datasets for a complete evaluation of their abilities.

Comparative Analysis	Description
Proposed Anomaly Detection System	The proposed anomaly detection system needs to be evaluated through comparison against existing anomaly detection techniques. The proposed detection method must provide better results than existing approaches when measuring precision, recall, F1-score, and AUC-ROC, thus proving its highest capability for detecting anomalies in IoT environments.
Random Forest Model	The Random Forest model demonstrates high ability in anomaly detection through its effective performance with accuracy alongside precision and recall and F1-score measurements.
Performance Evaluation Standards	Anomaly detection assessment standards depend on the purposes but necessitate early anomaly identification to prevent the negative aftermath from anomalies. Research involving anomaly detection systems should utilize diverse anomaly types and multiple benchmark datasets for a complete evaluation of their abilities.
Evaluation Metrics	The experiments use a parameter set to 1 within the F-measure calculation involving precision and recall measurement. Classification performance evaluation using macro-averaging considers every class equally, which reduces the impact of dominated classes. The AUC-PR curve applies to situations when positive class identification matters more than negative class identification because the AUC tends to generate overestimated model performance results.

The experiments use a parameter set to 1 within the F-measure calculation involving precision and recall measurement. Classification performance evaluation using macro-averaging considers every class equally, which reduces the impact of dominated classes[32,33].

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

The AUC-PR curve applies to situations when positive class identification matters more than negative class identification because the AUC tends to generate overestimated model performance results.

V. DISCUSSION

The discussion examines the importance of interpretability and explainability in anomaly detection models for IoT systems. It highlights the need for stakeholders to understand the decision-making processes of complex machine learning models to foster trust and acceptance of these systems in IoT deployments.

5.1. Interpretability and Explainability:

The explanation of anomaly detection models and their interpretation play a crucial role in the implementation of IoT systems since trust and transparency remain fundamental requirements. Amid their decision-making complexity, deep neural networks, along with other machine learning models, remain "black boxes" because people struggle to grasp their decision processes. Popular analysis methods, like feature importance analysis and SHAP values, enable stakeholders to learn about the elements that lead to anomalous detection outcomes[31].

The human-readable nature of interpretability systems facilitates both the discovery of anomaly root causes and proper remedy implementation[34,35]. The explanation of anomaly detection results increases both stakeholder trust and system acceptance, which creates conditions for wider IoT implementation.

AI explainability remains vital because machine systems directly affect human life. The user acceptance of AI systems increases when they know the reasons behind specific decisions made by the system. AI systems become more understandable due to explainable AI approaches that lead users to trust these programs while adopting them [36].

5.2. Real-time Processing and Scalability:

The real-time data creation by IoT environments pushes the demand for anomaly detection systems that process data streams rapidly. The ability to handle large-scale growth is another significant consideration since IoT devices and sensors usually increase substantially during the period. Apache Spark and Apache Kafka serve as distributed computing frameworks to process real-time data through horizontal scaling across multiple nodes for anomaly detection algorithms [37].

The continuous model update process during online learning improves real-time processing efficiency through the use of newly received data. The modern optimization methods enhance both the efficiency and effectiveness of adjustable deep learning models, which leads to better anomaly detection capabilities and stronger cybersecurity outcomes. During the IoT device anomaly detection system design, it is essential to weigh both the model's complexity level and the amount of resources it needs to operate effectively.

5.3. Security and Privacy Considerations:

Security and privacy require top priority status because IoT devices commonly operate in sensitive areas, including healthcare facilities and smart household environments. The security provisions of anomaly detection systems should protect user information privacy while maintaining and blocking unauthorized access to sensitive data types.

Through distributed machine learning principles known as federated learning models, one can acquire training from decentralized data repositories without needing to transmit actual data by itself. Through this method, organizations can accomplish better privacy protection and preserve anomaly detection model precision rates [38].

The implementation of differential privacy methods allows researchers to incorporate data noise, which protects sensitive information from disclosure. To prevent evasion, anomaly detection systems must have immunity against adversarial attacks that attempt manipulation of data or models.

Blockchain presents a solution to resolve storage space and processing capacity issues that affect intrusion detection systems when used within IoT environments. Blockchain technology generates decentralized audit logs that operate immutably to detect security breaches and prevent unauthorized actions.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

5.4. Adaptability to Dynamic Environments:

Blockchain presents a solution to resolve storage space and processing capacity issues that affect intrusion detection systems when used within IoT environments. The decentralized system of blockchain technology creates security audit logs that function as a detection and prevention mechanism against security breaches.

The continuous model updating process of online learning algorithms, which uses new data, helps achieve better adaptability. Anomaly detection systems need to add feedback capabilities that enable them to gain knowledge from historical errors to enhance their operational capabilities [39].

Machine learning anomaly detection represents a valid approach for anomaly identification, although it requires development to analyze evolving network designs and advanced attack methods. A reliable system for detecting anomalous network intrusions can be developed through a deep learning algorithm ensemble with stacking generalization methods.

VI. CONCLUSION

The research evaluates machine learning applications for anomaly detection in IoT networks while focusing on the individual difficulties that IoT environments present. A detailed introduction to anomaly detection included basic concepts alongside different anomaly categories and specific challenges caused by IoT data. The analysis assessed machine learning methods from supervised, unsupervised, and semi-supervised classifications in addition to their adaptability for different IoT anomaly detection conditions. The study presented an in-depth analysis of deep learning techniques, including autoencoders, recurrent neural networks, and convolutional neural networks for extracting complex IoT data features and effectively detecting minor anomalies. Both Spider Monkey Optimization and Stacked-Deep Polynomial Network work together to improve intrusion detection accuracy.

The paper examined ensemble learning techniques because they enable optimal performance improvement by uniting different model strengths. The study resolved various important matters, consisting of feature engineering, model selection, real-time processing, scalability, security, privacy, and adaptability to dynamic situations. Future research directions include the development of more robust and explainable anomaly detection models, investigating federated learning techniques for privacy-preserving anomaly detection, and developing adaptive anomaly detection systems capable of responding to evolving IoT environments. Machine learning-based anomaly detection systems will assume a more crucial position in securing IoT deployments through the solution of identified challenges and implementation of research directions across multiple industries and applications.

VII. REFERENCES

[1] D. Javeed, T. Gao, and M. T. Khan, "SDN-Enabled Hybrid DL-Driven Framework for the Detection of Emerging Cyber Threats in IoT," Apr. 12, 2021, Multidisciplinary Digital Publishing Institute. doi: 10.3390/electronics10080918.

[2] Nasib, N., Addula, S. R., Jain, A., Gulia, P., Gill, N. S., & V., B. D. (2024). Systematic analysis based on the conflux of machine learning and the Internet of Things using bibliometric analysis. Journal of Intelligent Systems and Internet of Things, 13(1), 196-224. https://doi.org/10.54216/jisiot.130115

[3] Konda, B. (2022). The Impact of Data Preprocessing on Data Mining Outcomes. World Journal of Advanced Research and Reviews, 15(3): 540-544

[4] D. Kumar, P. Pawar, H. Gonaygunta, and S. Singh, "Impact of Federated Learning on Industrial IoT - A Review," IJARCCE, vol. 13, no. 1. Dec. 30, 2023. doi: 10.17148/ijarcce.2024.13105.

[5] R. Daruvuri, “Harnessing vector databases: A comprehensive analysis of their role across industries,” International Journal of Science and Research Archive, vol. 7, no. 2, pp. 703–705, Dec. 2022, doi: 10.30574/ijsra.2022.7.2.0334.

[6] S. F. Chevtchenko et al., "Anomaly Detection in Industrial Machinery using IoT Devices and Machine Learning: a Systematic Mapping," arXiv (Cornell University), Jan. 2023, doi: 10.48550/arxiv.2307.15807.

[7] M. Yang and J. Zhang, "Data Anomaly Detection in the Internet of Things: A Review of Current Trends and Research Challenges," International Journal of Advanced Computer Science and Applications, vol. 14, no. 9. Science and Information Organization, Jan. 01, 2023. doi: 10.14569/ijacsa.2023.0140901.

[8] D. Kumar, P. Pawar, A. Bhuvanesh, S. Indhumathi, and M. Murugan, "ChOs_LSTM: Chebyshev Osprey Optimization-Based Model for Detecting Attacks," May 03, 2024.
doi: 10.1109/aiiot58432.2024.10574586.

[9] S. R. Addula and G. Sekhar Sajja, "Automated Machine Learning to Streamline Data-Driven Industrial Application Development," 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), Lucknow, India, 2024, pp. 1-4, doi: 10.1109/IC3TES62412.2024.10877481.

[10] S. E. Vadakkethil, K. Polimetla, Z. Alsalami, P. K. Pareek, and D. Kumar, "Mayfly Optimization Algorithm with Bidirectional Long-Short Term Memory for Intrusion Detection System in Internet of Things," Apr. 26, 2024. doi: 10.1109/icdcece60827.2024.10549401.

[11] K. Rahul, R. K. Banyal, and P. Goswami, "Analysis and processing aspects of data in big data applications," Feb. 17, 2020, Taylor & Francis. doi: 10.1080/09720529.2020.1721869.

[12] M. Kang and J. Tian, "Machine Learning: Data Preprocessing." p. 111, Aug. 24, 2018. doi: 10.1002/9781119515326.ch5.

[13] C. Cavallaro, V. Cutello, M. Pavone, and F. Zito, "Discovering anomalies in big data: a review focused on the application of metaheuristics and machine learning techniques," Frontiers in Big Data, vol. 6. Frontiers Media, Aug. 17, 2023. doi: 10.3389/fdata.2023.1179625.

[14] N. Davis, G. Raina, and K. Jagannathan, "A framework for end-to-end deep learning-based anomaly detection in transportation networks," May 01, 2020, Elsevier BV. doi: 10.1016/j.trip.2020.100112.

[15] T. Amarbayasgalan, B. Jargalsaikhan, and K. H. Ryu, "Unsupervised Novelty Detection Using Deep Autoencoders with Density-Based Clustering," Applied Sciences, vol. 8, no. 9, p. 1468, Aug. 2018, doi: 10.3390/app8091468.

[16] Yadulla, A. R., Yenugula, M., Kasula, V. K., Konda, B., Addula, S. R., & Rakki, S. B. (2023). A time-aware LSTM model for detecting criminal activities in blockchain transactions. International Journal of Communication and Information Technology, 4(2): 33-39

[17] A. Haque, M. N.-U.-R. Chowdhury, H. Soliman, M. S. Hosseini, T. Fatima, and I. Ahmed, "Wireless Sensor Networks anomaly detection using Machine Learning: A Survey," arXiv (Cornell University), Jan. 2023, doi: 10.48550/arXiv.2303.

[18] T. Islam, A. Miron, M. Nandy, J. Choudrie, X. Liu, and Y. Li, "Transforming Digital Marketing with Generative AI," Computers, vol. 13, no. 7, p. 168, Jul. 2024, doi: 10.3390/computers13070168.

[19] M. López-Vizcaíno, F. J. Nóvoa, D. Fernández, and F. Cacheda, “Measuring Early Detection of Anomalies,” Jan. 01, 2022, Institute of Electrical and Electronics Engineers. doi: 10.1109/access.2022.3224467.

[20] K. Patibandla and R. Daruvuri, "Reinforcement deep learning approach for multi-user task offloading in edge-cloud joint computing systems," International Journal of Research in Electronics and Computer Engineering, vol. 11, no. 3, pp. 47-58, 2023.

[21] W. Hwang, J.-H. Yun, J. Kim, and H. C. Kim, "Time-Series Aware Precision and Recall for Anomaly Detection," Nov. 03, 2019. doi: 10.1145/3357384.3358118.

[22] K. Doshi, S. Abudalou, and Y. Yılmaz, "TiSAT: Time Series Anomaly Transformer," arXiv (Cornell University), Jan. 2022, doi: 10.48550/arXiv.2203.

[23] Z. DeVries et al., "Development of an unsupervised machine learning algorithm for the prognostication of walking ability in spinal cord injury patients," Sep. 13, 2019, Elsevier BV. doi: 10.1016/j.spinee.2019.09.007.

[24] Kasula, V. K., Yadulla, A. R., Yenugula, M., & Konda, B. (2024, November). Enhancing Smart Contract Vulnerability Detection using Graph-Based Deep Learning Approaches. In 2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS) (pp. 1-6). IEEE.

[25] H. Gonaygunta, G. S. Nadella, P. Pawar, and D. Kumar, "Enhancing Cybersecurity: The Development of a Flexible Deep Learning Model for Enhanced Anomaly Detection," May 03, 2024. doi: 10.1109/sieds61124.2024.10534661.

[26] G. Singh, "Wearable IoT (w-IoT) artificial intelligence (AI) solution for sustainable smart-healthcare," Dec. 30, 2024, Elsevier BV. doi: 10.1016/j.jjimei.2024.100291.

[27] L. C. Brito, G. A. Susto, J. N. Brito, and M. A. V. Duarte, "An Explainable Artificial Intelligence Approach for Unsupervised Fault Detection and Diagnosis in Rotating Machinery," Jan. 01, 2021, Cornell University. doi: 10.48550/arXiv.2102.

[28] P. Pawar, D. Kumar, M. K. Meesala, P. K. Pareek, S. R. Addula, and K. S. Shwetha, "Securing Digital Governance: A Deep Learning and Blockchain Framework for Malware Detection in IoT Networks," Nov. 22, 2024. doi: 10.1109/iciics63763.2024.10860155.

[29] Kasula, V. K., Konda, B., Yadulla, A. R., & Yenugula, M. (2022). Hybrid Short Comparable Encryption with Sliding Window Techniques for Enhanced Efficiency and Security. International Journal of Science and Research Archive, 5(01), 151-161

[30] Addula, S. R., Tyagi, A. K., Naithani, K., & Kumari, S. (2024). Blockchain-empowered Internet of Things (IoTs) platforms for automation in various sectors. Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing, 443-477. https://doi.org/10.1002/9781394303601.ch20

[31] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," Jan. 01, 2020, Institute of Electrical and Electronics Engineers. doi: 10.1109/comst.2020.2986444.

[32] J. W. Sipple and A. Youssef, "A general-purpose method for applying Explainable AI for Anomaly Detection," arXiv (Cornell University), Jan. 2022, doi: 10.48550/arxiv.2207.11564.

[33] K.-J. Jeong, J.-D. Park, K. Hwang, S. Kim, and W.-Y. Shin, "Two-Stage Deep Anomaly Detection With Heterogeneous Time Series Data," Jan. 01, 2022, Institute of Electrical and Electronics Engineers. doi: 10.1109/access.2022.3147188.

[34] D. Fourure, M. U. Javaid, N. Posocco, and S. Tihon, "Anomaly Detection: How to Artificially Increase your F1-Score with a Biased Evaluation Protocol," arXiv (Cornell University), Jan. 2021, doi: 10.48550/arxiv.2106.16020.

[35] R. Daruvuri, "Efficient CSI feedback for large-scale MIMO IoT systems using YOLOv8-based network," in Proc. 1st IEEE Conf. Secure and Trustworthy CyberInfrastructure for IoT and Microelectronics (SaTC), Ohio, USA, 2025, pp. 1–5.

[36] F. Ayed, L. Stella, T. Januschowski, and J. Gasthaus, "Anomaly Detection at Scale: The Case for Deep Distributional Time Series Models," in Lecture notes in computer science, Springer Science+Business Media, 2021, p. 97. doi: 10.1007/978-3-030-76352-7_14.

[37] N. A. Stoian, "Machine Learning for anomaly detection in IoT networks :Malware analysis on the IoT-23 data set," 2020. Accessed: Mar. 2025. [Online]. Available: https://essay.utwente.nl/81979/

[38] S. F. Chevtchenko et al., "Anomaly Detection in Industrial Machinery Using IoT Devices and Machine Learning: A Systematic Mapping," Jan. 01, 2023, Institute of Electrical and ElectronicsEngineers. doi: 10.1109/access.2023.3333242.

[39] Yenugula, M., Yadulla, A. R., Konda, B., Addula, S. R., & Kasula, V. K. (2023). Enhancing Mobile Data Security with Zero-Trust Architecture and Federated Learning: A Comprehensive Approach to Prevent Data Leakage on Smart Terminals. JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 11(1), 52-64.