International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November-December 2025||

DOI:10.15662/IJRPETM.2025.0806018

AI-Based Intrusion Detection Systems for Organizational Cybersecurity

Ajay Chakravarty

Research Scholar, CCSIT, Teerthanker Mahaveer University Moradabad, India

ajay.chakravarty1@gmail.com

ABSTRACT: The rapid digital transformation of organizations has significantly increased their exposure to cyber threats, making traditional security mechanisms insufficient to counter sophisticated and evolving attacks. Intrusion Detection Systems (IDS) play a critical role in organizational cybersecurity by monitoring network traffic and system activities to identify malicious behavior. However, conventional IDS, which rely heavily on predefined signatures and static rules, often struggle with high false-positive rates and an inability to detect zero-day and advanced persistent threats. To address these limitations, Artificial Intelligence (AI)-based Intrusion Detection Systems have emerged as a powerful and adaptive solution.

AI-based IDS leverage machine learning and deep learning techniques to analyze large volumes of heterogeneous data generated across organizational networks, endpoints, and applications. By learning normal behavioral patterns and identifying deviations, these systems can effectively detect both known and unknown attacks. Supervised learning models enable accurate classification of previously observed threats, while unsupervised and semi-supervised approaches are particularly effective in anomaly detection where labeled data is scarce. Deep learning architectures, such as neural networks, further enhance detection capabilities by capturing complex, non-linear relationships within high-dimensional security data.

The integration of AI into IDS provides several advantages for organizations, including improved detection accuracy, reduced false alarms, real-time threat identification, and scalability across complex enterprise environments. AI-driven systems can continuously adapt to evolving attack patterns, making them suitable for dynamic infrastructures such as cloud computing and Internet of Things (IoT) ecosystems. Additionally, AI-based IDS can be integrated with automated response mechanisms, enabling faster mitigation of threats and minimizing potential damage.

Despite their advantages, AI-based Intrusion Detection Systems face several challenges. These include the need for large, high-quality datasets, significant computational resources for model training, vulnerability to adversarial attacks, and concerns related to data privacy and regulatory compliance. Moreover, the lack of explainability in certain AI models can hinder trust and decision-making for security analysts. Addressing these challenges requires a balanced approach that combines advanced AI techniques with explainable models, robust data governance, and human expertise.AI-based Intrusion Detection Systems represent a significant advancement in organizational cybersecurity by providing intelligent, adaptive, and proactive threat detection. When effectively implemented alongside traditional security controls and governance frameworks, they enhance an organization's ability to protect critical assets, maintain operational resilience, and respond efficiently to the rapidly evolving cyber threat landscape.

KEYWORDS: AI-based intrusion detection, cybersecurity, machine learning, deep learning, anomaly detection, network security, organizational security, zero-day attacks, Security Automation

I. INTRODUCTION

In today's highly interconnected digital environment, organizations increasingly rely on information systems, cloud platforms, and networked applications to support critical business operations. While this technological advancement improves efficiency and scalability, it also expands the attack surface for cyber threats, including malware, insider attacks, data breaches, and advanced persistent threats. Traditional security mechanisms such as firewalls and signature-based Intrusion Detection Systems (IDS) are no longer sufficient to address the complexity and sophistication of modern cyberattacks, as they depend on predefined rules and known attack patterns. As a result, organizations face challenges in detecting unknown threats, responding in real time, and reducing false alarms. Artificial Intelligence (AI)-based Intrusion Detection Systems have emerged as a promising solution to these challenges by leveraging machine

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November-December 2025||

DOI:10.15662/IJRPETM.2025.0806018

learning and deep learning techniques to analyze vast amounts of security data, identify abnormal behavior, and adapt to evolving attack strategies. By enabling intelligent, automated, and proactive threat detection, AI-based IDS play a crucial role in strengthening organizational cybersecurity and ensuring the confidentiality, integrity, and availability of digital assets.

II. LITERATURE REVIEW

Research on intrusion detection systems (IDS) has evolved from **signature- and rule-based approaches** toward **data-driven AI models** because modern attacks (e.g., multi-stage intrusions and zero-day exploits) often evade static signatures. Recent surveys emphasize that machine learning (ML) and deep learning (DL) methods can improve detection by learning patterns from traffic flows, logs, and host telemetry, while also highlighting persistent challenges such as class imbalance, concept drift, and operational deployment constraints. A comprehensive review of AI-based IDS literature summarizes how supervised, unsupervised, and hybrid learning methods are applied across network-based and host-based IDS, and identifies future needs such as robustness and real-time adaptability.

Early ML-based IDS research commonly applied **classical classifiers**—including Logistic Regression, Decision Trees, Random Forests, SVM, and shallow neural networks—due to their interpretability and lower computational cost. Studies comparing these models often show that ensemble learners (notably Random Forest and boosting variants) perform strongly on structured flow features when data is well-prepared and feature selection is applied. For example, recent work using the **UNSW-NB15** dataset demonstrates that classical ML models combined with exploratory data analysis and feature selection can yield competitive results, reinforcing the value of "strong baselines" before adopting more complex DL architectures.

With growing traffic volumes and complex attack behavior, DL-based IDS has gained prominence. Surveys and reviews report extensive use of **CNNs, RNN/LSTM, autoencoders, and hybrid DL pipelines** to capture non-linear and temporal patterns in high-dimensional security data. DL models are frequently positioned as more capable for multi-class attack detection and learning latent representations, particularly when raw or semi-processed features are available. However, the same reviews also note that DL systems can be sensitive to data quality, imbalance, and distribution shifts, which can reduce real-world generalization.

A major portion of IDS literature relies on benchmark datasets. Widely used datasets include **CICIDS2017** (flows and PCAPs with labeled attack scenarios) and **UNSW-NB15** (hybrid real + synthetic attack traffic with multiple attack families). These datasets are popular because they are publicly accessible and support repeatable evaluation. At the same time, multiple studies caution that benchmark datasets can embed artifacts and biases that inflate performance if preprocessing and splits are not carefully designed (e.g., leakage, duplicated patterns, or unrealistic distributions).

Domain-specific environments have also shaped IDS research directions. For IoT and distributed systems, surveys highlight constraints such as limited device resources, heterogeneous protocols, and high noise, motivating lightweight models, edge-assisted detection, and specialized feature engineering. In parallel, organizational adoption increasingly demands transparency and auditability, leading to growing interest in **Explainable AI (XAI)** for IDS to help analysts understand alerts and support compliance—while also acknowledging that explanations can introduce new security and privacy risks if not handled carefully.

Overall, the literature indicates that AI-based IDS is most effective when paired with (1) high-quality telemetry pipelines, (2) rigorous evaluation protocols that avoid leakage and reflect deployment realities, and (3) operational integration with SOC workflows (triage, correlation, and response). Current research trends increasingly focus on **robustness (including adversarial resilience), generalization across networks, explainability, and privacy-preserving learning**, aiming to bridge the gap between high benchmark accuracy and dependable organizational security outcomes.

III. RESEARCH METHODOLOGY

This study adopts a **quantitative and experimental research methodology** to evaluate the effectiveness of AI-based Intrusion Detection Systems (IDS) in enhancing organizational cybersecurity. The methodology is designed to systematically analyze intrusion detection performance using machine learning and deep learning techniques on benchmark cybersecurity datasets.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November-December 2025||

DOI:10.15662/IJRPETM.2025.0806018

The research begins with **data collection**, utilizing publicly available and widely accepted intrusion detection datasets such as CICIDS2017 and UNSW-NB15. These datasets contain both normal and malicious network traffic representing real-world attack scenarios, making them suitable for training and evaluating AI-based IDS models. Data preprocessing is performed to ensure quality and consistency, including data cleaning, handling missing values, normalization, and removal of redundant or irrelevant features.

Next, **feature extraction and selection** techniques are applied to identify the most relevant attributes that contribute to accurate intrusion detection. This step reduces dimensionality, improves computational efficiency, and enhances model performance. Statistical methods and correlation analysis are used to eliminate noisy or highly correlated features.

The core phase involves **model development and training**. Multiple AI algorithms are implemented to provide a comparative analysis, including supervised machine learning models (such as Decision Trees, Random Forests, and Support Vector Machines) and deep learning models (such as Artificial Neural Networks or Long Short-Term Memory networks). The dataset is divided into training and testing subsets using appropriate data-splitting techniques to avoid overfitting and data leakage.

For **model evaluation**, standard performance metrics are employed, including accuracy, precision, recall, F1-score, and false positive rate. These metrics allow a comprehensive assessment of the IDS's ability to correctly detect intrusions while minimizing false alarms. Cross-validation techniques are used to ensure the reliability and robustness of the results.

Finally, a **comparative and analytical approach** is used to interpret the findings. The performance of AI-based IDS models is compared against traditional detection approaches to highlight improvements and limitations. The results are analyzed to determine suitability for organizational environments, considering factors such as scalability, detection efficiency, and adaptability to evolving threats.

This structured methodology ensures the research outcomes are objective, reproducible, and relevant for real-world organizational cybersecurity applications.

IV. RESULTS

The experimental evaluation of the AI-based Intrusion Detection System demonstrates a significant improvement in intrusion detection performance compared to traditional rule-based approaches. After preprocessing and feature selection, the trained machine learning and deep learning models were tested on benchmark datasets containing both normal and malicious network traffic. The results indicate that AI-based models achieved **high detection accuracy**, with supervised learning algorithms such as Random Forest and Support Vector Machines performing consistently well in classifying known attack patterns. Deep learning models further enhanced detection capability by effectively identifying complex and previously unseen attack behaviors.

Across all experiments, the AI-based IDS showed a **notable reduction in false positive rates**, which is a critical requirement for organizational cybersecurity environments where excessive alerts can overwhelm security teams. Precision and recall values were significantly improved, indicating the system's ability to correctly identify malicious activities while minimizing misclassification of legitimate traffic. In particular, deep learning models demonstrated strong recall, making them effective in detecting subtle and multi-stage attacks that are difficult for traditional IDS to identify.

Comparative analysis revealed that AI-based IDS outperformed conventional signature-based systems, especially in detecting **zero-day and anomaly-based attacks**. The models adapted well to diverse traffic patterns and maintained stable performance across different attack categories. Cross-validation results further confirmed the robustness and generalizability of the proposed approach, with minimal performance variation across training and testing subsets.

Overall, the results validate the effectiveness of AI-based Intrusion Detection Systems in enhancing organizational cybersecurity. The findings highlight their capability to provide accurate, scalable, and adaptive threat detection, making them suitable for deployment in modern enterprise environments. However, the results also suggest that optimal performance depends on high-quality datasets and proper model tuning, emphasizing the importance of continuous monitoring and model updates in real-world implementations.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November-December 2025||

DOI:10.15662/IJRPETM.2025.0806018

V. CONCLUSION

This study concludes that **AI-based Intrusion Detection Systems (IDS)** play a vital role in strengthening organizational cybersecurity in the face of increasingly sophisticated and dynamic cyber threats. Unlike traditional signature-based IDS, which are limited to detecting known attack patterns, AI-driven approaches demonstrate the ability to identify both known and unknown intrusions by learning complex behavioral patterns from large volumes of security data. The experimental results confirm that machine learning and deep learning models significantly improve detection accuracy while reducing false positive rates, addressing one of the major challenges faced by security operations teams.

The findings further indicate that AI-based IDS are highly adaptable and scalable, making them suitable for modern organizational environments such as cloud computing, large enterprise networks, and distributed systems. Their capability to detect zero-day attacks and anomalous behavior highlights their effectiveness in proactive threat detection and early response. However, the study also acknowledges challenges related to data quality, computational requirements, and model interpretability, which must be carefully managed for successful real-world deployment.

In conclusion, AI-based Intrusion Detection Systems offer a robust and intelligent security solution when integrated with existing cybersecurity frameworks and supported by skilled human oversight. Continuous model training, proper data governance, and explainable AI techniques are essential to maximize their effectiveness. As cyber threats continue to evolve, AI-based IDS will remain a key component in ensuring the confidentiality, integrity, and availability of organizational information systems.

REFERENCES

1. Mahajan, R. A., Shaikh, N. K., Tikhe, A. B., Vyas, R., & Chavan, S. M. (2022). Hybrid Sea Lion Crow Search Algorithm-based stacked autoencoder for drug sensitivity prediction from cancer cell lines. International Journal of Swarm Intelligence Research, 13(1), 21. https://doi.org/10.4018/IJSIR.304723
2. Rathod, S. B., Ponnusamy, S., Mahajan, R. A., & Khan, R. A. H. (n.d.). Echoes of tomorrow: Navigating business realities with AI and digital twins. In Harnessing AI and digital twin technologies in businesses (Chapter 12). https://doi.org/10.4018/979-8-3693-3234-4.ch012
3. Rathod, S. B., Khandizod, A. G., & Mahajan, R. A. (n.d.). Cybersecurity beyond the screen: Tackling online harassment and cyberbullying. In AI tools and applications for women's safety (Chapter 4). https://doi.org/10.4018/979-8-3693-1435-7.ch004
4. Devan, Karthigayan. "ENHANCING CONCOURSE CI/CD PIPELINES WITH REAL-TIME WEBHOOK TRIGGERS: A SCALABLE SOLUTION FOR GITHUB RESOURCE MANAGEMENT."
5. Devan, K. (2025). Leveraging the AWS cloud platform for CI/CD and infrastructure automation in software development. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5049844
6. evan K, Driving Digital Transformation: LeveragingSite Reliability Engineering and Platform Engineeringfor Scalable and Resilient Systems. Appl. Sci. Eng. J.Adv. Res.. 2025;4(1):21-29.
7. Karthigayan Devan. (2025). Api Key-Driven Automation for Granular Billing Insights: An Sre and Finops Approach to Google Maps Platform Optimization. International Journal of Communication Networks and Information Security (IJCNIS), 17(1), 58–65. Retrieved from https://ijcnis.org/index.php/ijcnis/article/view/7939
8. P. Bavadiya, P. Upadhyaya, A. C. Bhosle, S. Gupta, and N. Gupta, "AI-driven Data Analytics for Cyber Threat Intelligence and Anomaly Detection," in 2025 3rd International Conference on Advancement in Computation & Computer Technologies (InCACCT), 2025, pp. 677–681. doi: 10.1109/InCACCT65424.2025.11011329.
9. Pathik Bavadiya. (2021). A Framework for Resilient Devops Automation in Multi-Cloud KubernetesEcosystems. Journal of Informatics Education and Research, 1(3), 61–66. https://jier.org/index.php/journal/article/view/3584
10. Gupta, P. K., Nawaz, M. H., Mishra, S. S., Roy, R., Keshamma, E., Choudhary, S., ... & Sheriff, R. S. (2020). Value Addition on Trend of Tuberculosis Disease in India-The Current Update. Int J Trop Dis Health, 41(9), 41-54.
11. Hiremath, L., Kumar, N. S., Gupta, P. K., Srivastava, A. K., Choudhary, S., Suresh, R., & Keshamma, E. (2019). Synthesis, characterization of TiO2 doped nanofibres and investigation on their antimicrobial property. J Pure Appl Microbiol, 13(4), 2129-2140.
12. Gupta, P. K., Lokur, A. V., Kallapur, S. S., Sheriff, R. S., Reddy, A. M., Chayapathy, V., ... & Keshamma, E. (2022). Machine Interaction-Based Computational Tools in Cancer Imaging. Human-Machine Interaction and IoT Applications for a Smarter World, 167-186.
13. Gopinandhan, T. N., Keshamma, E., Velmourougane, K., & Raghuramulu, Y. (2006). Coffee husk-a potential source of ochratoxin A contamination.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November-December 2025||

DOI:10.15662/IJRPETM.2025.0806018

14. Keshamma, E., Rohini, S., Rao, K. S., Madhusudhan, B., & Udaya Kumar, M. (2008). In planta transformation strategy: an Agrobacterium tumefaciens-mediated gene transfer method to overcome recalcitrance in cotton (Gossypium hirsutum L.). J Cotton Sci, 12, 264-272.
15. Gupta, P. K., Mishra, S. S., Nawaz, M. H., Choudhary, S., Saxena, A., Roy, R., & Keshamma, E. (2020). Value Addition on Trend of Pneumonia Disease in India-The Current Update.
16. Sumanth, K., Subramanya, S., Gupta, P. K., Chayapathy, V., Keshamma, E., Ahmed, F. K., & Murugan, K. (2022). Antifungal and mycotoxin inhibitory activity of micro/nanoemulsions. In Bio-Based Nanoemulsions for Agri-Food Applications (pp. 123-135). Elsevier.
17. Hiremath, L., Sruti, O., Aishwarya, B. M., Kala, N. G., & Keshamma, E. (2021). Electrospun nanofibers: Characteristic agents and their applications. In Nanofibers-Synthesis, Properties and Applications. IntechOpen.
18. Dash, P., Javaid, S., & Hussain, M. A. (2025). Empowering Digital Business Innovation: AI, Blockchain, Marketing, and Entrepreneurship for Dynamic Growth. In Perspectives on Digital Transformation in Contemporary Business (pp. 439-464). IGI Global Scientific Publishing.
19. Hussain, M. A., Hussain, A., Rahman, M. A. U., Irfan, M., & Hussain, S. D. (2025). The effect of AI in fostering customer loyalty through efficiency and satisfaction. Advances in Consumer Research, 2, 331-340.
20. Shanthala, K., Chandrakala, B. M., & Shobha, N. (2023, November). Automated Diagnosis of brain tumor classification and segmentation of MRI Images. In 2023 International Conference on the Confluence of Advancements in Robotics, Vision and Interdisciplinary Technology Management (IC-RVITM) (pp. 1-7). IEEE.
21. Karthik, S. A., Naga, S. B. V., Satish, G., Shobha, N., Bhargav, H. K., & Chandrakala, B. M. (2025). Ai and iot-infused urban connectivity for smart cities. In Future of Digital Technology and AI in Social Sectors (pp. 367-394). IGI Global.
22. Godi, R. K., P, S. R., N, S., Bhoothpur, B. V., & Das, A. (2025). A highly secure and stable energy aware multi-objective constraints-based hybrid optimization algorithms for effective optimal cluster head selection and routing in wireless sensor networks. Peer-to-Peer Networking and Applications, 18(2), 97.
23. Nagar, H., & Menaria, A. K. Compositions of the Generalized Operator ($\boldsymbol{G\rho}$, $\boldsymbol{\eta}$, $\boldsymbol{\gamma}$, $\boldsymbol{\omega}$; $\boldsymbol{a}$ $\boldsymbol{\Psi}$)($\boldsymbol{x}$) and their Application.
24. NAGAR, H., & MENARIA, A. K. (2012). Applications of Fractional Hamilton Equations within Caputo Derivatives. Journal of Computer and Mathematical Sciences Vol, 3(3), 248-421.
25. Nagar, H., & Menaria, A. K. On Generalized Function Gρ, η, γ [a, z] And It's Fractional Calculus.
26. Rajoria, N. V., & Menaria, A. K. Numerical Approach of Fractional Integral Operators on Heat Flux and Temperature Distribution in Solid.
27. Polamarasetti, S. (2022). Using Machine Learning for Intelligent Case Routing in Salesforce Service Cloud. International Journal of AI, BigData, Computational and Management Studies, 3(1), 109-113.
28. Polamarasetti, S. (2021). Enhancing CRM Accuracy Using Large Language Models (LLMs) in Salesforce Einstein GPT. International Journal of Emerging Trends in Computer Science and Information Technology, 2(4), 81-85.
29. Polamarasetti, S. (2023). Conversational AI in Salesforce: A Study of Einstein Bots and Natural Language Understanding. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(3), 98-102.
30. RAMADUGU, G. (2023). CLOUD-NATIVE DIGITAL TRANSFORMATION: LESSONS FROM LARGE-SCALE DATA MIGRATIONS. International Journal of Innovation Studies, 7(1), 41-54.
31. Thota, S., Chitta, S., Vangoor, V. K. R., Ravi, C. S., & Bonam, V. S. M. (2023). Few-ShotLearning in Computer Vision: Practical Applications and Techniques. Human-Computer Interaction, 3(1).
32. Ravi, C. S., Bonam, V. S. M., & chitta, S. (2024, December). Hybrid Machine Learning Approaches for Enhanced Insurance Fraud Detection. In International Conference on Recent Trends in AI Enabled Technologies (pp. 93-104). Cham: Springer Nature Switzerland.
33. Madunuri, R., Chitta, S., Bonam, V. S. M., Vangoor, V. K. R., Yellepeddi, S. M., & Ravi, C. S. (2024, September). IoT-Driven Smart Healthcare Systems for Remote Patient Monitoring and Management. In 2024 Asian Conference on Intelligent Technologies (ACOIT) (pp. 1-7). IEEE.
34. Madunuri, R., Ravi, C. S., Chitta, S., Bonam, V. S. M., Vangoor, V. K. R., & Yellepeddi, S. M. (2024, September). Machine Learning-Based Anomaly Detection for Enhancing Cybersecurity in Financial Institutions. In 2024 Asian Conference on Intelligent Technologies (ACOIT) (pp. 1-8). IEEE.
35. Madunuri, R., Yellepeddi, S. M., Ravi, C. S., Chitta, S., Bonam, V. S. M., & Vangoor, V. K. R. (2024, September). AI-Enhanced Drug Discovery Accelerating the Identification of Potential Therapeutic Compounds. In 2024 Asian Conference on Intelligent Technologies (ACOIT) (pp. 1-8). IEEE.
36. Kumar, A. (2024). Intelligent Edge Computing Architecture for Low-Latency AI Processing in IoT Networks. Global Journal of Emerging Technologies and Multidisciplinary Research, 5(5).

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November-December 2025||

DOI:10.15662/IJRPETM.2025.0806018

37. Chitta, S., Yandrapalli, V. K., & Sharma, S. (2024, June). Optimizing SVM for Enhanced Lung Cancer Prediction: A Comparative Analysis with Traditional ML Models. In International Conference on Data Analytics & Management (pp. 143-155). Singapore: Springer Nature Singapore.
38. Whig, P., Balantrapu, S. S., Whig, A., Alam, N., Shinde, R. S., & Dutta, P. K. (2024, December). AI-driven energy optimization: integrating smart meters, controllers, and cloud analytics for efficient urban infrastructure management. In 8th IET Smart Cities Symposium (SCS 2024) (Vol. 2024, pp. 238-243). IET.
39. Polamarasetti, S., Kakarala, M. R. K., kumar Prajapati, S., Butani, J. B., & Rongali, S. K. (2025, May). Exploring Advanced API Strategies with MuleSoft for Seamless Salesforce Integration in Multi-Cloud Environments. In 2025 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC) (pp. 1-9). IEEE.
40. Polamarasetti, S., Kakarala, M. R. K., Gadam, H., Butani, J. B., Rongali, S. K., & Prajapati, S. K. (2025, May). Enhancing Strategic Business Decisions with AI-Powered Forecasting Models in Salesforce CRMT. In 2025 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC) (pp. 1-10). IEEE.
41. Polamarasetti, S., Kakarala, M. R. K., Goyal, M. K., Butani, J. B., Rongali, S. K., & kumar Prajapati, S. (2025, May). Designing Industry-Specific Modular Solutions Using Salesforce OmniStudio for Accelerated Digital Transformation. In 2025 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC) (pp. 1-13). IEEE.
42. Ravi, C., Shaik, M., Saini, V., Chitta, S., & Bonam, V. S. M. (2025). Beyond the Firewall: Implementing Zero Trust with Network Microsegmentation. Nanotechnology Perceptions, 21, 560-578.
43. Chitta, S., Sharma, S., & Yandrapalli, V. K. (2025). Hybrid Deep Learning Model for Enhanced Breast Cancer Diagnosis Using Histopathological Images. Procedia Computer Science, 260, 245-251. https://doi.org/10.1016/j.procs.2025.03.199