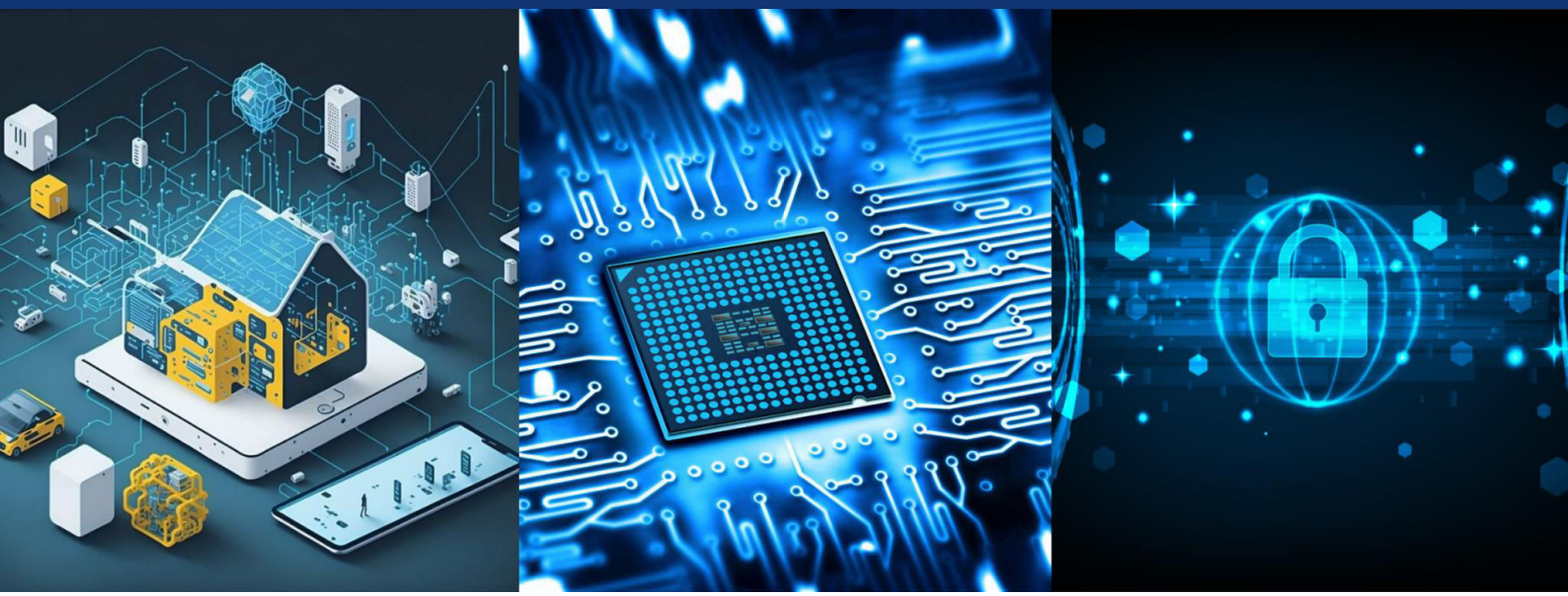
IJIRCCE

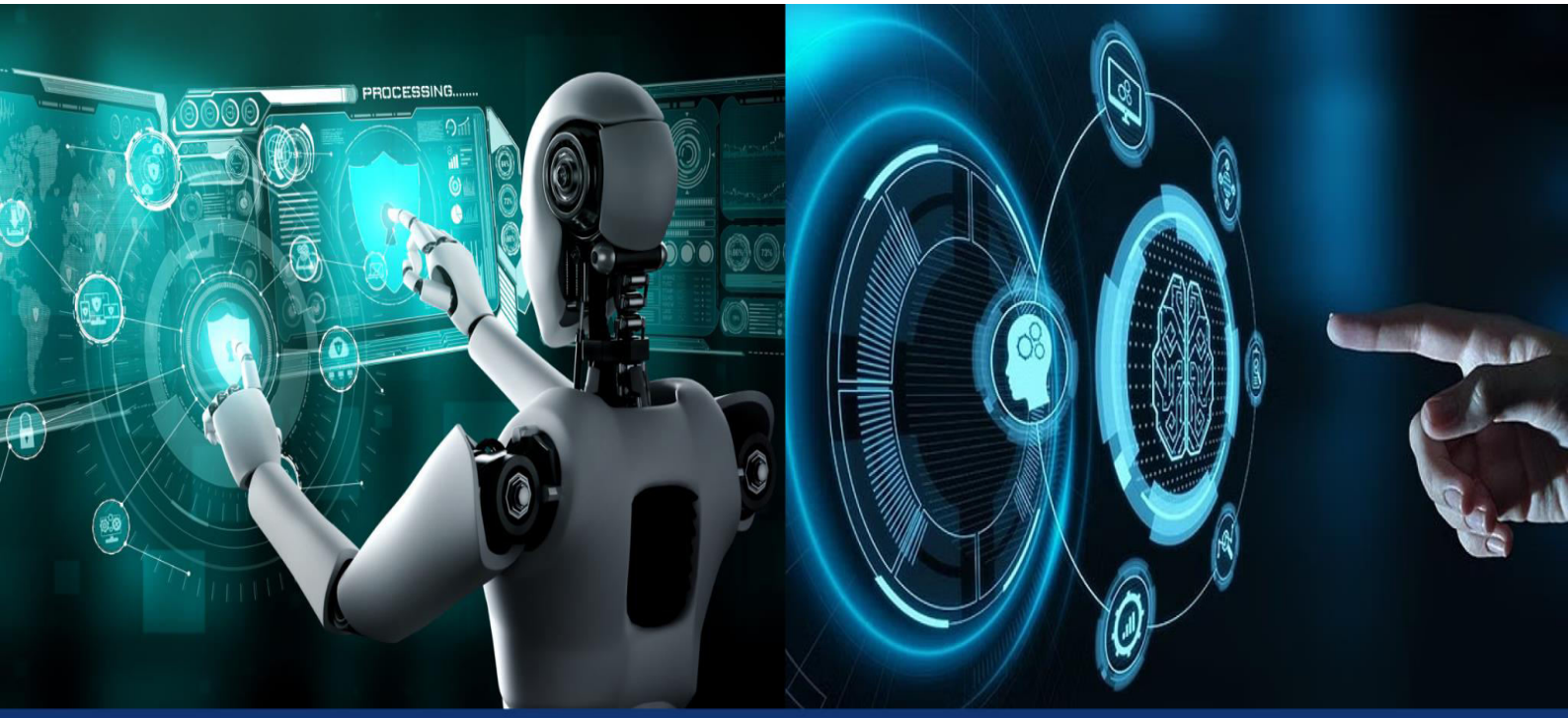
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 7, July 2026

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407039

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A Comparative Survey of Intrusion Detection Systems in IOT Environment with Machine Learning Frameworks

Snehal P.Chincholkar, Dr.Ajay P.Thakare

Research Scholar, PRMCEAM Bandera, Sant Gadge Baba Amravati University, Amravati, India

Principal, Prof. Ram Meghe College of Engineering and Management Bandera, Amravati, India

ABSTRACT: In the era we live in, the Internet is used by everyone. People, devices and smart things are connected to it. The Internet has made the world a smaller place. It is easier to converse with persons living at far distance and to share data in a moment. However, over the period of its usage, we have also learnt that the Internet is not a safe place for our information. People with bad intentions try to steal or misuse our information every day. We therefore need a system that can stop these people from doing such things. People use ways to make Intrusion Detection Systems. These systems use Machine Learning and Deep Learning to find people on the Internet. This paper will look at the Machine Learning and Deep Learning ways that are used to find identify such activities in cloud environments and IoT-based systems. We will look at how these ways work and how they can help keep our information safe. We shall also compare the Machine Learning and Deep Learning ways to see which ones are the best options. Further we will compare them based on how accurate they are. We will use things like accuracy and precision and sensitivity to compare them. We need to use them in a way that helps us and keeps our information safe.

KEYWORDS: Intrusion Detection Systems, Machine Learning and Deep Learning, Internet security

I. INTRODUCTION

The exponential advancements in recent technologies have become an important part of our lives. Though the internet of things (IoT) has gained significant attention to develop smart infrastructure, it also provides a large attack surface for intruders or hackers. Therefore, it requires identifying the attacks as soon as possible to provide a secure cyber infrastructure . Although there are various tools designed to protect against various cyberattacks such as firewalls, user authentication and data encryption, they seem to be limited in the level of protection they can provide. Intrusion Detection Systems (IDS) monitors network activities to identify patterns that breach security protocol and it remains one of the most widely used today.

The two broad categories of intrusion detection systems are heuristic-based and signature-based. Signature-based systems, also known as "pattern-matching" systems, identify threats by comparing the attack's signature to a recognized pattern. Heuristic-based systems, also known as anomaly-based systems, use departures from a model of typical behavior to identify attacks. HIDS uses the resources of its host to monitor traffic on the machine and identify potential threats. Host intrusion detection systems (HIDSs) are IDSs that run on a single workstation, whereas network intrusion detection systems (NIDSs) are standalone devices. These two types of NIDS provide a varying degree of security based on several objectives that will be analyzed in forthcoming sections.

The Internet of Things (IoT) is a new paradigm that enables sensors and electronic devices to communicate (sensing, aggregating, and connecting) via the Internet. IoT has its main application in smart homes industries, cities, transportation, health, and satellites. Rapid advancements in sensor and other network technology have led to the widespread use of these devices across a variety of application domains. However, this has made the network extremely diverse in terms of data models and communication protocols, making it challenging to share gateways at the network's edge and scale up and integrate new devices with the current ones

Recently, there has been intensive work in academia to explore the possibilities of applying ML methods to mitigate the shortcomings of traditional NIDS approaches have produced remarkable outcomes in other sub computing fields like

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

natural language processing (NLP) and computer vision. As a result of these achievement, since the detection task is essentially a classification problem, ML may be utilized to overcome the shortcomings of conventional NIDS. In threading this path, it is earlier understood that current machine learning algorithms cannot directly use network traffic as input, given that a fixed set of features derived from the traffic is needed. But in order to encode network traffic into fixed size feature vectors that accurately depict typical or anomalous behavior, it is necessary to examine what data (e.g., G. users, endpoints, programs, or protocols) ought to be taken into account.

RELATED WORK DONE: AI-BIDS: Enhancing Cyber Defense using Machine and Deep Learning Algorithms to Detect Attacks by Richard James REVA Academy for Corporate Excellence,suggested that Traditional IDS methods, like signature-based and anomaly-based detection, often struggle to detect new or evolving threats, whereas advanced IDS can be expensive and require a steep learning curve. And, due to the dynamic nature of cyber threats, traditional IDS struggles to accurately distinguish malicious network activities, like PortScan and Distributed Denial of Service (DDoS) attacks, from benigntraffic. It also faces limitations with scalability, poor performance on encrypted traffic, and challenges adapting tonew attack techniques, resulting in a high rate of false positivesand negatives. The paper demonstrates that integrating **Machine Learning (ML)** and **Deep Learning (DL)** techniques into a Network Intrusion Detection System (NIDS) can significantly improve the accuracy and efficiency of detecting cyber threats in modern networks. The proposed AI-based Intrusion Detection System (AI-BIDS) follows a systematic pipeline involving data preprocessing, feature engineering, model training, evaluation, and deployment using the CICIDS2017 dataset. By selecting the top 30 most relevant features through correlation analysis and applying MinMax scaling, the system effectively distinguishes between normal traffic and malicious activities such as DDoS and PortScan attacks. The comparative analysis of Support Vector Machine (SVM), Random Forest (RF), and Artificial Neural Network (ANN) reveals that ANN achieves the highest classification accuracy of **99.01%**, with excellent precision, recall, and F1-score across all attack categories. These results indicate that deep learning models are capable of capturing complex, non-linear relationships within network traffic, making them more suitable than conventional machine learning algorithms for developing reliable and intelligent intrusion detection systems. Furthermore, the deployment of the trained model using Flask and Socket programming demonstrates its practical applicability by enabling real-time threat detection, automatic IP blocking, attack probability prediction, and email alerts to network administrators, thereby supporting proactive cybersecurity management.

The study infers that although deep learning models achieve superior intrusion detection performance, their high computational complexity, longer training time, and greater hardware requirements limit their practical deployment. In comparison, Random Forest provides a better balance between accuracy and computational efficiency, making it more suitable for real-world applications. The research also emphasizes that effective intrusion detection depends on quality data preprocessing, feature selection, and rigorous model evaluation. Overall, the paper concludes that AI-driven intrusion detection systems have strong potential for enhancing network security, but future research should focus on improving computational efficiency, scalability, and adaptability to evolving cyber threats. [2]

A Comparative Study of AI Algorithms for Anomaly-based Intrusion Detection

The paper infers that **Intrusion Detection Systems (IDS)** remain one of the most effective mechanisms for protecting modern computer networks against increasingly sophisticated cyber threats. It highlights that different IDS approaches have distinct strengths and limitations. **Anomaly-based Intrusion Detection Systems (AIDS)** are capable of identifying both known and previously unseen attacks by continuously monitoring deviations from normal network behaviour, making them highly suitable for dynamic and evolving cyber environments. The study further emphasizes that supervised machine learning techniques can achieve high detection accuracy when sufficient labelled training data are available, while unsupervised learning methods offer an attractive alternative for analysing unlabelled network traffic without requiring costly manual data annotation. The comparison of various machine learning approaches—including Support Vector Machines (SVM), Decision Trees, Bayesian Networks, Neural Networks, Fuzzy Inference Systems, and Linear Genetic Programming—indicates that artificial intelligence has become a key enabler for improving intrusion detection accuracy, minimizing false alarms, and adapting to emerging attack patterns. Overall, the paper concludes that combining machine learning with anomaly detection provides a more intelligent and adaptive security solution than traditional rule-based detection methods.

The paper also concludes that **Signature-based Intrusion Detection Systems (SIDS)** continue to play a vital role in detecting known attacks because they can accurately match network traffic with predefined attack signatures while producing relatively few false positives. However, their inability to detect zero-day or previously unknown attacks

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

makes them insufficient as a standalone security solution. Based on this observation, the authors infer that future intrusion detection systems should integrate multiple detection techniques, including anomaly detection, signature detection, host-based IDS, network-based IDS, and advanced artificial intelligence algorithms, to achieve comprehensive network protection. The study further recommends improving the interoperability of different security mechanisms, enhancing AI-based intrusion detection algorithms, and developing integrated cybersecurity frameworks capable of responding to rapidly evolving threats. It also emphasizes that effective deployment of IDS depends not only on advanced algorithms but also on reliable user authentication, skilled IT personnel capable of analysing alerts and making informed decisions, and continuous system monitoring. Therefore, the paper suggests that the future of network security lies in intelligent, hybrid, and AI-driven intrusion detection systems that provide higher detection accuracy, lower false alarm rates, better scalability, and stronger resilience against both existing and emerging cyberattacks. [3]

AI-empowered Network Intrusion Detection System: The paper demonstrates that **Artificial Intelligence (AI)** and **Machine Learning (ML)** significantly improve the performance of **Network Intrusion Detection Systems (NIDS)** by achieving high detection accuracy with a low False Alarm Rate (FAR). The study highlights the importance of preprocessing techniques such as **SMOTE**, **Principal Component Analysis (PCA)**, and **XGBoost-based feature selection** in enhancing classification performance. Among the evaluated models, **K-Nearest Neighbor (KNN)** achieved the lowest FAR (0.0053) in binary classification, while **Random Forest (RF)** provided the best multiclass performance with **91.90% accuracy** and an **F1-score of 0.9292**, demonstrating its effectiveness in detecting complex cyberattacks. These results indicate that appropriate classifier selection combined with efficient preprocessing is essential for developing accurate and reliable intrusion detection systems.

The study further infers that traditional machine learning models, supported by robust feature engineering and preprocessing, can achieve excellent performance while remaining suitable for real-time deployment. The proposed models achieved **over 99.9% accuracy** in binary classification and outperformed several existing approaches on the **CSE-CIC-IDS2018** dataset. However, multiclass intrusion detection remains more challenging due to the similarity between attack categories. The paper concludes that future work should focus on improving multiclass detection, validating models on diverse real-world datasets, and integrating advanced AI techniques to develop scalable, adaptive, and efficient intrusion detection systems for modern cybersecurity applications.[4]

Mapping Cyber Threats in IoT-Driven MSPs: An Explainable Machine Learning Approach for Remote Work Security : The paper demonstrates that **machine learning techniques can significantly improve cybersecurity threat detection and classification for Managed Service Providers (MSPs)** operating in IoT-enabled remote work environments. By leveraging a carefully selected set of network traffic features, the proposed machine learning models achieved high classification accuracy while maintaining low false-positive rates, proving that effective intrusion detection does not necessarily require a large number of input features. A key contribution of the study is the integration of the **Cyber Kill Chain framework**, which enables the classification of detected threats according to different stages of an attack lifecycle. This structured approach allows security analysts to understand how far an attack has progressed and implement timely, stage-specific countermeasures. The validation of the proposed models using real-world datasets further confirms their practical applicability in protecting sensitive organizational data, maintaining the integrity of critical infrastructure, and supporting proactive cybersecurity management in increasingly complex IoT ecosystems.

The study also identifies several important challenges and future research opportunities. Although the developed models demonstrated strong predictive performance, their effectiveness may be limited by the use of static public datasets that cannot fully represent the continuously evolving nature of cyber threats or the diversity of real-world IoT devices and industrial environments. Additionally, advanced machine learning algorithms may require substantial computational resources, making deployment difficult for smaller organizations with limited infrastructure. The authors therefore recommend expanding training datasets with emerging attack scenarios, exploring unsupervised and semi-supervised learning techniques for detecting unknown threats, improving feature engineering methods, and integrating the models into broader cybersecurity frameworks. Furthermore, they highlight the growing potential of **Generative AI** and **Large Language Models (LLMs)** for simulating cyberattack scenarios, enhancing threat intelligence, automating phishing detection, and improving real-time threat analysis. Overall, the paper concludes that combining machine learning with established cybersecurity frameworks provides a scalable, intelligent, and proactive approach for strengthening IoT security, while emphasizing that continuous research and technological advancements are essential for building more robust, adaptive, and future-ready cybersecurity systems. [6]

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Multilabel Classification in IoT NIDS: A Proposed Cross Machine Learning Pipeline

The paper presents a **Cross-Machine Learning (Cross-ML) framework** for enhancing the performance and reliability of **Internet of Things (IoT)-based Network Intrusion Detection Systems (NIDS)**. Unlike conventional machine learning approaches that train and test models on the same dataset, the proposed framework evaluates a model's ability to generalize by training it on one dataset and testing it on another. This approach better represents real-world cybersecurity environments, where intrusion detection systems encounter previously unseen network traffic and attack patterns. The study emphasizes that successful Cross-ML implementation requires identifying common features across datasets, applying consistent preprocessing techniques such as normalization and encoding, and carefully mapping attack categories with similar characteristics. The authors used a Decision Tree classifier and evaluated its performance using accuracy, precision, recall, and F1-score on three benchmark datasets—UNSW-NB15, ToN-IoT, and X-IIoTID. Among these, the X-IIoTID dataset demonstrated the best overall performance, achieving over 90% across all evaluation metrics, indicating its suitability for multi-label intrusion detection.

The study also highlights several practical challenges associated with Cross-ML. Since the benchmark datasets were generated using different testbeds and employ different feature names and attack labels, the authors had to assume mappings between similar features and attack classes, which introduced classification errors. Analysis of the confusion matrices revealed that while normal network traffic was consistently identified, certain attack categories, such as RDOS and Lateral Movement, were frequently misclassified due to inconsistencies in dataset nomenclature. These findings demonstrate that dataset heterogeneity remains a major obstacle to developing generalized intrusion detection systems. The authors conclude that although the proposed Cross-ML framework shows significant promise for improving the robustness and real-world applicability of IoT-based NIDS, further research is required on standardized datasets, improved feature engineering, advanced machine learning algorithms, and binary classification approaches to achieve more reliable and scalable cybersecurity solutions. [7]

II. CONCLUSION AND FUTURE WORK

Future work could assess the effectiveness of generative AI in simulating cyberattack scenarios or enhancing threat intelligence. Additionally, LLMs could be used to automate and enhance the detection of phishing and other social engineering attacks by analyzing communication patterns. Evaluating the performance of these technologies in real-time threat detection scenarios will provide valuable insights into their practical benefits and limitations in cyber security.

Overall, future research is needed for the practical application of the Cross-ML pipeline, and non-experts should exercise caution in this approach to solving IoT-based NIDS. Further research may consider a binary classification approach as it reduces the complexity of the model in identifying all instances of the classes.

REFERENCES

1. Berrezzek, Amira & Hayet, Djellali & Mahnane, Lamia. (2025). A Survey of Intrusion Detection Systems in Deep Learning Era: Methods and Perspectives. 1-5. 10.1109/ICAECCS68240.2025.11384749..
2. R. James, P. Mishra and S. Abhi, "AI-BIDS: Enhancing Cyber Defense Using Machine and Deep Learning Algorithms to Detect Attacks," 2025 International Conference on Emerging Technologies in Computing and Communication (ETCC), Bangalore, India, 2025, pp. 1-6, doi: 10.1109/ETCC65847.2025.11108655.
3. V. P. Gandi, N. S. L. Jatla, G. Sadhineni, S. Geddamuri, G. K. Chaitanya and A. K. Velmurugan, "A Comparative Study of AI Algorithms for Anomaly-based Intrusion Detection," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 530-534, doi: 10.1109/ICCMC56507.2023.10084186.
4. Alsadawi, Saja & Foo, Yee-Loo. (2025). AI-empowered Network Intrusion Detection System. 1-7. 10.1109/MECON67253.2025.11277036.
5. S. P. Pratap, C. Devadiga, S. Channalli, V. P. Malagi, P. Angolkar and P. K. C, "Deep Generative Modeling for Unsupervised IoT Intrusion Detection: A VAE–GAN Approach with HDBSCAN Profiling," 2025 IEEE 9th International Conference on Information and Communication Technology (CICT), Chennai, India, 2025, pp. 1-6, doi: 10.1109/CICT67193.2025.11399186.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

6. J. Johnstone and A. Akinfaderin, "Mapping Cyber Threats in IoT-Driven MSPs: An Explainable Machine Learning Approach for Remote Work Security," 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC), Houston, TX, USA, 2025, pp. 1-9, doi: 10.1109/ICAIC63015.2025.10848740.
7. E. S. Shombot, G. Dusserre, R. Bestak and N. B. Ahmed, "Multilabel Classification in IoT NIDS: A Proposed Cross Machine Learning Pipeline," 2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON), Ado Ekiti, Nigeria, 2024, pp. 1-9, doi: 10.1109/NIGERCON62786.2024.10927096
8. A. Talukder, M. Baker, A. Rahman and M. A. Khan, "Evaluating the Efficacy of Explainable Machine Learning Algorithms for the Detection and Classification of Network Intrusions," 2025 IEEE 2nd International Conference on Computing, Applications and Systems (COMPAS), Kushtia, Bangladesh, 2025, pp. 1-6, doi: 10.1109/COMPAS67506.2025.11381867
9. Koravanavar, Madhu R, Sanika S Mithare and Rajendra S. Hegadi. "Interpretable Network Intrusion Detection Framework using Hybrid DL and ML Models." *2025 IEEE Future Networks World Forum (FNWF)* (2025): 1-6.
10. A. Grini, O. Taheri, B. El Khamlichi and A. El Fallah-Seghrouchni, "Constrained Network Adversarial Attacks: Validity, Robustness, and Transferability," 2025 21st International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), Lucca, Italy, 2025, pp. 771-776, doi: 10.1109/DCOSS-IoT65416.2025.00117.
11. Sood, Saksham & Kumar, P. & Singh, Uphar & Vyas, Raniana & Vyas, O. & Khondoker, Rahamatullah. (2022). LBDMIDS: LSTM Based Deep Learning Model for Intrusion Detection Systems for IoT Networks. 753-759. 10.1109/AIIoT54504.2022.9817245.
12. S. P. Pratap, C. Devadiga, S. Channalli, V. P. Malagi, P. Angolkar and P. K. C, "Deep Generative Modeling for Unsupervised IoT Intrusion Detection: A VAE–GAN Approach with HDBSCAN Profiling," 2025 IEEE 9th International Conference on Information and Communication Technology (CICT), Chennai, India, 2025, pp. 1-6, doi: 10.1109/CICT67193.2025.11399186.
13. Hnamte, Vanlalruata & Nguyen, Hong - Nhung & Hussain, Jamal & Hwa-Kim, Yong. (2023). A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE. IEEE Access. 10.1109/ACCESS.2023.3266979. Shilpa jain and Sourabh jain ,'Energy Efficient Maximum Lifetime Ad-Hoc Routing (EEMLAR)', international Journal of Computer Networks and Wireless Communications, Vol.2, Issue 4, pp. 450-455, 2012.
14. J. Vanitha and P. Anandababu, "Optimizing Cybersecurity Against Zero-Day Attacks Using Dandelion Optimization and Machine Learning Techniques," 2025 Second International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS), Coimbatore, India, 2025, pp. 189-196, doi: 10.1109/ICC-ROBINS64345.2025.11086151.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details