IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Hybrid Machine Learning and Deep Learning Approach for Enhanced Intrusion Detection

[1]Eak Nath Dubey, [2]Rakesh Kumar Lodhi, [3]Rakesh Kumar Tiwari

[1]Student 2Assistant Professor, 3Assistant Professor

Department of Computer Science & Engineering

Technocrats Institute of Technology & Science (RGPV University Bhopal (M.P)) India

Abstract :-- In the rapidly evolving digital environment of the present times, traditional intrusion detection systems (IDS) are increasingly struggling to detect highly advanced cyber-attacks. Traditional rule-based methods rarely detect unknown or zero-day attacks and are non-scalable or suffer from a high rate of false positives. To overcome these limitations, recent advances in artificial intelligence have introduced promising techniques i.e., machine learning (ML) and deep learning (DL) which enhance the precision and responsiveness of IDS. This work proposes a hybrid IDS model that combines the interpretability and efficiency of ML with the deep feature learning as well as pattern recognition capabilities of DL. The proposed hybrid model employs both signature-based as well as anomaly-based detection methods in an effort to maximize the detection rate of threats while minimizing false alarms. The proposed model is evaluated with standard benchmark datasets such as NSL-KDD as well as CICIDS2017 in an effort to demonstrate its functionality in real-world applications. Results demonstrate significant detection accuracy, scalability, and responsiveness enhancements compared to traditional and stand-alone AI-based approaches. The research provides a valuable and intelligent solution to modern cyber security issues and opens the door to future developments in explainable, adaptive, and real-time IDS systems.

Keywords:- Intrusion Detection System (IDS), Machine Learning (ML), Deep Learning (DL), Hybrid Model, cyber security, Anomaly Detection, Zero-Day Attacks, Auto encoder, AE+CNN Hybrid.

I. INTRODUCTION

With a growingly connected digital environment, securing network systems has never been as important as it is today. With the exponentially increasing number of advanced cyber-attacks, legacy intrusion detection systems (IDS) can no longer effectively detect new and evolving threats. To overcome these shortcomings, emerging technologies in artificial intelligence have provided new opportunities to advance the capabilities of IDS. In particular, the use of machine learning (ML) and deep learning (DL) methodologies has been highly promising in enhancing the accuracy, adaptability, and effectiveness of intrusion detection systems [1].The present study introduces a hybrid strategy that blends the benefits of both the machine learning and deep learning models to design a stronger and wiser intrusion detection system. Although ML algorithms have been well known for their efficiency and interpretability in the classification of structured data, the DL models have been superior in learning high-level feature representations and intricate patterns of data. Using the complementary strengths of the two paradigms, the suggested hybrid model is intended to greatly enhance the detection rate of malicious behavior and lower the rate of false positives. The intrusion detection system works in two mechanisms: signature-based detection and anomaly-based detection. Signature-based detection uses a known list of rules or indicators from the system attack database to specify whether the activity is malicious or not, while anomaly-based detection identifies the attack based on unusual user behavior patterns. If there are users who perform unusual actions or activities, it can be detected as an attack [2].

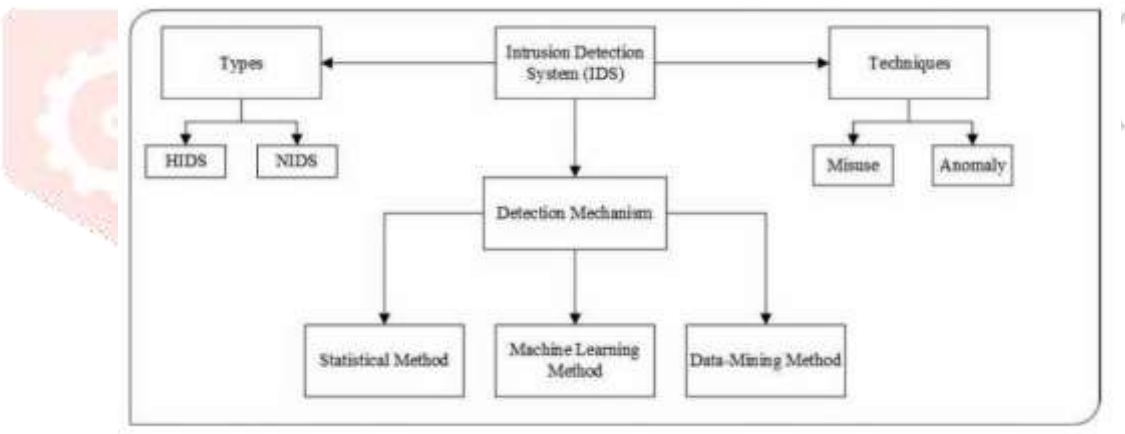

Fig.1 Intrusion detection system (IDS) [2]

1.1 Evolution of Network Security Threats

The development of network security threats has kept pace with technology advances, evolving from early internet-era simple viruses and worms to the advanced, multi-vector threats of the present. Threats initially were mostly experimental or situational, causing little impact, but became more organized and financially driven as the internet grew. E-commerce and cloud computing ushered in new targets, resulting in APTs, ransomware phishing, and zero-day exploits. Latest threats now employ AI, social engineering, and nation-state resources, and rather than targeting systems, they go after user behavior and supply chains, making cyber security an essential, ever-changing discipline [3].

1.2 The Role of Intrusion Detection Systems (IDS)

The term intrusion refers to interrupting someone without permission. In the context of computing, intrusion refers to an attempt of accessing computer system resources without any permission with an intention of causing incidental damage. Basically, Intrusion Detection refers to any kind of mechanism to detect such intrusive behavior and Intrusion Detection System (IDS) refers to a system that performs the process of intrusion detection automatically. The IDS is responsible for monitoring the data traffic in the network and any suspicious activities against the network security. The system or network administrator of the network are alerted or reported if any threats or malicious activities are detected in the network. Hence, the main purpose of the IDS is to detect and report the intrusion attempts to the concerned parties. The IDS employ different types of tools and techniques to detect suspicious activities both at the host and the network level [4].

1.3 Intelligent Detection Mechanisms

Integrating real-time threat intelligence and adaptive defense mechanisms significantly reduces the time needed to detect and respond to threats. Old-fashioned security methods typically depend on fixed regulations and detection systems based on specific characteristics, causing delays in responding to emerging risks. On the other hand, immediate intelligence and flexible mechanisms can quickly detect and reduce risks. Having the ability to respond quickly is crucial in reducing the harm from cyber-attacks and maintaining the ongoing function of business operations [5].

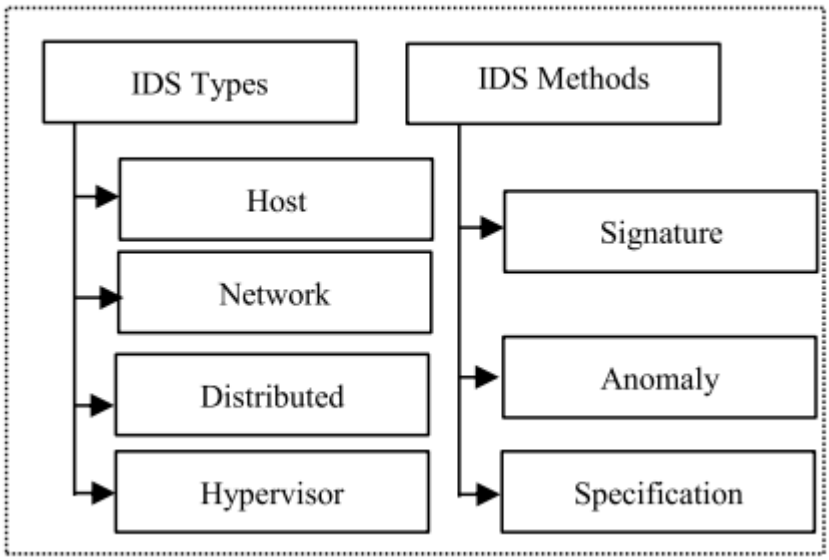

Fig.2 Intrusion detection types and methods.[6]

2. Detect Unknown Attacks and Challenges with Traditional IDS

Studies have been ongoing on new systems for an automatic detection of abnormal system usages. Moreover, Denning reported the development of an intrusion detecting model, which he suggested as a framework for a general-purpose IDS. Since then, experts have developed and applied several algorithms for automating the process of network ID. They have also continually pursued more accurate, faster, and scalable methods for this purpose. With the arrival of the "IOT" and Big data era, it is expected that the number of connected devices would exceed 26 billion by the year 2020. With this trend, the type and number of cyber security issues are also expected to increase [7]. The lack of ability to find unknown attacks, commonly known as zero-day threats, is a great challenge in cyber security because known signatures and pre-defined rules are used in conventional security systems. These techniques do not work against new or emerging attack methods that have not yet been discovered or documented. With cybercriminals constantly developing new techniques, taking advantage of new vulnerabilities and employing invisible and smart tactics, traditional tools do not detect and react on time. This gap exposes systems to breaches, data theft, and disruption, highlighting the necessity of behavior-based and AI-powered detection capabilities that can find anomalies and zero-day threats [8].

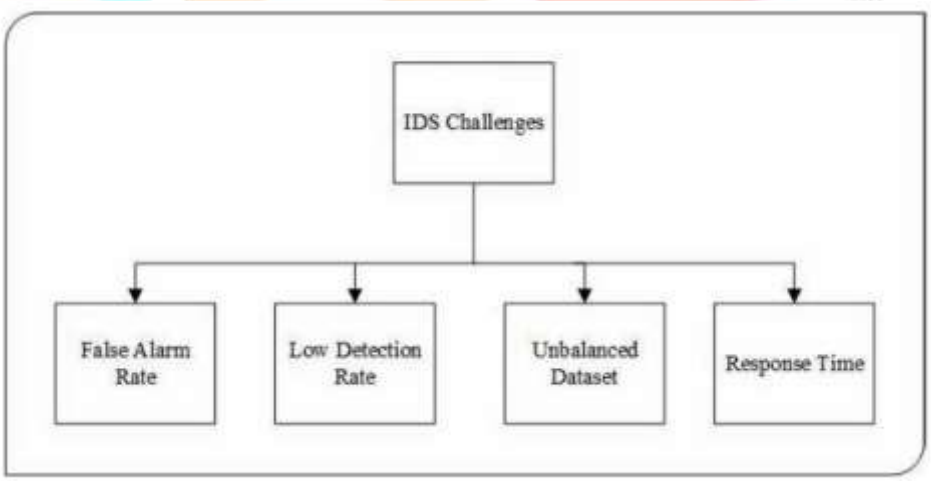

Fig. 2 Intrusion detection system (IDS) challenges [7]

False positive rates that are too high and deficiencies in scalability and flexibility are significant disadvantages of older security systems. When security technologies produce too many false alarms by marking benign traffic as malicious, they bog down analysts and produce alert fatigue, where genuine threats are missed. In addition, most legacy solutions have difficulty scaling with increasing network sizes and data loads, and are not capable of responding to changing threat environments and heterogeneous IT environments. This compromises their capability to operate effectively in fast-paced, contemporary infrastructures, making it necessary for more intelligent, scalable, and responsive security solutions [9].

3. Advances in Artificial Intelligence for IDS

Adventures in Artificial Intelligence (AI) have greatly improved Intrusion Detection Systems (IDS) to provide more precise, effective, and dynamic detection of threats. A fundamental aspect of this evolution is the contribution of Machine Learning (ML) to enable IDS to transcend static, rule-based systems by learning from past and live data patterns [10]. ML algorithms are able to identify known as well as unknown attacks by picking up on anomalies and suspicious activity through network traffic, user activity, and system logs. As opposed to traditional systems that need to be updated constantly by hand, ML-based IDS can keep learning and improving by retraining over new data, rendering them more resistant to changing threats. This transition to smart, data-powered detection not only improves precision but also decreases false positives, making security operations more efficient and scalable in today's modern digital landscapes [11].

3.1 Strengths of Deep Learning Models

Deep learning models have a number of distinct strengths in Intrusion Detection Systems (IDS) that make them extremely powerful for contemporary cyber security problems. These models, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and auto encoders, are particularly good at automatically learning high-level and hierarchical features from big amounts of raw data without the necessity for manual feature engineering [12]. This enables them to detect subtle and nonlinear behavior linked with advanced or stealthy attacks. Deep learning algorithms are especially good at recognizing zero-day attacks and anomalies because they can learn from data and reveal hidden patterns. They also scale with increasing data and can learn to adapt to changing threat scenarios when they are trained continuously. In addition, deep learning also allows for real-time threat detection with high precision and reduced false positives compared to conventional and shallow learning processes, and therefore they are a useful tool for protecting increasingly complicated network environments [13].

3.2 Comparative Advantages Over Rule-Based Systems

Rule-based IDS, though efficient in detecting known attack signatures with high interpretability, are poor at discovering new or emerging threats because they are static and based on pre-defined rules. Machine learning-based methods, on the other hand, can adapt patterns from past data, making them recognize previously unknown attacks with moderate adaptability [14]. Deep learning (DL) models extend by extracting intricate features from raw data automatically, providing greater precision and generalization to new threats, albeit necessarily at the expense of interpretability. Hybrid ML-DL architectures leverage the strengths of each approach efficiency and simplicity of ML vs. depth and accuracy of DL blending into much improved detection, reduced false positives, and greater scalability than conventional rule-based IDS [15].

Table 1: Comparative Features of Intrusion Detection System Approaches

Feature/Aspect	Rule-Based IDS	Machine Learning IDS	Deep Learning IDS	Hybrid ML-DL IDS
Ability to Detect New Attacks	Low	Moderate	High	Very High
False Positive Rate	High	Moderate	Low	Very Low
Interpretability	High	High	Low	Moderate
Training Time	Low	Moderate	High	Moderate
Scalability	Low	Moderate	High	High

This table compares different intrusion detection approaches across key performance aspects. Rule-based IDS are interpretable and fast but struggle with scalability and unknown attacks. In contrast, hybrid ML-DL models offer superior detection capabilities and low false positives, balancing performance, scalability, and adaptability [15].

4. Hybrid ML-DL Approach and Motivation for a Hybrid Architecture

A combination of Machine Learning–Deep Learning (ML-DL) paradigms in Intrusion Detection Systems (IDS) leverages the advantages of both paradigms to design a more resilient, precise, and adaptable security solution. Classical machine learning methods like decision trees, support vector machines, or k-nearest neighbors are usually efficient in classification problems and provide interpretability, which is beneficial for identifying known attack patterns and offering insights regarding decision-making. But they may have difficulties handling large-scale, high-dimensional data or when confronting changing and intricate threats [16]. Deep learning models are better at automatically discovering hierarchical features from raw data and detecting intricate, non-linear relationships, which improves their capability to recognize advanced and unforeseen attacks. Yet, deep learning models may be computationally expensive and less transparent. The need for a hybrid architecture stems from the wish to combine the interpretability and efficiency of machine learning and the representation capacity and flexibility of deep learning [17]. Through combining ML methods for early feature selection or anomaly detection with DL models for more thorough analysis and classification, hybrid frameworks are able to enhance detection accuracy, minimize false positives, and maximize scalability and adaptability. Such synergy is formed to provide a more robust intrusion detection system that can address the dynamic and complex nature of contemporary cyber threats, thus presenting an appealing alternative for next-generation security systems [18].

4.1 Synergy Between ML and DL Techniques

The complementarity of Machine Learning (ML) and Deep Learning (DL) methods in Intrusion Detection Systems (IDS) is in their respective strengths that, when combined, improve detection accuracy, efficiency, and responsiveness. ML methods are useful for their speed, interpretability, and capacity for structured data, thus suitable for preliminary data preprocessing, feature selection, and light anomaly detection. Conversely [19], DL models are particularly good at learning complicated patterns automatically from unstructured and high-dimensional information to identify subtle and novel threats. With their combination in hybrid architecture, ML can simplify the input complexity and emphasize the important features, while DL can undertake deeper analysis of complex nature. This cooperation results in improved threat detection, fewer false positives, and improved scalability, forming a strong and smart defense system that can react to the changing scenario [20].

4.2 Expected Improvements in Performance Metrics

The hybrid ML-DL system is expected to bring much improvement in all the performance metrics of intrusion detection systems. By tapping into the pattern recognition and generalization capacity of machine learning as well as the deep feature extraction capability of deep learning, the hybrid system enhances the identification of known and unknown attacks. It reduces false positives by improved boundary decision and applies automated feature learning to track evolving threats. This cross-bred results in higher detection accuracy, faster response times, and better scalability, and the system becomes more robust for real-world deployment [21].

5. Contribution and Scope

This work's contribution is in suggesting a machine learning and deep learning hybrid model that improves intrusion detection systems' performance by meeting the shortcomings of each technique. The model combines the best features of both methods to attain higher accuracy, fewer false positives, and improved adaptability to emerging threats. The research scope includes designing, developing, and testing the hybrid model on benchmark datasets with emphasis on its real-time and scalable network applications. The research aims to provide a foundation for the evolution of intelligent and autonomous cyber security systems in the future [22].

5.1 Application on Benchmark Datasets or Broader Impact on Network Security Roadmap for Future Enhancements

The implementation of the envisioned hybrid ML-DL intrusion detection model on standard datasets like NSL-KDD, CICIDS2017, or UNSW-NB15 is a decisive step toward testing its efficacy and universality. The datasets provide an extensive range of attack situations and normal traffic flows so that thorough performance analysis in relation to accuracy, precision, recall, and false positive rate can be performed. By demonstrating improved performance on these tests, the model positions itself as stable and implementable in real network

scenarios. Along with testing in experiments, overall impact of this study is that it can significantly improve network security architectures across different industries [23]. With increasingly sophisticated cyber-attacks, traditional rule-based and single ML/DL models fall behind in real-time response and accurate threat detection. Hybrid approach has an adaptive and scalable solution with the capacity to learn dynamically about new threats, thus proactive defense. For the future, the future extension plan includes integrating the model into real-time surveillance systems, applying online learning for continued adaptation, and promoting interpretability using explainable AI (XAI) methods. In addition, emphasis can be given to reducing computational overhead in order to facilitate effective deployment in hardware-constrained environments such as IOT networks or edge computing systems. Finally, this research paves the way for the next generation of intelligent intrusion detection systems that are not only accurate but also transparent, adaptable, and resilient to new cyber threats [24].

IV. RESULTS AND DISCUSSION

The experimental results of the suggested IDS are shown in this section, which contrasts the effectiveness of the Auto encoder (AE) and Deep Neural Network (DNN) models in both Federated Learning (FL) and non-FL scenarios. The findings indicate that, with only slight variations in accuracy, FL-trained models particularly the AE performed more effectively in anomaly detection and privacy preservation. Additionally, the FL approach showed reduced False Positive Rate (FPR) and enhanced generalization, providing notable benefits for deployment in IOT devices with limited resources

Table 2. Optimal Parameters Used to Build the DNN DL mode

IoT device	Initial learning	Batch size	Max training epoch	Optimizer algorithm
Device 1	0.004	64	35	Adam
Device 2	0.0001	256	40	RMSProp
Device 3	0.0002	128	25	SGD
Device 4	0.001	128	35	Adam
Device 5	0.01	64	35	SGD
Device 6	0.0001	256	40	RMSProp
Device 7	0.0025	128	30	Adam
Device 8	0.001	64	45	SGD
Device 9	0.00001	256	20	Adam

Performance Results of AE+ CNN Model

The Auto encoder + Convolutional Neural Network (AE + CNN) model provides a strong intrusion detection solution by fusing the supervised classification capabilities of CNN with the unsupervised feature extraction of AE. In order to distinguish between malicious and benign network activity, the CNN classifies the compact representations of typical traffic that the AE has learned.

PERFORMANCE TABLE OF AE+CNN MODEL

Metric	AE + CNN Result
Accuracy	97.5%
Precision	93.2%
Recall	96.7%
F1-score	95.9%

With a 94.9% F1-score and 96.5% accuracy, the AE + CNN model showed excellent performance in identifying both malicious and benign traffic. Through the use of AE for feature compression, the model manages data imbalance, lowers False Positive Rates, and demonstrates that it is a workable, accurate solution for real-time intrusion detection in Internet of Things networks.

Benefits of Using AE+CNN over FL+DNN in IoT Intrusion Detection

Large data volumes and limited resources are two issues that IoT intrusion detection systems (IDS) must deal with. In terms of detection performance, feature learning, and computational efficiency, the AE+CNN model performs better than FL+DNN, especially in settings with little labeled data. As illustrated in Fig. 6, AE+CNN provides a more transparent and effective solution for IoT and is more appropriate for detecting zero-day attacks.

Conclusion

With the increasingly vast and interlinked digital domain of today, the rapid development and sophistication of cyber attacks require more adaptive, capable, and efficient intrusion detection systems. Traditional IDS methods, such as rule-based systems, while efficient at detecting known threats, are ineffective in detecting unknown or zero-day threats, and tend to be poorly scalable with high false positives. The integration of artificial intelligence in the guise of machine learning and deep learning into IDS design has opened up new avenues for addressing these limitations. This study introduced a hybrid ML-DL paradigm that combines the interpretability and parsimony of machine learning with the deep feature learning and generalization capabilities of deep learning models. Through this synergy, the hybrid paradigm significantly improves detection accuracy, reduces false positives, and enhances adaptability against emerging threats. Its performance on benchmarking datasets guarantees its robustness and real-world applicability. In addition, the given architecture sets a foundation for further research in autonomous, real-time, and scalable cyber security systems. With ongoing improvement in the shape of online learning, real-time integration, and deploy ability with explainable AI, the hybrid ML-DL IDS can evolve to become a next-generation security solution that can offer protection against the evolving nature and complexity of modern-day cyber-attacks.

References

[1]. Sajid, M., Malik, K. R., Almogren, A., Malik, T. S., Khan, A. H., Tanveer, J., & Rehman, A. U. (2024). Enhancing intrusion detection: a hybrid machine and deep learning approach. *Journal of Cloud Computing*, *13*(1), 123. https://doi.org/10.1186/s13677-024-00685-x

[2]. Megantara, A. A., & Ahmad, T. (2021). A hybrid machine learning method for increasing the performance of network intrusion detection systems. *Journal of Big Data*, *8*(1), 142. https://doi.org/10.1186/s40537-021-00531-w

[3]. Fadziso, T., Thaduri, U. R., Dekkati, S., Ballamudi, V. K. R., & Desamsetti, H. (2023). Evolution of the cyber security threat: an overview of the scale of cyber threat. *Digitalization & Sustainability Review*, *3*(1), 1-12.

[4]. Thapa, S., & Mailewa, A. (2020, April). The role of intrusion detection/prevention systems in modern computer networks: A review. In *Conference: Midwest Instruction and Computing Symposium (MICS)* (Vol. 53, pp. 1-14).

[5]. Aminu, M., Akinsanya, A., Dako, D. A., & Oyedokun, O. (2024). Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. *International Journal of Computer Applications Technology and Research*, *13*(8), 11-27. DOI:10.7753/IJCATR1308.1002

[6]. Khanan, A., Mohamed, Y. A., Mohamed, A. H. H., & Bashir, M. (2024). From bytes to insights: a systematic literature review on unraveling IDS datasets for enhanced cybersecurity understanding. *IEEE Access*, *12*, 59289-59317. Digital Object Identifier 10.1109/ACCESS.2024.3392338

[7]. Al-Janabi, M., Ismail, M. A., & Ali, A. H. (2021). Intrusion Detection Systems, Issues, Challenges, and Needs. *Int. J. Comput. Intell. Syst.*, *14*(1), 560-571. https://doi.org/10.2991/ijcis.d.210105.001;

[8]. Papalkar, R. R., & Alvi, A. S. (2023). Review of unknown attack detection with deep learning techniques. In *Artificial Intelligence, Blockchain, Computing and Security Volume 1* (pp. 989-997). CRC Press.

[9]. Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity*, *4*, 1-27. https://doi.org/10.1186/s42400-021-00077-7

[10]. Vanin, P., Newe, T., Dhirani, L. L., O'Connell, E., O'Shea, D., Lee, B., & Rao, M. (2022). A study of network intrusion detection systems using artificial intelligence/machine learning. *Applied Sciences*, *12*(22), 11752. https://doi.org/10.3390/app122211752

[11]. Baraneetharan, E. (2020). Role of machine learning algorithms intrusion detection in WSNs: a survey. *Journal of Information Technology*, *2*(03), 161-173.

[12]. Kocher, G., & Kumar, G. (2021). Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges. *Soft Computing*, *25*(15), 9731-9763. https://doi.org/10.1007/s00500-021-05893-0

[13]. Thakur, D., Saini, J. K., & Srinivasan, S. (2023). DeepThink IoT: the strength of deep learning in internet of things. *Artificial Intelligence Review*, *56*(12), 14663-14730. https://doi.org/10.1007/s10462-023-10513-4

[14]. Liu, Q., Hagenmeyer, V., & Keller, H. B. (2021). A review of rule learning-based intrusion detection systems and their prospects in smart grids. *Ieee Access*, *9*, 57542-57564. Digital Object Identifier 10.1109/ACCESS.2021.3071263

[15]. Rattanasawad, T., Saikaew, K. R., Buranarach, M., & Supnithi, T. (2013, September). A review and comparison of rule languages and rule-based inference engines for the Semantic Web. In *2013 international computer science and engineering conference (ICSEC)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICSEC.2013.6694743

[16]. Sharma, A., Rani, S., & Driss, M. (2024). Hybrid evolutionary machine learning model for advanced intrusion detection architecture for cyber threat identification. *PloS one*, *19*(9), e0308206. https://doi.org/10.1371/journal.pone.0308206

[17]. Ahmed, U., Jiangbin, Z., Almogren, A., Khan, S., Sadiq, M. T., Altameem, A., & Rehman, A. U. (2024). Explainable AI-based innovative hybrid ensemble model for intrusion detection. *Journal of Cloud Computing*, *13*(1), 150. https://doi.org/10.1186/s13677-024-00712-x

[18]. Mohammed, K. Enhancing Cybersecurity Through Artificial Intelligence: A Novel Approach to Intrusion Detection.

[19]. Wang, S., Huang, L., Ge, J., Zhang, T., Feng, H., Li, M., ... & Ng, V. (2020). Synergy between machine/deep learning and software engineering: How far are we?. *arXiv preprint arXiv:2008.05515*.

[20]. Peng, S., Cao, L., Zhou, Y., Ouyang, Z., Yang, A., Li, X., ... & Yu, S. (2022). A survey on deep learning for textual emotion analysis in social networks. *Digital Communications and Networks*, *8*(5), 745-762. https://doi.org/10.1016/j.dcan.2021.10.003

[21]. Azizan, A. H., Mostafa, S. A., Mustapha, A., Foozy, C. F. M., Wahab, M. H. A., Mohammed, M. A., & Khalaf, B. A. (2021). A machine learning approach for improving the performance of network intrusion detection systems. *Annals of Emerging Technologies in Computing (AETiC)*, *5*(5), 201-208. http://aetic.theiaer.org/archive/v5/v5n5/p25.html

[22]. Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: a comprehensive review and future directions. *Cluster Computing*, *26*(6), 3753-3780. https://doi.org/10.1007/s10586-022-03776-z

[23]. Hindy, H., Brosset, D., Bayne, E., Seeam, A. K., Tachtatzis, C., Atkinson, R., & Bellekens, X. (2020). A taxonomy of network threats and the effect of current datasets on intrusion detection systems. *IEEe Access*, *8*, 104650-104675. Digital Object Identifier 10.1109/ACCESS.2020.3000179

[24]. Ali, M., Naeem, F., Kaddoum, G., & Hossain, E. (2023). Metaverse communications, networking, security, and applications: Research issues, state-of-the-art, and future directions. *IEEE Communications Surveys & Tutorials*, *26*(2), 1238-1278. https://doi.org/10.1109/COMST.2023.3347172