Transforming Cyber Defense: AI, Intrusion Detection and the Future of Security

S. Akilandeswari[1], J. Amutha[1], S. Sundar[2], K. Rahapriya[3], T. Sakthivel[3] and R. Divyabharathi[3]
[1]*Department of AI&DS, E.G.S. Pillay Engineering College, Nagapattinam 611002, Tamil Nadu, India*
[2]*Tech Lead, Ministry of Transportation, U.A.E.*
[3]*E.G.S. Pillay Engineering College, Nagapattinam 611002, Tamil Nadu, India*

Keywords: Intrusion Detection Systems, Cybersecurity, Machine Learning, Deep Learning, Network Security.

Abstract: Thus, Modern Intrusion Detection Systems (IDS) forms an essential part of the critical infrastructures in order to detect and protect against unwanted malicious actions over networks and hosts. As the cyber threats are becoming more innovative, advanced deep learning (DL) and machine learning (ML) techniques are widely used to develop IDS with better performance. This survey focuses on the newest applications and trends in the field of IDS with respect to current ideas and techniques within the discipline of ML and DL methods being used along with the challenges they were developed to address and the limitations inherent in their solutions. In addition, it summarizes the recent techniques, reviews the performance, and indicates the gap for future research by developing the intelligent and adaptive Intrusion Detection System (IDS).

1 INTRODUCTION

Nishani, L. and Biba, M., 2016. With the rising numbers and growing sophistication of cyberattacks, Intrusion Detection Systems became evolved and improved over time but retained their same core identity that is still remarkably relevant. Presently, the deployment of ML and DL provides the basis for all modern IDS to ensure correct identification of the irregularities and ascertain the possibility of an attack. Siddiqui, et al., 2021. This section, both summarizing current trends and appearing informational on ML and DL potentiality for identifying advanced attacks or the trajectory towards constant evolution. However, this article provides a survey on the main research publications focusing on the application of contemporary deep learning-based techniques acting as intrusion detection system in the fog computing framework. Some issues regarding cybersecurity emerge because of this approach, but we can say that Fog Computing is a decentralized approach that provides real-time data processing. Goyal, N.,et al, 2021,There are various types of neural networks used to improve the behavior of IDS and some limitations about their behavior during the scaling, which are due to limitation of resources and its capabilities, such as CNN, RNN, hybrid structures, etcany.

1.1 Deep Learning Paradigms

Goodfellow, I., et al., 2016 Approaches based on deep learning have achieved impressive results isolating the intricate patterns present in network traffic, for example Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). Thakkar, A. and Lohiya, R., 2021, A few examples of models built upon RNNs are able to classify malicious network activity with an accuracy of over 90%.

1.2 Ensemble Learning Strategies

Abdan, M. and Seno, S.A.H., 2022, Ensemble frameworks which combine different learning models can improve detection accuracy and robustness. Xiao, H., et al, 2015 Ensemble methods such as random forests and boosting algorithms adapt better to different attack scenarios compared to single models.

1.3 Optimization Techniques for Feature Selection

Kanthimathi, S. and Prathuri, J.R., 2020, To improve this process further, optimization techniques like genetic algorithm and particle swarm optimization

Akilandeswari, S., Amutha, J., Sundar, S., Rahapriya, K., Sakthivel, T. and Divyabharathi, R.
Transforming Cyber Defense: AI, Intrusion Detection and the Future of Security.
DOI: 10.5220/0013890200004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 2*, pages 800-807
ISBN: 978-989-758-777-1

have been adopted more and more to fine grained the feature selection process to help to improve the performance of the IDS focusing on the most relevant properties Shams, E.A. and Rizaner, A., 2018.

2 ADVANCEMENTS IN DETECTION METHODOLOGIES

2.1 Hybrid Models

Sobehy, A., et al, 2020; Farahani, G., 2021. Hybrid approaches, integrating supervised and unsupervised techniques, combine the strengths of anomaly detection and signature-based methods. Such models are particularly effective in detecting zero-day attacks and reducing false positives.

2.2 Proactive Threat Mitigation

Pan, Z., et al., 2020; Scherer, D., et al., 2010, Proactive approaches leverage predictive analytics to anticipate and prevent attacks before they occur. Strategies include employing reinforcement learning to adapt IDS models dynamically.

2.3 Cloud-Based Intrusion Detection

O'shea, K. and Nash, R., 2015.; Dalal, R., Khari, M. and Hernandez, M., 2021, The transition to cloud-centric infrastructures necessitates IDS optimized for scalability and efficiency in virtualized environments. Recent advancements emphasize lightweight models for real-time anomaly detection in high-speed networks.

3 CHALLENGES AND RESEARCH GAPS

Despite advancements, IDS development faces persistent challenges:

- **Data Limitations:** Access to diverse and comprehensive datasets remains a critical bottleneck. Ensuring datasets represent varied attack scenarios is essential for model generalization.
- **Evolving Threats:** The dynamic nature of cyber threats demands IDS capable of adapting to novel attack patterns without manual intervention.
- **Interpretability:** Deep learning models, while accurate, often lack transparency. Enhancing interpretability is vital for building trust in automated systems. The comparative analysis of various IDS approaches is shown in Table 1.

Table 1: Comparative analysis of IDS approaches.

Model Type	Strengths	Weaknesses	Applications
Traditional IDS	Simple, rule-based	High false positives, inflexible	Basic networks
Deep Learning (CNN)	High accuracy, pattern recognition	High computational cost	Real-time traffic analysis
Deep Learning (RNN)	Handles sequential data	Slow for large datasets	Anomaly detection
Hybrid Models	Combines strengths of multiple approaches	Complex to implement, resource-intensive	Resource-constrained environments

3.1 Key Findings

- **Effectiveness of Deep Learning Models:** Studies demonstrate that CNNs and RNNs significantly improve the accuracy of IDS by recognizing patterns in large datasets**.**
- **Scalability and Efficiency:** Hybrid models combine cloud and edge processing for scalability while optimizing resource usage**.**
- **Challenges in Explainability:** Capuano, N., et al., 2022 The fact that deep learning models are opaque that requires integration of explainable AI (XAI) to improve trust and usability.

The research underscores the critical role of deep learning in advancing IDS for fog computing. While progress has been significant, addressing challenges like interpretability, data diversity, and ethical considerations are essential for future developments.

3.2 Detailed Insights from Literature Review

Table 2: Comparison between traditional and deep learning-based IDS.

Criteria	Traditional IDS	DeepLearning-Based IDS
Adaptability	Limited to predefined rules	Learns and adapts dynamically
Accuracy	Moderate, prone to false positives	High, robust anomaly detection
Scalability	Difficult to scale	Easily scalable with cloud and edge integration
Interpretability	High (rule-based)	Low (requires explainableAI)

The literature reveals the evolution of Intrusion Detection Systems (IDS) from traditional methods to sophisticated deep learning models tailored for fog computing environments. Key highlights include:

- **Transition from Rule-Based to Intelligent Systems**: Laqtib, S., et al, 2019; Nweke, et al., 2018 Traditional IDS relied on predefined rules, which limited their ability to adapt to emerging threats. Deep learning approaches have addressed these limitations by enabling dynamic anomaly detection.
- **Advancements in Neural Architectures**: Bjerrum, E.J. and Threlfall, R., 2017. Convolutional Neural Networks (CNN) excel in spatial data analysis, while Recurrent Neural Networks (RNN) handle temporal data effectively. Hybrid models integrating multiple architectures offer promising results.
- C**hallenges in Real-World Deployment**: Issues such as computational overhead, lack of interpretability, and data diversity remain significant barriers to adoption.The comparison of Traditional and Deep Learning-Based IDS is shown in Table 2.

3.3 Methodologies and Key Studies

A variety of methodologies have been employed in the development of IDS for fog computing. Table 3 highlights some key studies and their contributions.

Table 3: Methodologies, key findings and challenges.

Methodology	Key Findings	Challenges
CNN-based IDS	95% accuracy in anomaly detection	High computational cost
Hybrid CNN-LSTM	Improved detection of sequential patterns	Complex implementation
Transfer learning	Enhanced performance with less training data	Limited bydata scarcity
Real-time IDS	Significant reductionin response time for DDoS attacks	Resource constraints

3.4 Comprehensive Comparison of AI-Based Intrusion Detection Systems (IDS)

The comparison between various review articles based on their focus, approach, and methodology regarding AI-based Intrusion Detection Systems (IDS) is shown in Table 4.

The comparative analysis across various methodologies and systems reveals that while deep learning-based IDS offer significant advantages in terms of accuracy and adaptability, they require substantial computational resources and face challenges related to interpretability and real-world deployment. Hybrid models and explainable AI are promising directions to address these issues.

Table 4: Comparison of AI-based intrusion detection systems (IDS).

Reference	NIDS Focused	AI Approach	Specific IDS (SIDS)	HybridIDS
Aziz, Et al,	✓	ML, DL		✓
Ahmad,et al,	✓	ML, DL	✓	
Hodo, E., et al.	✓	ML	✓	✓
Sultana, Et al.	✓	DL	✓	
Moustafa, et al.,	✓	XAI	✓	✓
Fejrskov, Et al,	✓	ML	✓	
Lunt, T.F.	✓	DL	✓	
Axelsson		ML		✓
Liao		ML		✓

3.5 Literature Review on Key Themes

Literature reviews play a fundamental role in the scenario of academic research, providing a systematic framework through which a researcher can synthesize existing knowledge, identify predominant topics and discover vital gaps to establish a basis for greater research. In the domain of models for the detection of efficient intruders that use deep learning techniques for fog computing, the importance of the exhaustive review of literature cannot be exaggerated Poongothai, T. and Duraiswamy, K., 2014, These revisions serve not only as a complete description of the knowledge accumulated in the field, but also function as a critical evaluation tool that encourages the academic discourse necessary for the progress of knowledge.

Popli, R., et al., 2021 The proliferation of computing Nieblahas introduced a myriad of advances in cloud computing paradigms. The unique architecture of fog computing, characterized by its decentralized and distributed nature, introduces complexities and challenges in cybersecurity, which requires robust intruder detection mechanisms. This intersection of deep learning and computing fog requires a detailed exploration of existing literature to present not only the technological advances that have been made but also the critical theoretical and empirical frameworks applicable within this context.

Hussain, A., et al., 2020; Pilli, E.S., 2018. Research in intruder detection has gone through several methodological approaches ranging from statistical analysis to automatic learning. However, the advent of deep learning has redefined these approaches, offering new frames that demonstrate higher performance by recognizing patterns in large datasets. A review of the literature that focuses on this area reveals significant issues, such as the evolution of intruder detection techniques, from traditional methods to sophisticated neural networks that focus in the extraction of characteristics and the optimization of performance. Studies have illustrated how CNN and RNN can effectively analyse complex data flows in real - time fog computer networks, significantly improving intrusions detection rates while maintaining the low positive fake relationships.

Janicke, H., et al., 2019., In addition, the systematic analysis of the methodologies used in these studies is essential to understand the advances made in the field. Several researchers have used various experimental designs, including comparative analysis of different deep learning models, set techniques and the merger of automatic learning with rules -based systems. Mambo, M., et al., 2018. This methodological diversity articulates the multifaceted nature of cybersecurity challenges in computing fog and underlines the need for personalized solutions that can dynamically respond to evolving threats. An examination of these methodologies not only informs researchers about best practices, but also highlights the deficiencies present in current research, preparing the scenario for innovative solutions.

Karasfi, B., et al., 2024. Insights derived from the corpus of studies listed in Table 1 above concerning deep learning-based intrusion detection in fog computing highlight the urgent need for an effective solution. Numerous experiments provide evidence of how deep -learning methods positively impact the accuracy and performance characteristics of intrusion detection systems, as they help to overcome the aforementioned stagnation issues that have characterized long-standing traditional techniques. Moreover, these results shed light on the practical relevance of such approaches in the real world, e.g., taking into account the scalability, adaptability and efficiency of critical computing resources in fog environments.

In summary, the exploration of the existing literature within the scope of intrusions within the computing environments serves as a critical component to advance in this field in constant evolution. This systematic approach not only helps delineate the existing knowledge, but also facilitates the identification of gaps that demand more research, ultimately contributing to the development of improved intruder's detection models capable of safeguarding the integrity of the computer systems of fog against an increasingly sophisticated landscape of cyber security threats. The evolution of intrusions detection systems (ID) was significantly modelled by the proliferation of different processing environments, in particular with the advent of fog technologies. IDs, originally designed to monitor and analyse network traffic for suspicious activities, have more and more integrated methodologies advanced to adapt to the complexities of modern IT infrastructures. One of the predominant themes in literature is the transition from traditional ID based on the network to more dynamic systems and sensitive to the context capable of operating in distributed environments.

Min, G., et al., 2017, Another critical theme that emerges from literature is the challenge of dealing with large quantities of data generated in the fog computing scenarios. The researchers identified the need for scalable architecture that exploit the distributed nature of the calculation of the fog to process and analyse the data efficiently. This led to

the proposal of hybrid models that combine the strengths of the centralized elaboration of the cloud with the calculation solutions of the edges, allowing a more robust and resilient IDS framework. These models often use learning techniques of ensembles, which aggregate forecasts from various deep learning models to improve accuracy and reduce false positive rates, a common problem in many IDS implementations.

Kumar, V., et al., 2017. In addition, security and privacy problems in the fog calculation environments introduce further levels of complexity that are addressed in existing literature. The dynamic nature limited to the resources of the nodes of fog requires the development of light learning models that maintain performance by minimizing computational general expenses. Techniques such as the pruning of the model and the distillation of knowledge have been designed as a means of optimizing deep learning algorithms for distribution in bound environments, ensuring that ID can operate efficiently without compromising safety measures.

Venkatraman, S., et al., 2019., The integration of deep learning within IDS is not without critical points of view. Some scholars underline the interpretation of profound learning models, raising concerns about the opaque decision -making processes relating to these algorithms. This problem has significant implications for computer security applications, in which the understanding of the logic underlying the surveys of the threats is crucial for the response to accidents. Ranjan, R., et al., 2023.Consequently, literature has also explored methods to improve interpretation, such as the integration of AI Techniques of explainable (XAI), allowing safety analysts to obtain insights on the underlying processes of detection of anomalies.

In summary, the intersection of intrusions detection systems, fog and deep learning methodologies has led to significant progress in the safety measures within modern processing environments. Key themes emerging from literature underline the adaptability of IDS technologies to meet rapid changes in the generation of data and in the processing requirements, while facing the intrinsic challenges posed by scalability, performance and interpretation., The examination of methodologies employed in the current research on intrusions has revealed a significant change in the implementation of deep learning approaches, particularly in the context of fog computing environments. Sukarno, P., et al., 2024.The need for robust and efficient intrusion detection systems (IDS) is underlined by the growing complexity and scale of network architectures that integrate fog computing, characterized by their distributed nature and heterogeneous resources. Recent literature highlights that traditional intrusion detection techniques, usually limited by set sets of predefined rules and inability to adapt to evolving threats, may be insufficient to meet the demands of contemporary digital communication infrastructures.

Ai, X., et al., 2023 Moreover, deep learning methodologies are not only applicable to traditional network intrusion scenarios, but also were effectively adapted to improve pedagogical approaches, particularly in educational environments. Deep learning models can be used to analyze writing and understanding, which can be used to detect not only cyber security threats, but also indicative patterns of student challenges. This interdisciplinary application illustrates the movement towards a holistic view of intrusive detection systems, where the resilience of educational platforms against potential vulnerabilities is fundamental.

Tao, X., et al., 2021.In addition to CNNS and RNNS, a variety of hybrid models have also emerged that combine the strengths of multiple deep learning architectures to further improve detection capabilities. For example, the integration of short-term memory networks (LSTM) with CNNs has shown to produce higher results in the recognition of sequential patterns in the typical data flows of attempted intrusion. Such innovations emphasize a methodological trend for the adoption of set learning techniques that amalgamates various model predictions to improve general performance and robustness.

The literature suggests that the complexity of cyber threats requires a multidisciplinary approach, drawing from areas such as data science, behavioral analysis and network theory. The need for comprehensive literature revisions becomes even more pronounced in considering the wide range of emerging challenges - from rapidly changing threat actors to the wide variety of environments in which intrusive detection systems are implanted. A strict analysis of previous research provides a fundamental context to categorize these challenges and identify gaps in which more innovation is imperative.

Data errors and complexity in diverse domains warrant methodological and technological evolution for effective resolution of intrusions, especially in adaptive contexts such as those in networks under consideration of IoT and Cloud computing methods. As successful initiatives demonstrate, addressing these modern challenges requires not just an up technological infrastructure, but also a re-examination of the geostrategic paradigms that have historically guided research. These roles highlight the

importance of ongoing engagement with the existing literature to shape new questions and research approaches that address modern cyber security needs.

Last but not least, the review pushes scholars and practitioners to explore the literature further. Findings of previous section emphasize how in-depth revision drives future analyses and increment success of intrusion detection model. This amalgamation will help the community go beyond the limitations of both the frameworks and the emerging technologies while paving the way for novel frameworks that would help us in the continuous evolution of the field and its effective mitigation of threats. Therefore, the future of intrusion detection research should be guided by literature reviews that meet high standards.

4 FUTURE DIRECTIONS

- **Explainable AI:** Developing interpretable IDS models will foster collaboration between human analysts and automated systems, improving overall threat management.
- **Adversarial Robustness:** Enhancing resilience to adversarial attacks is critical. This includes designing models that can withstand deliberate perturbations in input data.
- **Integration with Emerging Technologies:** Future IDS will benefit from integration with technologies such as **blockchain** and **quantum computing** for enhanced security and scalability.

5 CONCLUSIONS

Deep learning and machine learning techniques have merged together to result in improved capabilities of intrusion detection systems. By addressing current problems and exploring emerging technologies, researchers can offer robust defensive capabilities against the ever-evolving cyber threat landscape and thus lay the groundwork for next-generation IDS technology.

Deep learning approaches such as RNN, wrapper-based feature maps, long short-term memory (LSTM) are interesting. The goal of these approaches is to improve the performance and resilience of IDS against advanced cyber-attacks. In addition, optimization strategies, on the other hand, integrate PSO, global optimization algorithms, nature-inspired optimization, and metaheuristic methods. This in turns allows to make Systems more reliable, optimize their performance and accurate detection.

Studies of ensemble learning and hybrid models show that proposed methods are neural networks, hybrid approaches, and combined classifiers. This not only improves the performance of IDS but also addresses real world attacks and increases accuracy, while reducing false alarms. In addition, benchmarking and comparison studies provide useful insights about the benefits and drawbacks of deep learning models compared to traditional machine learning models. The importance of cloud-oriented security solutions speaks to the need for specialized intrusion detection systems suited for the cloud-based architectures. Cloud computing networks must adapt to shifting security threats using scalable, efficient and secure approaches.

These studies are aimed at protecting wireless platforms and developing dedicated intrusion detection systems (IDS) for secure wireless communications. In conclusion, proactive intrusion detection research can be referred to as a preventive approach to detect intrusions beforehand. These models increase the IDSs' ability to combat new threats by focusing on the optimization of search algorithms and by converging quickly.

REFERENCES

Abdan, M. and Seno, S.A.H., 2022. Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET). Wireless Communications and Mobile Computing, 2022(1), p.2375702.

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J. and Ahmad, F., 2021. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), p.e4150.

Ahmim, A., Maglaras, L., Ferrag, M.A., Derdour, M. and Janicke, H., 2019, May. A novel hierarchical intrusion detection system based on decision tree and rules-based models. In 2019 15th International conference on distributed computing in sensor systems (DCOSS) (pp. 228-233). IEEE.

Axelsson, S., 2000. Intrusion detection systems: A survey and taxonomy. Chalmers Univ. Technol., Gothenburg, Sweden, Tech. Rep. 99-15

Aziz, A.S.A., Sanaa, E.L. and Hassanien, A.E., 2017. Comparison of classification techniques applied for network intrusion detection and classification. Journal of Applied Logic, 24, pp.109-118.

Bjerrum, E.J. and Threlfall, R., 2017. Molecular generation with recurrent neural networks (RNNs). arXiv preprint arXiv:1705.04612.

Capuano, N., Fenza, G., Loia, V. and Stanzione, C., 2022. Explainable artificial intelligence in cybersecurity: A survey. Ieee Access, 10, pp.93575-93600.

Dalal, R., Khari, M. and Hernandez, M., 2021. Persuasive simulation of optimized protocol for OppNet. Dynamic Systems and Applications, 30(5), pp.865-900.

Dwivedi, R., Dave, D., Naik, H., Singhal, S., Omer, R., Patel, P., Qian, B., Wen, Z., Shah, T., Morgan, G. and Ranjan, R., 2023. Explainable AI (XAI): Core ideas, techniques, and solutions. ACM Computing Surveys, 55(9), pp.1-33.

Farahani, G., 2021. Black hole attack detection using K-nearest neighbor algorithm and reputation calculation in mobile ad hoc networks. Security and communication Networks, 2021(1), p.8814141.

Fejrskov, M., Pedersen, J.M. and Vasilomanolakis, E., 2020, June. Cyber-security research by ISPs: a NetFlow and DNS anonymization policy. In 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-8). IEEE.

Ghimire, S., Yaseen, Z.M., Farooque, A.A., Deo, R.C., Zhang, J. and Tao, X., 2021. Streamflow prediction using an integrated methodology based on convolutional neural network and long short-term memory networks. Scientific Reports, 11(1), p.17497.

Goodfellow, I., Bengio, Y. and Courville, A Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

Hamza, F. and Maria Celestin Vigila, S., 2019. Review of machine learning-based intrusion detection techniques for MANETs. In Computing and Network Sustainability: Proceedings of IRSCNS 2018 (pp. 367-374). Springer Singapore

Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C. and Atkinson, R., 2017. Shallow and deep networks intrusion detection system: A taxonomy and survey. arXiv preprint arXiv:1701.02145.

Ieracitano, C., Adeel, A., Morabito, F.C. and Hussain, A., 2020. A novel statistical analysis and autoencoder driven intelligent intrusion detection approach. Neurocomputing, 387, pp.51-62.

Kanthimathi, S. and Prathuri, J.R., 2020, November. Classification of misbehaving nodes in MANETS using machine learning techniques. In 2020 2nd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS) (pp. 1-2). IEEE

Kim, S. and Park, K.J., 2021. A survey on machine-learning based security design for cyber-physical systems. Applied Sciences, 11(12), p.5458.

Laqtib, S., Yassini, K.E. and Hasnaoui, M.L., 2019, October. A deep learning method for intrusion detection systems-based machine learning in MANET. In Proceedings of the 4th international conference on smart city applications (pp. 1-8).

Laqtib, S., El Yassini, K. and Hasnaoui, M.L., 2020. A technical review and comparative analysis of machine learning techniques for intrusion detection systems in MANET. International Journal of Electrical and Computer Engineering, 10(3), p.2701.

Liao, H.J., Lin, C.H.R., Lin, Y.C. and Tung, K.Y., 2013. Intrusion detection system: A comprehensive review. Journal of network and computer applications, 36(1), pp.16-24.

Liu, Y., Fieldsend, J.E. and Min, G., 2017. A framework of fog computing: Architecture, challenges, and optimization. IEEE Access, 5, pp.25445-25454.

Lunt, T.F., 1993. A survey of intrusion detection techniques. Computers & Security, 12(4), pp.405-418.

Mishra, P., Varadharajan, V., Tupakula, U. and Pilli, E.S., 2018. A detailed investigation and analysis of using machine learning techniques for intrusion detection. IEEE communications surveys & tutorials, 21(1), pp.686-728.

Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A.Y. and Tari, Z., 2023. Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions. IEEE Communications Surveys & Tutorials, 25(3), pp.1775-1807

Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M.A., Choudhury, N. and Kumar, V., 2017. Security and privacy in fog computing: Challenges. IEEE Access, 5, pp.19293-19304.

Najafli, S., Toroghi Haghighat, A. and Karasfi, B., 2024. Taxonomy of deep learning-based intrusion detection system approaches in fog computing: a systematic review. Knowledge and Information Systems, 66(11), pp.6527-6560.

Nishani, L. and Biba, M., 2016. Machine learning for intrusion detection in MANET: a state-of-the-art survey. Journal of Intelligent Information Systems, 46, pp.391-407.

Nishani, L. and Biba, M., 2016. Machine learning for intrusion detection in MANET: a state-of-the-art survey. Journal of Intelligent Information Systems, 46, pp.391-407.

Nweke, H.F., Teh, Y.W., Al-Garadi, M.A. and Alo, U.R., 2018. Deep learning algorithms for human activity recognition using mobile and wearable sensor networks: State of the art and research challenges. Expert Systems with Applications, 105, pp.233-261.

O'shea, K. and Nash, R., 2015. An introduction to convolutional neural networks. arXiv preprint arXiv:1511.08458

Pan, Z., Wang, Y. and Pan, Y., 2020. A new locally adaptive k-nearest neighbor algorithm based on discrimination class. Knowledge-Based Systems, 204, p.106185.

Pandey, A., Kumar, S., Pattanaik, B. and Pattnaik, M., 2021. A Survey: Machine Learning Algorithms for Network Security. SSRN Electron. Journal

Poongothai, T. and Duraiswamy, K., 2014, February. Intrusion detection in mobile AdHoc networks using machine learning approach. In International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1-5). IEEE

Popli, R., Sethi, M., Kansal, I., Garg, A. and Goyal, N., 2021, August. Machine learning based security solutions in MANETs: State of the art approaches. In Journal of physics: conference series (Vol. 1950, No. 1, p. 012070). IOP Publishing

Popli, R., Sethi, M., Kansal, I., Garg, A. and Goyal, N., 2021, August. Machine learning based security solutions in MANETs: State of the art approaches. In Journal of physics: conference series (Vol. 1950, No. 1, p. 012070). IOP Publishing.

Roman, R., Lopez, J. and Mambo, M., 2018. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, pp.680-698.

Scherer, D., Müller, A. and Behnke, S., 2010, September. Evaluation of pooling operations in convolutional architectures for object recognition. In International conference on artificial neural networks (pp. 92-101). Berlin, Heidelberg: Springer Berlin Heidelberg.

Shams, E.A. and Rizaner, A., 2018. A novel support vector machine-based intrusion detection system for mobile ad hoc networks. Wireless Networks, 24, pp.1821-1829

Siddiqui, M.N., Malik, K.R. and Malik, T.S., 2021, May. Performance analysis of blackhole and wormhole attack in MANET based IoT. In 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2) (pp. 1-8). IEEE.

Sobehy, A., Renault, É. and Mühlethaler, P., 2020. CSI-MIMO: K-nearest neighbor applied to indoor localization. In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

Sultana, N., Chilamkurti, N., Peng, W. and Alhadad, R., 2019. Survey on SDN based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking and Applications, 12(2), pp.493-501.

Thakkar, A. and Lohiya, R., 2021. A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges. Archives of Computational Methods in Engineering, 28(4), pp.3211-3243.

Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A. and Venkatraman, S., 2019. Deep learning approach for intelligent intrusion detection system. IEEE access, 7, pp.41525-41550.

Wardana, A.A., Kołaczek, G., Warzyński, A. and Sukarno, P., 2024. Collaborative intrusion detection using weighted ensemble averaging deep neural network for coordinated attack detection in heterogeneous network. International Journal of Information Security, 23(5), pp.3329-3349.

Weng, C., Chen, C. and Ai, X., 2023. A pedagogical study on promoting students' deep learning through design-based learning. International journal of technology and design education, 33(4), pp.1653-1674.

Xiao, H., Biggio, B., Nelson, B., Xiao, H., Eckert, C. and Roli, F., 2015. Support vector machines under adversarial label contamination. Neurocomputing, 160, pp.53-62.