Sl. No	Title	Journal	Authors' Name	Year	Novelty	Advantage/Disadvantage
1	Machine Learning Algorithms for Network Intrusion Detection	IEEE Xplore	Jie Li, Yanpeng Qu, Fei Chao, Hubert P. H. Shum	2019	This work innovatively focuses on combating network intrusion by systematically reviewing and evaluating intrusion detection systems using fuzzy logic and artificial neural networks. The study distinguishes itself through a rigorous analysis utilizing the widely accepted KDD 99 benchmark dataset, providing a credible basis for findings. The proactive identification and disconnection of malicious network traffic emphasize a preventive approach. The comparative analysis of fuzzy logic and artificial neural networks offers valuable insights, and the forward-looking perspective, summarizing key challenges and suggesting future directions, enhances the research's novelty by contributing to ongoing advancements in artificial intelligence-based cybersecurity.	Advantages: Novel focus on fuzzy logic and neural networks enhances intrusion detection. Rigorous evaluation using the KDD 99 dataset adds credibility. Proactive identification and disconnection of malicious traffic strengthen cybersecurity. Disadvantages: Limited discussion on potential limitations of fuzzy logic and neural networks. The scope of the KDD 99 dataset may not capture all contemporary threats.
	Network intrusion detection system: A systematic study of machine learning and deep learning approaches	Emerging Telecommunication Technologies	Zeeshan Ahmad, Adnan Shahid Khan,Cheah, Wai Shiang Johari Abdullah, Farhan Ahmad	2020	The novelty of this article lies in its comprehensive exploration of machine learning (ML) and deep learning (DL)-based Intrusion Detection Systems (IDS) in the context of network security. It provides a refined taxonomy of ML and DL techniques, reviews recent NIDS-based articles, discusses strengths and limitations, and highlights current trends. The identification of research challenges and future research directions adds depth, offering a valuable roadmap for improving ML and DL-based NIDS amid evolving cyber threats.	Advantage: The article provides a thorough exploration of ML and DL-based Intrusion Detection Systems, offering a refined taxonomy, reviewing recent articles, and identifying trends. It serves as a valuable resource for researchers and practitioners in the rapidly evolving field of network security. Disadvantage: The article may lack specificity in addressing individual limitations of ML and DL-based IDS solutions, potentially requiring readers to seek more detailed insights into specific challenges associated with these systems.

3	Deep learning applications and challenges in big data analytics	Journal of Big Data, Springer	Maryam M Najafabadi, Flavio Villanustre	2015	This study explores the synergy between Big Data Analytics and Deep Learning, emphasizing Deep Learning's ability to extract intricate patterns from vast unlabeled datasets. Novel aspects include addressing challenges such as streaming data, high-dimensional data, and scalability in the context of Big Data, paving the way for future research in sampling criteria, domain adaptation, and improved data abstraction techniques.	Advantages: Deep Learning excels in extracting complex patterns from massive unlabeled data, enhancing semantic indexing, and simplifying discriminative tasks in Big Data Analytics. Disadvantages: Challenges include handling streaming and high-dimensional data, ensuring model scalability, and addressing distributed computing complexities, requiring ongoing research for effective solutions in these domains.
4	Comparison Deep Learning Method to Traditional Methods Using for Network Intrusion Detection	IEEE International Conference on Communication Software and Networks	Bo Dong, Xue Wang	2016	This paper explores the application of deep learning techniques in intrusion detection, aiming to enhance performance and accuracy beyond traditional methods. Through experiments on an open dataset, various classification methods are employed to identify the most effective approach for robust network traffic classification and intrusion detection.	Advantages: Deep learning offers superior pattern recognition, adaptability, and automated feature extraction, improving intrusion detection accuracy. It excels in handling complex, evolving threats. Disadvantages: Challenges include high computational requirements, the need for extensive labeled data, and potential vulnerability to adversarial attacks. Interpretability and explainability can be limited in deep learning models.
5	Taxonomy and Survey of Collaborative Intrusion Detection	Research Gate	EMMANOUIL VASILOMANOLAKIS, SHANKAR KARUPPAYAH, MAX MUHLH ¨ AUSER, ¨ and MATHIAS FISCHER	2015	The novelty lies in Collaborative Intrusion Detection Systems (CIDS), a response to escalating cyber threats. CIDS integrates monitoring components to analyze and correlate data, addressing scalability issues of conventional IDS. This framework enhances defense against sophisticated attacks, safeguarding the growing dependency of society on networked computers and critical infrastructures.	Advantages of Collaborative Intrusion Detection Systems (CIDS): Enhanced scalability, holistic network protection, and improved threat detection through collaborative data analysis. Disadvantages: Increased complexity, potential privacy concerns due to extensive data sharing, and susceptibility to coordinated attacks targeting the CIDS infrastructure.

6	Deep Learning Approach for Intelligent Intrusion Detection System	IEEE journal	R. VINAYAKUMAR, MAMOUN ALAZAB	2019	This paper introduces a novel approach in the field of intrusion detection systems (IDS) by leveraging deep neural networks (DNNs) to effectively detect and classify dynamic cyberattacks. Through comprehensive evaluations on diverse publicly available malware datasets, the study establishes DNNs as superior to classical machine learning classifiers, culminating in the proposal of a highly scalable and hybrid framework, "scale-hybrid-IDS-AlertNet," capable of real-time monitoring and proactive cyberattack alerts.	Advantages: DNNs excel in capturing complex, evolving cyber threats, providing high-dimensional feature representation. The proposed "scale-hybrid-IDS-AlertNet" offers scalability and real-time monitoring. Disadvantages: DNNs require substantial computational resources, and hyperparameter tuning can be challenging. The model's reliance on extensive data may pose privacy concerns.
7	TIDCS: A Dynamic Intrusion Detection and Classification System Based Feature Selection	IEEE journal	ZINA CHKIRBENE, , AIMAN ERBAD	2020	TIDCS introduces a feature selection algorithm grouping and ranking features for reduced data complexity. TIDCS-A adds a dynamic algorithm for optimal node cleansing, enhancing intrusion detection in secure networks.	Advantages: TIDCS and TIDCS-A improve intrusion detection with feature selection, achieving higher accuracy, detection rates, and lower false alarms. Dynamic system cleansing, based on trust relationships, ensures adaptive responses to evolving threats. Disadvantages: Challenges include potential delays due to periodic system cleansing and the feature selection algorithm's sensitivity to initial random grouping. The effectiveness of trust-based models may vary based on network characteristics, and the robustness of the approach could be impacted. Network-dependent factors may influence the adaptability of the proposed models.

8	An Analysis of the KDD99 and UNSW-NB15 Datasets for the Intrusion Detection System	MDPI	Muataz Salam Al-Daweri, Khairul Akram Zainol Ariffin	2017	This study introduces a comprehensive analysis of feature relevance in KDD99 and UNSW-NB15 intrusion detection datasets using rough-set theory, back-propagation neural network, and a discrete variant of the cuttlefish algorithm, aiming to aid in the development of lightweight and accurate IDS models.	Advantages: The study identifies key features contributing to high classification accuracy, providing insights for creating efficient intrusion detection systems with reduced feature sets. Disadvantages: While effective, the proposed methods may require further validation and consideration of potential biases in the dataset, and the study's applicability to evolving cybersecurity threats needs continuous assessment.
9	Machine Learning Techniques for Classifying Network Anomalies and Intrusions	IEEE Xplore	Zhida Li, Ana Laura Gonzalez	2019	This study introduces a comparative analysis of deep learning models, including LSTM, GRU, and BLS variants, for network intrusion detection using diverse BGP and NLS-KDD datasets. It explores the effectiveness of these models in cybersecurity applications.	Advantages: LSTM and GRU capture sequential dependencies, enhancing the detection of complex patterns. BLS introduces a novel approach by leveraging broad learning, potentially improving adaptability. The study provides insights into their performance on real-world datasets, contributing to the evolving field of network intrusion detection. Disadvantages: LSTM and GRU's computational complexity may limit scalability. BLS may face challenges in handling diverse network patterns due to its reliance on broad learning. Careful consideration of dataset characteristics and computational resources is crucial for selecting the most suitable model in practical cybersecurity applications.

10	A Novel Intrusion Detector Based on Deep Learning Hybrid Methods	IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity)	Wang Shizhao, Xia Chunhe	2019	Introducing the LSTMTree model, an enhanced intrusion detection system using long short-time memory (LSTM) in recurrent neural network (RNN) units, featuring secondary detection capabilities to address the high false negative rates of traditional RNN-based detectors.	Advantages: LSTMTree significantly improves detection performance over previous models, particularly in predicting unknown attacks and achieving higher detection accuracy. Disadvantages: While effective, LSTMTree may potentially involve increased computational complexity and resource requirements compared to simpler intrusion detection systems.
11	Deep Learning for IoT Big Data and Streaming Analytics: A Survey	IEEE COMMUNICATIONS SURVEYS & TUTORIALS	Mehdi Mohammadi	2018	Novelty: Focus on IoT data characteristics, distinction between big data and streaming analytics, exploration of fog/cloud integration, and guidance for future research contribute to the paper's novelty.	Advantages: Deep learning enables scalable processing and predictive analytics on large IoT datasets, facilitating real-time insights and comprehensive overviews. Integration into smart IoT devices enhances edge intelligence for improved efficiency. Disadvantages: Complex implementation and resource demands, privacy/security concerns, limited device resources, interpretability challenges, and susceptibility to overfitting pose obstacles.
12	Packet Sniffing and Sniffing Detection	international Journal of Innovations in Engineering and Technology	Ruchi Tuli	2020	Novelty: The paper delves into the basics of packet sniffing, vulnerable network protocols, and defensive techniques, offering a comprehensive understanding of sniffing attacks and detection methods.	Advantages: Packet sniffers provide insight into network traffic, aiding in troubleshooting and network optimization. They can detect vulnerabilities in network protocols and help improve security measures. Disadvantages: Misuse of packet sniffers can compromise privacy and security, enabling attackers to intercept sensitive information. Defending against sniffing attacks requires constant vigilance and implementation of robust security measures.

13	Comparative Study of two Most Popular Packet Sniffing Tools-Tcpdump and Wireshark	International Conference on Computational Intelligence and Communication Networks	Piyush Goyal1 and Anurag Goyal2	2017	Novelty: The paper provides a thorough comparison of Wireshark and Tcpdump, two widely used open-source packet sniffing and network monitoring tools. This comparative analysis offers insights into their features, capabilities, and suitability for various network security needs.	Advantages: Network monitoring and packet sniffing tools such as Wireshark and Tcpdump assist network administrators in assessing server performance, diagnosing issues, and ensuring data transfer security. White Hat hackers utilize these tools to identify and filter out malicious packets, preventing cyber attacks. Disadvantages: Despite their intended purpose, these tools can be exploited by cyber criminals for eavesdropping and illegal access to unprotected data, posing security risks to networks and systems.
14	Ethical Network Surveillance using Packet Sniffing Tools: A Comparative Study	MECS	ibrahim Ali Ibrahim Diyeb , Dr. Anwar Saif	2018	Novelty: This paper offers a comprehensive comparison of three popular packet sniffing tools—TCPDump, Wireshark, and Colasoft—based on detection ability, filtering, availability, operating system support, open-source status, GUI features, and other characteristics. It serves as a valuable resource for researchers seeking insights into packet sniffing techniques and tools for network security.	Advantages: Intrusion detection systems and packet sniffing tools enhance network security by gathering and analyzing data traffic, aiding in identifying external threats and monitoring internal misuse of IT assets. Packet sniffers convert binary data into readable formats, allowing administrators to detect vulnerabilities and make informed decisions to safeguard the network. Disadvantages: While beneficial for security, packet sniffing tools can also pose privacy risks by capturing sensitive information such as usernames and passwords. Moreover, the abundance of sniffing tools requires careful consideration of their detection abilities, filtering capabilities, and compatibility with various operating systems.

15	Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis	International Journal of Electrical, Electronics and Computer Engineering	Pallavi Asrodia and Hemlata Patel	2016	Novelty: This paper provides an overview of packet sniffers, detailing their working principles and capabilities for network monitoring and analysis. It serves as a valuable resource for understanding the basics of packet sniffing and selecting appropriate tools for network management.	Advantages: Packet sniffing aids in network management, maintenance, and monitoring, improving economic efficiency by troubleshooting and logging network activities. It benefits both software engineers and administrators, offering insights into network performance and potential issues. Disadvantages: While beneficial for network management, packet sniffing raises privacy concerns as it can capture sensitive data. Additionally, the multitude of available packet sniffing tools requires careful consideration of their capabilities and compatibility for effective network monitoring.

16	A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked SystemsStudy of Vulnerabilities of ARP Spoofing and its detection using SNORT	IEEE International Conference on Distributed Computing Systems	Xinyu Yang, Jie Lin, Paul Moulema†, Wei Yu	2017	Novelty: PCREF introduces the use of polynomials instead of MACs for endorsing measurement reports, enhancing resilience to attacks. Through theoretical analysis and simulation experiments, PCREF demonstrates superior filtering capacity and resilience to a large number of compromised nodes compared to existing schemes, contributing to advancements in CPNS security.	Advantages: PCREF addresses the challenge of false measurement injection in Cyber-Physical Networked Systems (CPNS) by proposing a Polynomial-based Compromised-Resilient En-route Filtering scheme. It effectively filters false data and demonstrates high resilience to compromised nodes without relying on static routes or node localization. Disadvantages: The implementation complexity of PCREF may require careful consideration, and its effectiveness in real-world CPNS scenarios would need validation through practical deployment and testing.
17	Study of Vulnerabilities of ARP Spoofing and its detection using SNORT	International Journal of Advanced Research in Computer Science	Rajneet Kaur Bijral , Alka Gupta	2017	Novelty: This paper contributes to the understanding of ARP Spoofing as a design-level vulnerability and its potential for various attacks like session hijacking. It presents empirical evidence of Snort's performance in detecting ARP Spoofing on real networks, offering insights for improving network security.	Advantages: The paper addresses the growing threats to information security by discussing the design-level vulnerability of ARP Spoofing. It highlights the importance of detecting such vulnerabilities using tools like Snort to protect organizational information from unauthorized access. Disadvantages: While Snort is effective for detecting ARP Spoofing, its performance may vary based on factors like the number of targets, necessitating careful experimentation and analysis for optimal deployment.

18	A Detailed Survey for Detection and Mitigation Techniques against ARP Spoofing	IEEE Xplore	Vaishnavi Rohatgi , Shimpy Goyal	2021	Novelty: By addressing ARP Spoofing Attacks and comparing detection and mitigation techniques, the paper contributes to the understanding of network security vulnerabilities and strategies for protecting against malicious attacks. However, the novelty of the paper may be limited without original research or innovative approaches to ARP security.	Advantages: The paper provides a comprehensive overview of ARP (ADDRESS RESOLUTION PROTOCOL) and its role in computer networking, offering insight into its vulnerabilities and susceptibility to ARP Spoofing Attacks. It also compares different detection and mitigation techniques, facilitating informed decisions for network security. Disadvantages: While the paper discusses detection and mitigation techniques, it may lack detailed analysis or empirical evidence of their effectiveness in real-world scenarios. Additionally, the inclusion of 11 journals may lead to information overload without clear synthesis or prioritization of key findings.
19	ARP SPOOFING DETECTION FOR IOT NETWORKS USING NEURAL NETWORKS	IEEE Xplore	Husain Abdulla, Hamed Al-Raweshidy,	2018	Novelty: This paper contributes to the field of IoT security by introducing an innovative detection method using artificial intelligence and neural networks. By demonstrating superior accuracy compared to traditional methods, it offers a novel approach to mitigating ARP-Spoofing attacks in IoT networks, paving the way for future research in this area.	Advantages: The paper addresses the growing threat of ARP-Spoofing attacks on IoT devices and proposes a novel detection method based on artificial intelligence and neural networks. It demonstrates high accuracy, surpassing traditional statistical methods like ARIMA, thus offering a promising solution for securing IoT networks. Disadvantages: While the proposed method shows high accuracy, its implementation complexity and resource requirements may pose challenges for practical deployment in IoT environments. Additionally, the paper could benefit from further discussion on the limitations or potential drawbacks of the neural network-based approach.

20	Experimental and Comparative Analysis of Packet Sniffing Tools	International Conference on Data Engineering and Communication Technology	Chunduru Anilkumar, D. Paul Joseph, V. Madhu Viswanatham, Aravind Karrothu	2018	Novelty: By exploring various attacks and threats faced by IDPS and proposing a new attack scenario, the paper offers insights into the challenges and vulnerabilities of current network security measures. The comparison of existing IDS/IDPS techniques and tools provides valuable information for enhancing network security in diverse environments, contributing to advancements in the field.	Advantages: The paper provides an overview of intrusion detection systems (IDS) and intrusion detection and prevention systems (IDPS), highlighting their significance in detecting and preventing malicious activities across networks. It explores the limitations of IDS and the introduction of IDPS to address new attack vectors, contributing to the understanding of network security measures. Disadvantages: While the paper discusses the evolution of IDS and IDPS and their role in network security, it may lack in-depth analysis or empirical evidence of the effectiveness of different techniques and tools. Additionally, the creation of a new attack to bypass IDPS monitoring could pose ethical concerns and may require careful consideration.