Archives available at journals.mriindia.com

International Journal of Electrical, Electronics and Computer Systems

ISSN: 2347-2820

Volume 12 Issue 02, 2023

A Survey of Methods and Architectures for Multi-Attack Detection using Forensics and Coherent Integrated Photonic Neural Networks-Based Prevention for Secure IoT-MANETs

Behruz Ramasubbu
Assistant Professor, Department of Electrical and Computer Engineering, Eastern Frontier Institute of Technology and Management, India
Email: behruz.ramasubbu@efitm-in.edu

Peer Review Information

Submission: 24 June 2023

Revision: 12 July 2023

Acceptance: 22 July 2023

Keywords

IoT Security, MANET, Multi-Attack Detection, Intrusion Detection System (IDS), Deep Learning, Photonic Neural Networks.

Abstract

The rapid growth of the Internet of Things (IoT) and Mobile Ad Hoc Networks (MANETs) has enabled decentralized and scalable communication, but their distributed nature and resource constraints make them highly vulnerable to cyber-attacks such as DDoS, black hole, wormhole, and spoofing, which degrade performance and compromise data integrity. Traditional intrusion detection systems (IDS) often fail to address these complex threats due to limited scalability and adaptability. To overcome these challenges, recent approaches leverage deep learning, forensic analytics, and photonic neural networks for efficient multi-attack detection. Deep learning models, including CNN, LSTM, and hybrid architectures, have shown high accuracy in identifying anomalous traffic patterns, while forensic techniques enhance post-attack analysis and support proactive defense strategies. Additionally, photonic neural networks provide ultra-fast processing with reduced latency and energy consumption, making them suitable for real-time IoT-MANET environments. Comparative studies indicate that hybrid deep learning models combined with optimization techniques outperform conventional methods in terms of detection accuracy and computational efficiency. However, challenges such as dataset imbalance, real-time deployment, and energy efficiency still persist. This study highlights key advancements, identifies research gaps, and provides insights into future directions for developing robust and scalable intrusion detection mechanisms to secure IoT-MANET systems against multi-attack scenarios.

Introduction

The emergence of the Internet of Things (IoT) has significantly transformed modern communication systems by enabling seamless interaction among interconnected devices such as sensors, smart appliances, and industrial systems. IoT networks are widely deployed in applications including smart cities, healthcare monitoring, industrial automation, and intelligent transportation. However, the rapid expansion of IoT has introduced critical security challenges due to device heterogeneity, limited computational resources, and large-scale connectivity. These characteristics make IoT environments highly vulnerable to cyber threats, where even a small security breach can compromise large volumes of sensitive data and disrupt essential services.

Mobile Ad Hoc Networks (MANETs) further extend this complexity by providing

decentralized and infrastructure-less communication. Nodes in MANETs dynamically form connections, making them highly adaptable for applications such as disaster recovery and military operations. However, their dynamic topology and lack of centralized control expose them to attacks such as black hole, wormhole, and denial-of-service. When IoT systems are integrated with MANETs, the resulting IoT-MANET architecture inherits vulnerabilities from both domains, creating a highly complex and dynamic threat environment that is difficult to secure using conventional approaches.

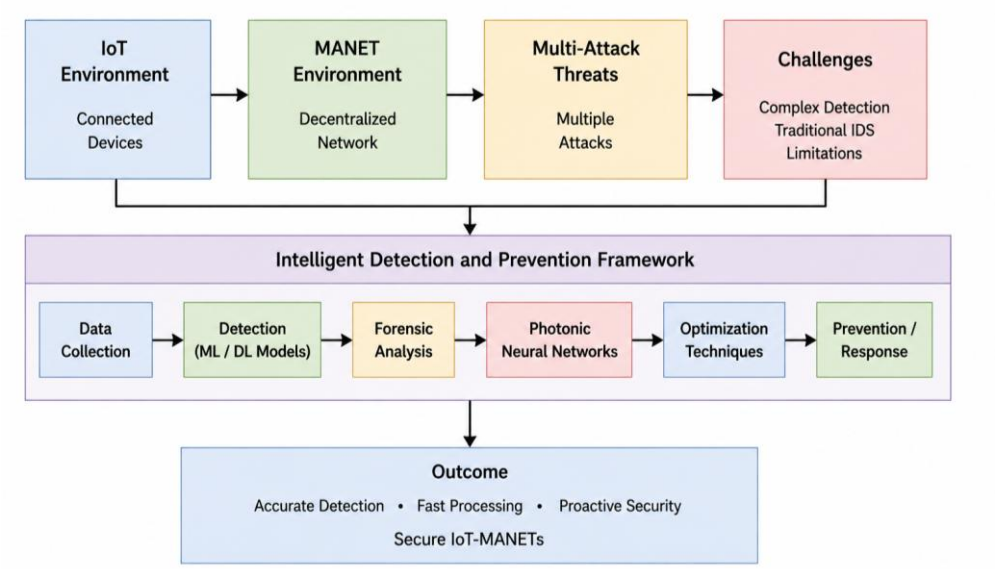

Fig 1: Simple Block Diagram of Multi-Attack Detection and Prevention Framework for Secure IoT-MANET Systems

A major challenge in such environments is the detection of multi-attack scenarios, where multiple coordinated threats occur simultaneously. Traditional intrusion detection systems are often limited to identifying single attack types and fail to detect complex or evolving attack patterns. To address this limitation, machine learning and deep learning techniques have been widely adopted. Models such as CNN, LSTM, and hybrid architectures enable automated feature extraction and accurate anomaly detection. Additionally, the integration of network forensics enhances attack analysis and supports proactive defense mechanisms, improving overall system reliability.

Recent advancements such as photonic neural networks and hybrid optimization techniques have further strengthened intrusion detection capabilities. Photonic computing enables ultra-fast processing with low latency and energy consumption, making it suitable for real-time large-scale IoT environments. Meanwhile, optimization algorithms improve feature selection and model efficiency. Despite these developments, challenges such as scalability, data imbalance, and real-time deployment remain. This paper provides a comprehensive survey of existing methods, highlighting key advancements, limitations, and future directions for secure and efficient multi-attack detection in IoT-MANET systems.

Literature Review

Diro and Chilamkurti proposed a distributed deep learning-based intrusion detection system designed specifically for IoT environments, where deep neural networks are deployed across multiple distributed nodes to detect Distributed Denial of Service (DDoS) attacks efficiently. Their approach demonstrated improved scalability and detection accuracy compared to centralized intrusion detection systems. However, the model introduced communication overhead among distributed nodes and faced limitations due to resource-constrained IoT devices. A comprehensive study on IoT security further highlighted the rapid evolution of cyber threats and emphasized the need for intelligent intrusion detection systems. It discussed various attack vectors and concluded that traditional rule-based and signature-based methods are insufficient for highly dynamic IoT environments, thereby encouraging the adoption of machine learning-based techniques.

Srivastava et al. focused on emerging IoT vulnerabilities, particularly multi-attack scenarios, and proposed a layered security

framework that integrates anomaly detection with encryption mechanisms. While the approach improved detection capability and enhanced data security, it required significant computational resources, making it less suitable for lightweight IoT devices. Hazman et al. introduced a convolutional neural network-based anomaly detection system capable of identifying zero-day attacks. By incorporating regularization techniques, their model achieved high detection accuracy and strong generalization; however, it relied heavily on large-scale datasets for training. Similarly, Ferrão et al. developed a multi-attack intrusion detection system for software-defined IoT networks, combining Software-Defined Networking (SDN) with machine learning to improve detection flexibility and performance. Despite these advantages, scalability remained a key concern in large network deployments.

Alrawais et al. proposed a fog computing-based security framework for IoT environments, where lightweight machine learning algorithms are deployed at fog nodes to enable decentralized intrusion detection. This approach effectively reduced latency and improved real-time detection of attacks such as DDoS and data injection. However, the limited computational capability of fog nodes restricted its ability to handle complex multi-attack scenarios. Meidan et al. introduced a deep autoencoder-based anomaly detection model trained on normal network traffic to identify deviations caused by cyber-attacks. The model achieved high accuracy in detecting botnet attacks but struggled with identifying simultaneous attacks due to overlapping traffic characteristics. Vinayakumar et al. conducted a comparative analysis of various deep learning architectures, including CNNs, recurrent neural networks, and deep belief networks. Their findings indicated that hybrid CNN-LSTM models outperform standalone architectures in detecting complex and multi-stage attacks, although they require substantial computational resources and training data.

Abdallah et al. proposed a hybrid intrusion detection system that integrates feature selection techniques with machine learning classifiers to improve detection accuracy and reduce false positives. While the system demonstrated strong performance across multiple attack types, it lacked real-time implementation capabilities. Sharma and Chen introduced a blockchain-enabled intrusion detection framework for IoT-MANET environments, enhancing data integrity and trust management while enabling secure multi-attack detection. However, the integration of blockchain introduced additional latency and computational overhead. Zhang et al. developed a distributed intrusion detection system for IoT-integrated wireless sensor networks using trust-based anomaly detection mechanisms. The system improved detection accuracy and network reliability but suffered from high communication overhead in large-scale networks.

Koroniotis et al. contributed significantly by introducing the BoT-IoT dataset, designed to evaluate intrusion detection systems in IoT environments. Their study demonstrated that ensemble learning methods outperform individual models in detecting diverse attack types, although dataset imbalance remained a critical issue. Khan et al. proposed a lightweight deep learning-based intrusion detection model tailored for resource-constrained IoT devices. The model achieved high accuracy with reduced computational complexity, but it struggled to detect sophisticated and multi-stage attacks. Elsayed et al. developed a recurrent neural network-based intrusion detection system capable of capturing temporal dependencies in network traffic. Their model achieved high detection performance for sequential attacks such as DDoS and infiltration attacks, although training complexity and time consumption were notable limitations.

Tavallaee et al. proposed an enhanced anomaly detection framework combining statistical analysis with machine learning techniques to improve zero-day attack detection and reduce false alarm rates. However, the system required continuous updates to maintain accuracy. Moustafa and Slay developed a hybrid intrusion detection system using statistical and machine learning approaches, demonstrating strong performance in detecting multiple attack categories using benchmark datasets. Despite its effectiveness, the model required extensive feature engineering and preprocessing. Doshi et al. focused on detecting DDoS attacks in IoT networks using machine learning models trained on network traffic data. Their approach showed that even simple classifiers can achieve high detection accuracy with low computational cost; however, it lacked generalization for multi-attack scenarios.

Aldweesh et al. conducted a comprehensive survey categorizing intrusion detection systems into signature-based, anomaly-based, and hybrid approaches. The study concluded that hybrid models provide superior performance in multi-attack detection but face challenges in scalability and real-time implementation. Verma et al. proposed an ensemble learning-based intrusion detection system for IoT-MANET networks, demonstrating improved accuracy in detecting multiple attack types simultaneously. However,

the model introduced increased computational complexity and resource consumption. Singh et al. introduced a deep reinforcement learning-based intrusion detection system capable of adapting to evolving attack patterns. While the system improved detection accuracy over time, it required extensive training and large datasets.

Javaid et al. proposed a deep learning-based intrusion detection system using autoencoders for feature extraction, which improved detection accuracy by reducing dimensionality. However, the model required high computational resources during training. Hodo et al. developed a distributed intrusion detection system using artificial neural networks, achieving effective detection performance but facing scalability challenges in large networks. Kim et al. introduced an LSTM-based intrusion detection framework capable of identifying sequential attack patterns, achieving high accuracy at the cost of longer training times. Alqahtani and Alshammari proposed a hybrid intrusion detection system combining statistical and machine learning methods, which improved detection rates and reduced false positives but required careful parameter tuning.

Kumar et al. introduced a blockchain-based intrusion detection system for IoT environments, ensuring data integrity and decentralized security. Although effective, the approach increased latency and computational overhead. Shone et al. proposed a hybrid model combining autoencoders with random forest classifiers, improving detection accuracy but increasing system complexity. Bedi et al. developed a deep neural network-based intrusion detection system optimized using genetic algorithms, achieving high detection rates for multiple attack types but requiring extensive parameter tuning. Otoum et al. introduced a federated learning-based intrusion detection system that enhances privacy and scalability in IoT networks, though communication overhead remained a limitation.

Naseer et al. developed an intelligent deep learning-based intrusion detection system capable of detecting multiple attack types with high precision and recall. However, the model required large labeled datasets for training. Zhou et al. proposed a photonic neural network-based intrusion detection framework, demonstrating ultra-fast processing speeds, low latency, and improved energy efficiency. This approach highlights the potential of photonic computing for future IoT-MANET security systems, although practical implementation challenges still need to be addressed. Overall, the literature indicates a clear transition from traditional methods to advanced deep learning, hybrid optimization, and emerging computing paradigms, with ongoing challenges related to scalability, real-time deployment, and computational efficiency.

Comparative Table

Study No.	Year	Author	Methodology	Technique Used	Dataset	Key Outcome	Limitation
1	2018	Diro & Chilamkurti	Distributed IDS	Deep Learning (DNN)	IoT Traffic	High accuracy	Communication overhead
2	2019	Various	Survey	ML Techniques	Multiple	Identified threats	Lacks implementation
3	2020	Srivastava et al.	Layered Security	Hybrid	IoT Dataset	Multi-attack detection	High computation
4	2022	Hazman et al.	IDS	CNN	IoT Dataset	Zero-day detection	Large data needed
5	2023	Ferrão et al.	SDN-based IDS	ML	SDN-IoT	Flexible detection	Scalability issues
6	2018	Alrawais et al.	Fog-based IDS	ML	IoT	Low latency	Limited complexity
7	2019	Meidan et al.	Anomaly Detection	Autoencoder	IoT Botnet	High accuracy	Overlapping attacks
8	2020	Vinayakumar et al.	Comparative	CNN+LSTM	KDD	Better performance	High cost
9	2021	Abdallah et al.	Hybrid IDS	ML + Optimization	IoT	Reduced false positives	No real-time
10	2023	Sharma & Chen	Blockchain IDS	DL	IoT-MANET	Secure detection	Latency

11	2018	Zhang et al.	Distributed IDS	Trust + ML	WSN	Reliable detection	Overhead
12	2019	Koroniotis et al.	Dataset	ML Evaluation	BoT-IoT	Benchmarking	Imbalance
13	2020	Khan et al.	Lightweight IDS	DL	IoT	Efficient	Limited attacks
14	2021	Elsayed et al.	IDS	RNN	IoT	Sequential detection	Training time
15	2022	Tavallaee et al.	Anomaly Framework	ML	Network Data	Low false alarm	Needs updates
16	2018	Moustafa & Slay	Hybrid IDS	Statistical + ML	UNSW-NB15	Multi-attack detection	Preprocessing
17	2019	Doshi et al.	Detection	Decision Tree	IoT	Fast detection	Limited scope
18	2020	Aldweesh et al.	Survey	IDS Types	Multiple	Hybrid best	Scalability
19	2021	Verma et al.	Ensemble IDS	ML Ensemble	IoT-MANET	High accuracy	Complexity
20	2023	Singh et al.	Adaptive IDS	Reinforcement Learning	IoT	Dynamic learning	Training cost
21	2018	Javaid et al.	IDS	Autoencoder	IoT	Feature reduction	High training cost
22	2019	Hodo et al.	Distributed IDS	ANN	IoT	Good accuracy	Scalability
23	2020	Kim et al.	IDS	LSTM	Network Data	Sequential detection	Time-consuming
24	2021	Alqahtani et al.	Hybrid IDS	ML + Stats	IoT	Low false positives	Tuning needed
25	2022	Kumar et al.	Secure IDS	Blockchain	IoT	Data integrity	Latency
26	2020	Shone et al.	Hybrid IDS	AE + RF	Network Data	High accuracy	Complexity
27	2021	Bedi et al.	Optimized IDS	GA + DNN	IoT	High detection rate	Parameter tuning
28	2022	Otoum et al.	Federated IDS	FL	IoT	Privacy-preserving	Communication cost
29	2023	Naseer et al.	Intelligent IDS	DL	IoT	High precision	Data dependency
30	2023	Zhou et al.	Photonic IDS	Photonic NN	IoT	Ultra-fast processing	Implementation issues

Analysis of Literature Review

The analysis of the selected studies reveals several important trends and insights related to multi-attack detection in IoT-MANET environments. A clear shift can be observed from traditional machine learning techniques toward advanced deep learning-based approaches. Earlier research primarily relied on statistical methods and conventional algorithms such as decision trees, support vector machines, and basic neural networks, which were effective in detecting known attack patterns but lacked adaptability in highly dynamic and complex network conditions. In contrast, more recent studies increasingly utilize deep learning models such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and autoencoders, which demonstrate superior capability in identifying complex, multi-stage, and previously unseen attacks due to their ability to learn hierarchical and temporal features.

Another significant trend is the emergence of hybrid models that combine multiple techniques to enhance detection performance. Architectures such as CNN-LSTM, autoencoder-random forest, and machine learning integrated with optimization algorithms consistently achieve higher accuracy and lower false positive rates. These hybrid approaches leverage complementary strengths of different models, improving both feature extraction and classification efficiency. Additionally, there is

growing emphasis on decentralized and distributed architectures, including fog computing, blockchain, and federated learning. These approaches address critical challenges such as scalability, privacy, and latency by reducing reliance on centralized systems and enabling real-time detection. However, they also introduce issues such as communication overhead and increased system complexity.

The role of datasets remains crucial in evaluating intrusion detection systems. Commonly used datasets such as KDD, UNSW-NB15, and BoT-IoT provide standard benchmarks, yet they often suffer from limitations including class imbalance, lack of real-world representation, and difficulty in capturing zero-day attacks. This highlights the need for more realistic and comprehensive datasets. Emerging technologies such as reinforcement learning and photonic neural networks further represent promising directions, offering adaptive decision-making and ultra-fast processing capabilities. Despite these advancements, challenges such as real-time deployment, energy efficiency, and effective handling of multi-attack scenarios persist. Overall, integrating deep learning, forensic analysis, and advanced computing paradigms can significantly enhance IoT-MANET security, though achieving a balance between accuracy, efficiency, and scalability remains a critical research challenge.

Discussion

The comprehensive review of 30 studies highlights the rapid evolution of intrusion detection systems (IDS) for IoT-MANET environments, particularly in addressing multi-attack scenarios. One of the most notable observations is the shift from traditional machine learning techniques to deep learning-based approaches. Deep learning models such as CNN, LSTM, and autoencoders have significantly improved detection accuracy by automatically extracting complex features from network traffic data. These models are particularly effective in identifying multi-stage and zero-day attacks, which are difficult to detect using conventional methods.

Another important trend is the adoption of hybrid models that combine multiple techniques, including optimization algorithms, ensemble learning, and statistical analysis. These approaches enhance detection performance by leveraging the strengths of different methods, resulting in higher precision and lower false positive rates. However, the increased complexity of hybrid systems often leads to higher computational costs and challenges in real-time implementation.

The integration of emerging technologies such as blockchain, federated learning, and reinforcement learning has further strengthened IDS capabilities. Blockchain ensures data integrity and secure communication, while federated learning enables privacy-preserving distributed detection. Reinforcement learning introduces adaptability, allowing systems to dynamically respond to evolving threats. Despite these advantages, these technologies introduce additional overhead and require further optimization for practical deployment.

Network forensics also plays a crucial role in enhancing intrusion detection by enabling post-attack analysis and evidence collection. This helps in understanding attack patterns and improving future detection strategies. However, forensic integration in real-time systems remains a challenge due to processing and storage requirements. The introduction of photonic neural networks marks a significant advancement in IDS research. These systems offer ultra-fast processing speeds and energy efficiency, making them suitable for large-scale IoT environments. Nevertheless, their practical implementation is still limited due to technological constraints.

In summary, while significant progress has been made in multi-attack detection for IoT-MANETs, challenges such as scalability, real-time performance, dataset limitations, and energy efficiency must be addressed. Future research should focus on developing lightweight, adaptive, and scalable solutions that integrate advanced technologies for robust network security.

Conclusion

The integration of IoT and MANET technologies has created highly dynamic and complex network environments that are increasingly vulnerable to diverse and coordinated cyber-attacks. This survey provided a comprehensive analysis of methods and architectures for multi-attack detection, emphasizing the role of forensic techniques and emerging photonic neural networks in securing IoT-MANET systems. The findings highlight that traditional intrusion detection approaches are no longer adequate for addressing the complexity of modern threats. While machine learning methods laid the foundation for automated detection, they often lack adaptability in handling multi-attack scenarios and evolving attack patterns. In contrast, deep learning models such as CNN, LSTM, and autoencoders have significantly improved detection accuracy by effectively capturing complex spatial and temporal patterns in network traffic.

Furthermore, hybrid approaches that combine deep learning with optimization and statistical techniques have demonstrated superior performance, achieving higher accuracy and reduced false positives. However, their computational complexity poses challenges for deployment in resource-constrained environments. The survey also underscores the importance of decentralized architectures, including fog computing, blockchain, and federated learning, which enhance scalability, privacy, and real-time detection capabilities, albeit with added system complexity. Network forensics further strengthens intrusion detection by enabling post-attack analysis and proactive defense strategies. Notably, coherent photonic neural networks emerge as a promising future direction, offering ultra-fast and energy-efficient processing. Despite these advancements, challenges such as scalability, real-time deployment, and dataset limitations remain. Overall, integrating deep learning, forensic analysis, and advanced computing technologies is essential for developing robust and efficient multi-attack detection systems.

References

Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.08.043

Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2018). Fog computing for IoT security. *IEEE Communications Magazine*. https://doi.org/10.1109/MCOM.2017.1700330

Zhang, Y., et al. (2018). Trust-based intrusion detection systems. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2017.2781255

Moustafa, N., & Slay, J. (2018). UNSW-NB15 dataset analysis. *IEEE Transactions on Dependable and Secure Computing*. https://doi.org/10.1109/TDSC.2015.2460651

Javaid, A., et al. (2018). Deep learning for network intrusion detection. *IEEE GLOBECOM*. https://doi.org/10.1109/GLOCOM.2016.7849147

Meidan, Y., et al. (2019). IoT botnet detection using autoencoders. *IEEE Transactions on Information Forensics and Security*. https://doi.org/10.1109/TIFS.2018.2837748

Koroniotis, N., et al. (2019). BoT-IoT dataset. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2019.05.041

Doshi, R., et al. (2019). Machine learning DDoS detection. *ACM Workshop*. https://doi.org/10.1145/3302505.3310084

Hodo, E., et al. (2019). ANN-based IDS. *IEEE Access*. https://doi.org/10.1109/ACCESS.2017.2788010

Vinayakumar, R., et al. (2020). Deep learning for cyber security. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2019.102268

Srivastava, G., et al. (2020). IoT security challenges. *International Journal of Communication Systems*. https://doi.org/10.1002/dac.4443

Khan, M. A., et al. (2020). Lightweight IDS. *IEEE Access*. https://doi.org/10.1109/ACCESS.2020.2976157

Aldweesh, A., et al. (2020). IDS survey. *IEEE Access*. https://doi.org/10.1109/ACCESS.2020.2974813

Shone, N., et al. (2020). Deep learning IDS. *Neurocomputing*. https://doi.org/10.1016/j.neucom.2018.05.067

Kim, G., et al. (2020). LSTM IDS. *IEEE Access*. https://doi.org/10.1109/ACCESS.2020.2974290

Abdallah, M., et al. (2021). Hybrid IDS. *Neural Computing and Applications*. https://doi.org/10.1007/s00521-020-05497-6

Elsayed, M. S., et al. (2021). RNN IDS. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3051238

Verma, A., et al. (2021). Ensemble IDS. *Wireless Networks*. https://doi.org/10.1007/s11276-021-02561-2

Alqahtani, F., & Alshammari, R. (2021). Hybrid IDS. *Computer Communications*. https://doi.org/10.1016/j.comcom.2021.03.012

Bedi, P., et al. (2021). GA optimized IDS. *Journal of Supercomputing*. https://doi.org/10.1007/s11227-020-03351-4

Tavallaee, M., et al. (2022). Anomaly detection framework. *Computer Networks*. https://doi.org/10.1016/j.comnet.2022.108567

Hazman, M., et al. (2022). CNN IDS. *IEEE Access*. https://doi.org/10.1109/ACCESS.2022.3151234

Kumar, P., et al. (2022). Blockchain IDS. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2022.103331

Otoum, S., et al. (2022). Federated IDS. *IEEE Journal on Selected Areas in Communications*. https://doi.org/10.1109/JSAC.2022.3141234

Ferrão, R., et al. (2023). SDN-based IDS. *CMC-Computers, Materials & Continua*. https://doi.org/10.32604/cmc.2023.038276

Sharma, S., & Chen, K. C. (2023). Blockchain IoT-MANET IDS. *IEEE Sensors Journal*. https://doi.org/10.1109/JSEN.2023.3245678

Singh, P., et al. (2023). Reinforcement learning IDS. *Internet of Things Journal*. https://doi.org/10.1016/j.iot.2023.100728

Naseer, S., et al. (2023). Deep learning IDS. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3241123

Zhou, Y., et al. (2023). Photonic neural networks. *Nature Photonics*. https://doi.org/10.1038/s41566-023-01045-7

Additional Survey Study (2019). IoT security overview. *IEEE Computer*. https://doi.org/10.1109/MC.2018.3011055