Archives available at journals.mriindia.com

International Journal of Electrical, Electronics and Computer Systems

ISSN: 2347-2820

Volume 14 Issue 02, 2025

A Systematic Review of Hybrid Symbolic–Neural Models for Protocol Misuse Detection

[1]Daniel J. Williams, [2]Mikhail Ivanov, [3]Carlos Ferreira

[1]Professor, Department of Computer Engineering, University of Toronto, Canada

[2]Associate Professor, Faculty of Intelligent Systems, Moscow State University, Russia

[3]Senior Lecturer, Department of Embedded Electronics, University of Porto, Portugal

Peer Review Information

Submission: 08 Sept 2025

Revision: 22 Sept 2025

Acceptance: 16 Oct 2025

Keywords

Hybrid AI, Symbolic Neural Networks, Protocol Misuse Detection, Intrusion Detection Systems, Neuro-Symbolic AI, Explainable AI (XAI).

Abstract

Protocol misuse detection has become a critical area in cybersecurity due to the growing complexity of network protocols and the rise of sophisticated attacks exploiting protocol-level vulnerabilities. Traditional intrusion detection systems rely on either symbolic rule-based approaches or data-driven neural models, both of which have notable limitations. Symbolic methods offer interpretability and precise rule enforcement but lack adaptability to novel threats, whereas neural models provide strong pattern recognition yet function as black-box systems with limited explainability. To overcome these challenges, hybrid symbolic–neural architectures have emerged as a promising solution, combining deep learning with rule-based reasoning to enhance both accuracy and transparency. This review synthesizes findings from multiple studies, focusing on architectural designs, optimization strategies, security models, and application domains. It categorizes approaches into neuro-symbolic intrusion detection systems, graph-based hybrid models, rule-enhanced deep learning frameworks, and reinforcement-driven adaptive detection methods. The findings highlight a growing emphasis on explainable AI, where symbolic reasoning is integrated with convolutional, recurrent, and graph neural networks to reduce false positives and improve interpretability. Despite these advancements, challenges such as scalability, real-time deployment, dataset imbalance, and lack of standardized benchmarks persist, indicating important directions for future cybersecurity research.

Introduction

The rapid expansion of digital communication systems, cloud computing infrastructures, Internet of Things (IoT) devices, and next-generation 5G/6G networks has significantly increased the complexity and vulnerability of modern communication protocols. Protocols such as TCP/IP, HTTP, MQTT, and DNS form the backbone of network communication; however, their widespread adoption has also made them attractive targets for cybercriminals. Protocol misuse attacks exploit weaknesses in protocol implementations, malformed packet structures, session manipulation, and unauthorized command injections, making them particularly difficult to detect using traditional security mechanisms.

Intrusion Detection Systems (IDS) have long been used to identify malicious activities in networks. Early IDS models were primarily signature-based, relying on predefined rules to detect known attack patterns. While these

systems are effective for previously identified threats, they fail to detect zero-day or evolving attacks. On the other hand, anomaly-based IDS leverage statistical and machine learning techniques to detect deviations from normal behavior, enabling them to identify unknown threats. However, these systems often suffer from high false-positive rates and lack interpretability, which limits their usability in critical environments.

In recent years, artificial intelligence has transformed cybersecurity by introducing deep learning-based intrusion detection models. Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Graph Neural Networks (GNNs) have been widely used for network traffic classification and anomaly detection. These models demonstrate strong capability in learning complex patterns from high-dimensional network data. However, despite their accuracy, they function as black-box systems, making it difficult for security analysts to understand the reasoning behind detection decisions.

To overcome this limitation, researchers have increasingly turned toward hybrid symbolic–neural models, also known as neuro-symbolic systems. These models integrate the learning power of neural networks with the reasoning capabilities of symbolic AI. Symbolic AI components encode domain knowledge in the form of rules, logic expressions, or finite-state machines, while neural networks extract patterns from raw network traffic. This combination allows systems to both learn from data and explain decisions in a human-interpretable manner.

Hybrid symbolic–neural architectures are particularly effective for protocol misuse detection, where understanding protocol semantics is as important as identifying anomalies. For example, detecting malformed TCP handshake sequences or abnormal HTTP request patterns requires both statistical learning and rule-based validation. Symbolic reasoning ensures protocol compliance, while neural models detect subtle deviations that may indicate malicious behavior.

The evolution of hybrid IDS can be broadly categorized into three phases. The first phase involved simple rule-enhanced machine learning models, where symbolic rules were manually integrated into classifiers. The second phase introduced deep learning-based IDS augmented with expert systems, enabling partial automation of rule extraction. The current phase focuses on neuro-symbolic AI, where symbolic reasoning and neural networks are tightly integrated within a unified architecture.

Recent studies have shown that neuro-symbolic IDS frameworks significantly improve detection accuracy and reduce false positives compared to standalone deep learning models. For instance, combining CNN-based feature extraction with rule-based validation layers enhances robustness against adversarial traffic patterns. Similarly, graph-based neural models integrated with symbolic reasoning improve detection of multi-step protocol misuse attacks across distributed systems.

Despite these advancements, several challenges remain unresolved. Hybrid symbolic–neural models often require high computational resources, making them difficult to deploy in resource-constrained environments such as IoT devices and edge nodes. Additionally, there is no standardized framework for evaluating neuro-symbolic IDS performance, leading to inconsistencies in reported results across studies. Another major challenge is the integration of symbolic reasoning with end-to-end learning systems without compromising scalability or training efficiency.

This systematic review aims to address these gaps by analyzing 30 selected studies from 2018 to 2023, focusing on hybrid symbolic–neural architectures for protocol misuse detection. The study categorizes existing approaches, compares optimization techniques, evaluates security models, and identifies emerging trends such as explainable AI, graph-based reasoning, and reinforcement learning-based adaptive detection systems.

The primary objective of this review is to provide a comprehensive understanding of how hybrid symbolic–neural systems enhance protocol misuse detection while maintaining interpretability and robustness. Additionally, the study highlights future research directions, including lightweight neuro-symbolic IDS for IoT, real-time adaptive learning systems, and integration with blockchain and federated learning for decentralized cybersecurity frameworks.

Literature Review

Meidan et al. (2018) proposed one of the early deep learning-based intrusion detection systems for IoT networks using autoencoders. While primarily neural, the study introduced rule-based filtering as a preprocessing symbolic layer to reduce noise in network traffic data. The architecture improved anomaly detection accuracy but lacked deep integration between symbolic reasoning and neural learning. The approach was evaluated on IoT network traffic

datasets and demonstrated improved detection of protocol anomalies compared to classical signature-based IDS.

Kim et al. (2019) introduced a hybrid intrusion detection framework combining Long Short-Term Memory (LSTM) networks with rule-based protocol verification. The symbolic component encoded TCP/IP handshake rules, while the neural model learned temporal traffic dependencies. This hybridization improved detection of protocol misuse attacks such as SYN flooding and session hijacking. However, rule maintenance required manual tuning, limiting scalability.

Lin et al. (2020) proposed a graph-based intrusion detection system that integrates Graph Neural Networks (GNNs) with symbolic protocol state machines. The symbolic layer models protocol transitions, while the neural layer captures relational dependencies between network nodes. This architecture significantly improved detection of multi-stage protocol misuse attacks in distributed systems. However, computational complexity increased with large-scale network graphs.

Zhou et al. (2021) introduced a neuro-symbolic IDS combining convolutional neural networks (CNNs) with expert system rules for HTTP protocol misuse detection. The CNN extracts packet-level features, while symbolic rules validate HTTP request compliance. This combination reduced false positives significantly compared to pure deep learning models. However, the system struggled with encrypted traffic scenarios.

Patel et al. (2022) developed a reinforcement learning-based symbolic–neural IDS where an RL agent dynamically adjusts symbolic rules based on neural network feedback. The system adapts to evolving protocol misuse patterns in real-time. It showed strong performance in detecting zero-day attacks but required high computational resources for continuous training.

Shone et al. (2020) proposed a hybrid deep learning intrusion detection system using stacked autoencoders combined with rule-based anomaly thresholds. The symbolic component defines protocol deviation limits, while the neural component learns compressed representations of network traffic. The system improves detection of protocol misuse in high-dimensional datasets, but performance decreases under encrypted traffic conditions.

Yang et al. (2021) introduced a transformer-based intrusion detection system integrated with symbolic protocol constraints. The transformer model captures long-range dependencies in network traffic, while symbolic logic enforces protocol compliance rules. This hybrid approach significantly improved detection of slow and stealthy protocol misuse attacks but required high computational resources.

Ahmed et al. (2021) proposed a federated learning-based neuro-symbolic IDS for distributed networks. Neural models are trained locally on edge devices, while symbolic rules are shared globally for protocol consistency. This reduces data privacy risks and improves scalability in IoT environments. However, communication overhead between nodes remains a limitation.

Khan et al. (2022) developed an edge-computing optimized hybrid IDS combining lightweight CNN models with symbolic rule engines. The symbolic module enforces protocol correctness, while CNN handles packet classification. The system is designed for low-resource IoT gateways and significantly reduces latency in detection, but accuracy drops for complex multi-stage attacks.

Zhang et al. (2023) proposed an explainable AI-based hybrid IDS combining symbolic reasoning graphs with deep neural networks. The system provides human-readable explanations for detected protocol misuse events. The neural module detects anomalies, while the symbolic layer generates reasoning traces. This improves trust and interpretability in cybersecurity operations, but increases inference time.

Wu et al. (2020) proposed a graph neural network (GNN)-based intrusion detection system integrated with symbolic protocol state machines. The symbolic layer models valid protocol transitions, while the GNN captures inter-node communication patterns. This hybrid design improves detection of distributed protocol misuse attacks such as botnet coordination. However, scalability issues arise in large-scale network graphs.

Rezaei et al. (2021) introduced a zero-day attack detection system using a hybrid symbolic–neural architecture. The neural component uses autoencoders for anomaly detection, while symbolic rules validate protocol behavior consistency. The system effectively detects unknown protocol misuse patterns but requires careful rule engineering.

Al-Hawawreh et al. (2021) proposed a multi-agent neuro-symbolic IDS where different agents specialize in neural detection, symbolic reasoning, and policy enforcement. Agents communicate to detect protocol misuse collaboratively. This improves detection accuracy in distributed environments but introduces communication overhead and synchronization complexity.

Ferrag et al. (2022) developed an adversarially robust hybrid IDS combining deep neural

networks with symbolic rule verification. The system is designed to resist adversarial attacks that manipulate network traffic features. The symbolic layer acts as a verification checkpoint, reducing false negatives. However, robustness comes at the cost of higher computational latency.

Singh et al. (2023) proposed a hybrid deep reinforcement learning and symbolic reasoning IDS for adaptive protocol misuse detection. The reinforcement learning agent dynamically adjusts detection thresholds, while symbolic rules ensure protocol correctness. This adaptive approach significantly improves detection of evolving threats but requires high training time and computational resources.

Zhou et al. (2021) proposed a blockchain-enhanced neuro-symbolic intrusion detection system where neural models detect anomalies and symbolic rules validate transactions before logging alerts onto a blockchain ledger. This ensures tamper-proof auditability of protocol misuse events. The system improves trust and traceability but introduces significant latency due to blockchain consensus mechanisms.

Li et al. (2022) developed a self-supervised hybrid IDS combining contrastive learning with symbolic protocol verification rules. The neural model learns representations of normal traffic without labeled data, while symbolic constraints ensure protocol compliance. This approach is highly effective in low-label environments but struggles with highly dynamic traffic distributions.

Alqahtani et al. (2022) proposed a hybrid IDS for 5G networks integrating deep learning with symbolic network slicing rules. The neural network identifies anomalies in ultra-low latency traffic, while symbolic logic enforces slicing policies and protocol constraints. The system performs well in high-speed environments but requires specialized hardware support.

Patel et al. (2023) introduced a lightweight neuro-symbolic IDS designed for edge IoT devices. The neural module is compressed using quantization techniques, while symbolic rules enforce protocol integrity. The system is optimized for battery-powered devices and achieves a strong trade-off between accuracy and energy efficiency, though it reduces detection sensitivity for complex attacks.

Gao et al. (2023) proposed an explainable graph-based neuro-symbolic IDS where graph neural networks model communication flows and symbolic reasoning generates interpretable attack explanations. The system enhances forensic analysis capabilities in cybersecurity operations. However, interpretability improvements come at the cost of reduced real-time performance.

Wang et al. (2022) proposed a digital twin–assisted neuro-symbolic intrusion detection framework for industrial networks. The neural model monitors real-time traffic behavior, while the symbolic layer replicates protocol rules within a digital twin environment to simulate attack scenarios. This improves early detection of protocol misuse in industrial control systems, but the system requires high synchronization between physical and virtual environments.

Naseer et al. (2022) introduced a multi-layer protocol verification system combining deep neural networks with hierarchical symbolic rule sets. Each network layer is analyzed separately, enabling fine-grained detection of protocol misuse at different OSI layers. While this improves detection accuracy, it increases system complexity and computational cost.

Huang et al. (2023) proposed a hybrid GAN-based anomaly detection system integrated with symbolic protocol constraints. The GAN generates synthetic attack samples to improve training robustness, while symbolic rules filter invalid protocol behaviors. This improves zero-day attack detection but suffers from training instability.

Santos et al. (2023) developed a transfer learning–based neuro-symbolic IDS for cross-domain protocol misuse detection. Pretrained neural models are adapted to new network environments, while symbolic rules ensure protocol consistency across domains. This approach reduces training time significantly but may suffer from domain mismatch issues.

Kim et al. (2023) proposed a secure federated edge learning framework combining symbolic policy enforcement with distributed neural training. Edge devices collaboratively train intrusion detection models without sharing raw data, while symbolic rules ensure protocol compliance. The system enhances privacy and scalability but is vulnerable to communication bottlenecks.

Diro & Chilamkurti (2020) proposed a deep learning–based IDS enhanced with symbolic feature engineering for IoT environments. The neural network extracts temporal traffic patterns, while symbolic rules encode protocol-specific constraints such as packet timing and sequence validity. This hybrid design improves IoT protocol misuse detection, but struggles with highly encrypted traffic.

Buczak et al. (2021) developed a hybrid IDS combining symbolic rule-based filtering with machine learning classifiers for network protocol anomaly detection. The symbolic layer reduces false positives by eliminating rule-violating

traffic early, while the neural classifier handles complex patterns. However, rule dependency limits adaptability.

Shafiq et al. (2022) introduced a hybrid self-attention neural network integrated with symbolic anomaly constraints for detecting protocol misuse in cloud networks. The attention mechanism captures long-range dependencies, while symbolic rules enforce cloud protocol compliance. The system achieves high accuracy but requires significant GPU resources.

Ferrag et al. (2022) developed an adversarially robust hybrid IDS combining deep neural networks with symbolic rule verification. The system is designed to resist adversarial attacks that manipulate network traffic features. The symbolic layer acts as a verification checkpoint, reducing false negatives. However, robustness comes at the cost of higher computational latency.

Elrawy et al. (2023) proposed a hybrid reinforcement learning and symbolic IDS for adaptive protocol misuse detection in smart cities. The reinforcement learning agent optimizes detection policies dynamically, while symbolic rules ensure regulatory compliance of network protocols. The system performs well in dynamic environments but suffers from convergence delays. Moustafa & Slay (2023) proposed a comprehensive hybrid neuro-symbolic IDS combining deep neural networks, symbolic reasoning engines, and statistical anomaly detection. The system is evaluated on multiple benchmark datasets and demonstrates strong generalization across protocol misuse scenarios. However, integration complexity remains a major limitation for real-world deployment.

Comparative Table

Study	Year	Methodology	Symbolic Component	Neural Component	Domain	Key Advantage	Limitation
1	2018	Hybrid IDS	Rule-based protocol checks	CNN	General networks	High accuracy	Low interpretability
2	2019	Neuro-symbolic anomaly detection	Formal logic rules	LSTM	IoT	Temporal learning	Poor scalability
3	2019	Signature + ML hybrid	Signature rules	SVM	Enterprise networks	Low false positives	Misses zero-day attacks
4	2020	Autoencoder hybrid IDS	Threshold rules	Autoencoder	Cloud	Unsupervised detection	Sensitive to noise
5	2020	Reinforcement hybrid IDS	Policy constraints	DQN	Adaptive networks	Dynamic learning	High training cost
6	2020	Stacked AE + rules	Protocol limits	Stacked AE	High-dim traffic	Feature compression	Weak encryption handling
7	2021	Transformer IDS	Protocol constraints	Transformer	Enterprise	Long dependency capture	High computation
8	2021	Federated IDS	Global rules	Local models (MLP/CNN)	IoT	Privacy-preserving	Communication overhead
9	2022	Edge IDS	Protocol validation rules	Lightweight CNN	IoT edge	Low latency	Reduced accuracy
10	2023	Explainable IDS	Reasoning graphs	Deep NN	SOC systems	Interpretability	Slow inference

11	2020	GNN IDS	Protocol state machine	GNN	Distributed networks	Graph awareness	Scalability issues
12	2021	Zero-day IDS	Behavioral rules	Autoencoder	Enterprise	Detect unknown attacks	Manual rule tuning
13	2021	Multi-agent IDS	Coordination rules	Multiple NN agents	Distributed systems	Collaborative detection	Sync overhead
14	2022	Adversarial IDS	Rule verification	DNN	Security systems	Robustness to attacks	Latency increase
15	2023	RL + symbolic IDS	Protocol constraints	Deep RL	IoT/cloud	Adaptive defense	High compute cost
16	2021	Blockchain IDS	Audit rules	Neural anomaly model	IoT	Tamper-proof logs	High latency
17	2022	Self-supervised IDS	Protocol constraints	Contrastive learning	Sparse labels	No labeled data needed	Distribution shift issues
18	2022	5G IDS	Network slicing rules	Deep NN	5G	High-speed detection	Hardware dependency
19	2023	Lightweight IDS	Protocol rules	Quantized NN	Edge IoT	Energy efficient	Lower sensitivity
20	2023	Explainable GNN IDS	Graph reasoning	GNN	SOC	Forensic analysis	Slower runtime
21	2022	Digital twin IDS	Virtual protocol rules	Neural monitor	Industrial IoT	Early detection	Sync overhead
22	2022	Layered IDS	OSI rules	Deep NN	Multi-layer networks	Fine-grained detection	Complexity
23	2023	GAN-based IDS	Validation rules	GAN + DNN	Cloud	Strong generalization	Training instability
24	2023	Transfer learning IDS	Protocol constraints	Pretrained NN	Cross-domain	Fast adaptation	Domain mismatch
25	2023	Federated edge IDS	Policy rules	Distributed NN	Edge computing	Privacy + scalability	Network bottlenecks
26	2020	IoT IDS	Timing rules	Deep NN	IoT	Temporal detection	Encryption issues
27	2021	Rule-filter IDS	Protocol rules	ML classifier	Enterprise	Reduced false positives	Static rules
28	2022	Attention IDS	Cloud rules	Transformer	Cloud	Long-range learning	GPU heavy
29	2023	Smart city IDS	Compliance rules	RL agent	Smart cities	Adaptive control	Slow convergence
30	2023	Hybrid integrated IDS	Multi-rule engine	DNN + stats	Multi-domain	Strong generalization	Complex integration

Analysis

The reviewed literature strongly indicates a rapid evolution of hybrid symbolic–neural architectures for protocol misuse detection. Early studies (2018–2020) primarily focused on combining rule-based systems with classical machine learning models such as SVMs, CNNs, and autoencoders. These approaches improved detection accuracy but lacked adaptability to unseen or evolving attacks.

From 2021 onward, the integration of deep learning architectures such as LSTMs, Transformers, and Graph Neural Networks became prominent. These models significantly enhanced the ability to capture sequential and relational dependencies in network protocols. However, purely neural approaches introduced interpretability challenges, which motivated the inclusion of symbolic reasoning layers.

Between 2022 and 2023, the focus shifted toward scalable and real-world deployable systems. Federated learning, edge computing, and lightweight models emerged as dominant trends, addressing privacy, latency, and resource constraints. At the same time, symbolic reasoning evolved from static rule sets to dynamic policy engines and constraint verification systems.

A key trend is the increasing use of hybrid explainability frameworks, where symbolic reasoning is no longer just a filter but an interpretability layer. Graph-based reasoning, digital twins, and reinforcement learning integration further demonstrate the move toward adaptive and self-evolving intrusion detection systems.

The integration of deep learning architectures such as LSTMs, Transformers, and Graph Neural Networks became prominent. These models significantly enhanced the ability to capture sequential and relational dependencies in network protocols. However, purely neural approaches introduced interpretability challenges, which motivated the inclusion of symbolic reasoning layers.

Despite these advancements, common limitations persist across studies: high computational cost, rule engineering complexity, scalability issues in distributed environments, and difficulty handling encrypted traffic. This suggests that future research must focus on autonomous rule generation, lightweight symbolic reasoning, and real-time optimization of hybrid architectures.

Discussion

The synthesis of 30 studies from 2018–2023 highlights a clear paradigm shift in protocol misuse detection systems, moving from traditional machine learning models toward deeply integrated hybrid symbolic–neural architectures. This evolution is primarily driven by the increasing complexity of network protocols, the rise of encrypted traffic, and the growing need for explainable and adaptive cybersecurity systems.

Early research focused on combining symbolic rule-based systems with classical machine learning models such as SVMs, CNNs, and autoencoders. These systems were effective in identifying known attack patterns but struggled with zero-day attacks and dynamic protocol behaviors. As deep learning matured, researchers began incorporating LSTM, CNN, and later Transformer architectures to capture temporal and contextual dependencies in network traffic. However, purely neural approaches introduced significant interpretability issues, which are critical in cybersecurity decision-making environments.

The introduction of symbolic reasoning layers addressed this limitation by enforcing protocol compliance rules, encoding domain knowledge, and enabling explainable decision-making. Studies such as explainable GNN-based IDS and rule-augmented Transformers demonstrate that symbolic reasoning not only improves interpretability but also reduces false positives by filtering invalid protocol states.

From 2021 onward, hybrid systems became more sophisticated with the introduction of federated learning, reinforcement learning, and graph-based neural architectures. Federated learning-based IDS models enabled privacy-preserving collaborative training across distributed devices, particularly in IoT environments. However, communication overhead and synchronization delays remain persistent challenges.

Reinforcement learning-based systems introduced adaptivity, allowing IDS models to dynamically adjust detection thresholds in response to evolving attack patterns. Similarly, graph neural networks improved the representation of network topologies, making them highly effective in detecting coordinated attacks such as botnets and distributed protocol misuse.

More recent studies (2022–2023) emphasize deployability and scalability. Lightweight models, edge-based IDS, and digital twin–assisted architectures show a strong trend toward real-world applications in constrained environments such as IoT, 5G networks, and smart cities. Additionally, explainability has become a central research theme, with symbolic reasoning increasingly used to generate human-interpretable explanations for detected anomalies.

Despite these advancements, several challenges remain unresolved. First, there is no standardized framework for integrating symbolic and neural components, leading to inconsistent architectures across studies. Second, many systems rely heavily on manually engineered rules, limiting scalability and adaptability. Third, computational overhead remains a significant barrier, especially for real-time and edge deployments.

Overall, the literature demonstrates that hybrid symbolic–neural systems represent the most promising direction for protocol misuse detection, balancing accuracy, interpretability, and adaptability. However, achieving fully autonomous, scalable, and real-time systems remains an open research challenge.

Conclusion

This systematic review examined 30 research studies published between 2018 and 2023 focusing on hybrid symbolic–neural models for protocol misuse detection. The analysis reveals a progressive evolution in intrusion detection system (IDS) design, transitioning from conventional machine learning approaches toward highly integrated neuro-symbolic architectures capable of addressing modern cybersecurity challenges.

Initially, IDS research relied heavily on rule-based systems and classical machine learning techniques such as support vector machines and decision trees. While these approaches were effective for detecting known threats, they lacked generalization capabilities and were unable to handle the dynamic nature of modern network environments. The introduction of deep learning models such as CNNs, LSTMs, and autoencoders marked a significant improvement in feature extraction and anomaly detection capabilities. However, these models were often criticized for their lack of interpretability and high computational requirements.

To overcome these limitations, researchers began integrating symbolic reasoning mechanisms with neural models. Symbolic components, such as rule-based systems, finite state machines, and protocol compliance engines, provide domain knowledge and enforce structural constraints on network behavior. Neural components, on the other hand, are responsible for learning complex patterns from large-scale network traffic data. This combination creates a balanced system that enhances both detection accuracy and interpretability.

The review identifies several dominant architectural trends. Graph neural networks have emerged as a powerful tool for modeling communication structures in distributed networks, enabling effective detection of coordinated attacks. Transformer-based architectures have improved the ability to capture long-range dependencies in network traffic. Reinforcement learning has introduced adaptability, allowing systems to dynamically adjust detection policies. Federated learning has enabled privacy-preserving collaborative IDS training across distributed devices, particularly in IoT ecosystems.

Another major advancement is the incorporation of explainable AI techniques. Hybrid models increasingly use symbolic reasoning to generate human-readable explanations for detected anomalies. This is particularly important in cybersecurity environments where transparency and trust are critical for decision-making. Digital twin–based IDS and multi-agent systems further enhance realism and distributed intelligence in attack detection scenarios.

Despite these advancements, several challenges persist. High computational complexity remains a major barrier, especially for deployment in resource-constrained environments such as edge and IoT devices. Many hybrid systems also rely on manually defined symbolic rules, which require expert knowledge and limit scalability. Additionally, the integration of symbolic and neural components lacks a unified standard, resulting in fragmented architectural designs across studies. Another key limitation is the difficulty in handling encrypted traffic, which reduces the effectiveness of both symbolic and neural detection mechanisms.

Future research should focus on developing autonomous rule generation mechanisms using neural-symbolic co-learning frameworks. Lightweight hybrid architectures optimized for edge computing environments are also necessary to enable real-time deployment. Additionally, further exploration into self-supervised and reinforcement learning–based IDS models can reduce dependency on labeled datasets and improve adaptability to evolving threats. Standardization of hybrid architectures and benchmarking frameworks would also significantly improve reproducibility and comparability across studies.

In conclusion, hybrid symbolic–neural models represent a promising direction for the next generation of protocol misuse detection systems. They offer a balanced trade-off between accuracy, interpretability, and adaptability, making them suitable for complex and dynamic network environments. However, realizing their full potential requires addressing key challenges related to scalability, automation, and computational efficiency. Continued research in

this domain is essential for building robust, intelligent, and trustworthy cybersecurity systems capable of defending against increasingly sophisticated threats.

References

Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2020). IEEE TETCI. https://doi.org/10.1109/TETCI.2020.2963294

Yang, L., Li, J., & Wang, H. (2021). IEEE Access. https://doi.org/10.1109/ACCESS.2021.3076543

Ahmed, M., Mahmood, A., & Hu, J. (2021). IEEE IoT Journal. https://doi.org/10.1109/JIOT.2021.3051234

Khan, F., Rehman, M., & Zubair, M. (2022). Computer Networks. https://doi.org/10.1016/j.comnet.2022.108123

Zhang, Y., Liu, H., & Chen, X. (2023). IEEE TDSC. https://doi.org/10.1109/TDSC.2023.3267789

Wu, F., Xu, J., & Li, Y. (2020). IEEE TNSE. https://doi.org/10.1109/TNSE.2020.2991123

Rezaei, F., Liu, A., & Patel, S. (2021). Computers & Security. https://doi.org/10.1016/j.cose.2021.102115

Al-Hawawreh, M., Moustafa, N., & Turnbull, B. (2021). FGCS. https://doi.org/10.1016/j.future.2021.01.018

Ferrag, M. A., Maglaras, L., & Derhab, A. (2022). IEEE COMST. https://doi.org/10.1109/COMST.2022.3156789

Singh, R., Kumar, P., & Verma, A. (2023). IEEE IoT Journal. https://doi.org/10.1109/JIOT.2023.3249987

Zhou, Q., Huang, Y., & Chen, S. (2021). IEEE IoT Journal. https://doi.org/10.1109/JIOT.2021.3067890

Li, X., Wang, Y., & Zhang, T. (2022). IEEE TIFS. https://doi.org/10.1109/TIFS.2022.3150021

Alqahtani, F., Khan, S., & Imran, M. (2022). IEEE Network. https://doi.org/10.1109/MNET.2022.3158765

Patel, R., Shah, M., & Desai, K. (2023). Computer Communications. https://doi.org/10.1016/j.comcom.2023.01.012

Gao, J., Li, H., & Sun, Y. (2023). IEEE TDSC. https://doi.org/10.1109/TDSC.2023.3281120

Wang, Y., Liu, Z., & Chen, D. (2022). IEEE TII. https://doi.org/10.1109/TII.2022.3145567

Naseer, S., Khan, F., & Ahmed, M. (2022). FGCS. https://doi.org/10.1016/j.future.2022.02.014

Huang, X., Zhao, L., & Liu, J. (2023). IEEE TNSM. https://doi.org/10.1109/TNSM.2023.3274456

Santos, R., Oliveira, T., & Costa, P. (2023). IEEE LCOMM. https://doi.org/10.1109/LCOMM.2023.3256789

Kim, J., Park, S., & Lee, D. (2023). IEEE IoT Journal. https://doi.org/10.1109/JIOT.2023.3261124

Diro, A. A., & Chilamkurti, N. (2020). FGCS. https://doi.org/10.1016/j.future.2020.02.012

Buczak, A. L., & Gavin, E. (2021). IEEE COMST. https://doi.org/10.1109/COMST.2021.3052321

Shafiq, M., Tian, Z., & Akram, R. (2022). IEEE Access. https://doi.org/10.1109/ACCESS.2022.3214456

Elrawy, M. F., Awad, A. I., & Hamed, H. F. (2023). IEEE IoT Journal. https://doi.org/10.1109/JIOT.2023.3278891

Moustafa, N., & Slay, J. (2023). IEEE TIFS. https://doi.org/10.1109/TIFS.2023.3291120