Indiana Journal of Multidisciplinary Research
Abbreviated Tittle- Ind J Multi Res
ISSN *(Online)*- 2583-3820
Journal Homepage Link- https://indianapublications.com/Journals/IJMR
DOI: https://doi.org/10.5281/zenodo.21602117

INDIANA PUBLICATIONS
PRODUCTIVE AND QUALITY RESEARCH

Review Article

Volume-06|Issue-04|2026

Deep Reinforcement Learning-based Holistic Cybersecurity System: A Comprehensive Survey and Proposed Architecture

Aiman Sabah[1], Dr. Niharika Prasanna[2], Honnu Shree B. L.[3], Chethan B. L.[4], Chandrakanth S. Devanagaon and Balaji V. N.[6]

[1,3,4,5,6]UG Student, Information Science and Engineering, RV Institute of Technology and Management (RVITM), Bangalore, Karnataka, India.
[2]Associate Professor, Information Science and Engineering, RV Institute of Technology and Management (RVITM), Bangalore, Karnataka, India.

Article History
Received: 05.05.2026
Accepted: 22.06.2026
Published: 25.07.2026

Citation
Sabah, A., Prasanna, N., Shree, H. B. L., Chethan, B. L., Devanagaon, C. S., Balaji, V. N. (2026). Deep Reinforcement Learning-based Holistic Cybersecurity System: A Comprehensive Survey and Proposed Architecture. *Indiana Journal of Multidisciplinary Research, 6*(4), 198-207.

Abstract: With traditional defenses against adversarial and zero-day attacks proving insufficient, AI- and ML-enabled tools provide real-time, adaptive, and autonomous protection for servers, networks, and personal computing systems. This review presents intrusion detection systems (IDS), integrated malware and antivirus solutions, web application firewalls (WAF), and cyber defense mechanisms based on distributed learning, considering their applicability across IoT, mobile, and general-purpose computing environments. These approaches include supervised learning, deep learning, federated learning, AutoML, and hybrid AI techniques. While deep neural networks and federated learning have demonstrated significant benefits, challenges related to data non-uniformity, energy efficiency, and explainability remain unresolved. The study anticipates that layered, energy-aware, explainable, and autonomous cybersecurity systems integrating IDS, antivirus, and WAF technologies will address current gaps in adaptive and proactive cybersecurity.

Keywords: Cybersecurity · Deep Reinforcement Learning · Intrusion Detection · Federated Learning · Explainable AI

INTRODUCTION

Cybersecurity has become a crucial component of modern computing, particularly given the increasing sophistication of cyberattacks targeting personal computers, enterprise servers, and organizational networks across various industries [14,28]. Although IoT security has received significant research attention, there is an equally pressing need to focus on autonomous cybersecurity for non-IoT systems such as personal computers, data centers, and enterprise infrastructure, where the consequences of security breaches are often far more severe [30].

Recent advances in Artificial Intelligence (AI) have enabled the development of self-learning and adaptive security systems capable of detecting, preventing, and mitigating cyber threats with minimal human intervention [19,46]. These systems employ Machine Learning (ML) and Deep Learning (DL) techniques that have demonstrated high effectiveness in intrusion detection, malware classification, and real-time cyber threat detection [23,20,39]. Hybrid AI approaches combine rule-based reasoning with data-driven models, providing a balanced trade-off between explainability and adaptability [16,47].

Federated Learning (FL) has emerged as a privacy-preserving training paradigm that enables collaborative model training without sharing sensitive raw data across participating networks [40,31]. AutoML techniques further simplify the design and optimization of ML pipelines, streamlining cybersecurity deployment [38]. The integration of FL and AutoML can facilitate autonomous cybersecurity systems capable of delivering end-to-end, multi-layered defense through components such as Intrusion Detection and Prevention Systems (IDPS), antivirus software, malware detection engines, and Web Application Firewalls (WAF) [42,29].

Despite these advancements, several challenges remain in achieving fully autonomous and adaptive protection across heterogeneous computing environments. These include optimizing detection accuracy while efficiently utilizing computational resources, defending against adversarial attacks, and ensuring interoperability among different security modules [41,44,12].

This study presents a structured literature survey that classifies contemporary research into four major domains: intrusion detection systems, antivirus technologies, malware defense mechanisms, and Web Application Firewalls. By synthesizing existing knowledge and methodologies, this work aims to identify

***Corresponding Author:** Niharika Prasanna

research gaps and contribute toward the development of a unified and intelligent cybersecurity ecosystem for non-IoT systems [45,27].

BACKGROUND AND TERMINOLOGY

1. **Zero-day attacks** – Exploits that target previously unknown vulnerabilities for which no patches or signatures exist, posing significant security risks due to the absence of prior protection mechanisms.
2. **Autonomous cybersecurity** – AI-powered tools and systems capable of detecting, assessing, and responding to cyber threats in real time with little or no human intervention.
3. **IDS/IPS (NIDS, HIDS)** – Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) monitor and identify malicious activities within computer systems and networks. Network-based IDS (NIDS) analyzes network traffic, whereas Host-based IDS (HIDS) examines host-level evidence such as logs, files, and system calls.
4. **Malware detection pipeline (static, dynamic, hybrid)** – Static detection analyzes executable files and source code without execution; dynamic detection observes malware behavior during runtime; hybrid approaches combine both techniques to improve detection accuracy.
5. **Federated Learning, AutoML, Hybrid AI** – Federated Learning enables collaborative model training across distributed nodes without sharing raw data. AutoML automates model development and optimization, while Hybrid AI combines multiple AI paradigms, such as symbolic reasoning and machine learning, to improve performance.
6. **Antivirus vs. EDR** – Traditional antivirus software primarily relies on signature-based scanning and heuristic detection to identify known malware, whereas Endpoint Detection and Response (EDR) provides continuous monitoring, threat hunting, behavioral analysis, and incident response capabilities.

LITERATURE CATEGORISATION AND ANALYSIS

Autonomous Intrusion Detection and Prevention Systems (NIDS/NIDPS)

Recent developments in Network Intrusion Detection and Prevention Systems (NIDPS) indicate a transition from traditional signature-based defenses toward adaptive AI-driven solutions capable of providing real-time protection. Hybrid approaches combine conventional Machine Learning algorithms, including Decision Trees, Random Forests, and Gradient Boosting, with deep learning models such as Deep Neural Networks (DNN) and ConvLSTM architectures. These models are trained using carefully preprocessed datasets involving duplicate removal, outlier elimination, feature scaling, Principal Component Analysis (PCA), and class balancing.

Studies conducted by Toyin *et al.* [40], Patil *et al.* [31], Shanthi *et al.* [38], and Vadisetty *et al.* [42] report detection accuracies exceeding **94.66%**, demonstrating the effectiveness of hybrid AI approaches for intrusion detection.

Emerging research directions include transformer-based intrusion detection systems, adversarially robust learning frameworks, and Federated Learning-based intrusion detection architectures that enable proactive, scalable, and intelligent cyber defense suitable for modern computing environments.

Malware and Antivirus Systems Using AI

Research in malware detection has evolved from traditional signature-based techniques toward data-driven and behavior-based detection approaches. Modern systems employ CNN-DNN hybrid architectures, attention mechanisms, opcode sequence analysis, and hybrid static-dynamic malware analysis to improve detection accuracy.

Commercial solutions such as **Singularity AV** [22] combine behavioral indicators with conventional antivirus techniques, while **CyberCure** [25] integrates machine learning-based detection with signature scanning. Explainable AI (XAI)-based antivirus systems have reported detection accuracies exceeding **98.5%**, improving both transparency and user trust.

Recent advancements include Android malware detection using CNN-DNN models [18], opcode-based malware detection through LSTM-TCN architectures [20], image-based IoT malware detection [21], Self-Paced Class Incremental Learning (SPCIL) [17] for adaptive malware defense, and federated learning-based smart datasets [16]. Additional research on adversarial robustness [12,19] and supervised contrastive learning [36] has further enhanced malware detection capabilities.

Although many of these techniques have primarily been developed for mobile and IoT environments, their underlying methodologies can be extended to enterprise computing platforms by adapting them to x86 and ARM architectures commonly deployed in organizational infrastructures.

Federated and Distributed Learning-Based Cyber Defenses

Federated Learning (FL) and Distributed Learning have emerged as promising paradigms for building scalable, privacy-preserving, and intelligent cyber defense systems. Unlike traditional centralized machine learning approaches that require transferring raw data to a central server, Federated Learning enables collaborative model training across multiple distributed nodes—including IoT devices, enterprise servers, and security gateways—while ensuring that sensitive local data never leaves the originating device [21,4]. Consequently, FL inherently enhances privacy, reduces the risk of data breaches

***Corresponding Author:** Niharika Prasanna

during transmission, and supports compliance with regulatory frameworks such as GDPR and HIPAA.

From a practical perspective, FL architectures are particularly well suited for large-scale and heterogeneous computing environments where participating devices differ significantly in computational capabilities, communication bandwidth, and local data distributions. Ullah and Srivastava [17] emphasize that the adaptability of FL enables cybersecurity systems to scale efficiently from resource-constrained IoT networks to high-throughput enterprise infrastructures. Yang *et al.* [4] further demonstrate that integrating AutoML with FL automates hyperparameter optimization, feature selection, and neural architecture design, thereby accelerating deployment in complex real-time cybersecurity environments.

Despite these advantages, several limitations remain. Federated Learning systems remain vulnerable to adversarial threats such as model poisoning and backdoor attacks. Additionally, non-identically distributed (non-IID) data across participating devices can introduce model bias, while communication and computational overhead may limit applicability in time-critical tasks such as intrusion detection and malware prevention [21].

Although current FL implementations primarily target IoT security applications, similar architectures can be effectively adapted for enterprise environments. For example, geographically distributed branch offices can collaboratively train cybersecurity models without exposing sensitive internal telemetry to external aggregators, thereby enabling unified threat intelligence while preserving local data privacy.

Web Application Firewalls and API Security

In [43], Wu *et al.* developed **WAFBooster**, which constructs a CNN-based shadow model of the target WAF and employs an RNN generator to craft adversarial payloads. An edit-distance payload corrector ensures payload validity, while a signature producer clusters high-impact substrings to derive simplified regular expressions (regex). Across eight WAFs, WAFBooster increased the true rejection rate of mutated payloads from **21% to 96%**, while maintaining **zero false rejections**.

In [26], a multi-task Seq2Seq translation framework exploits semantic similarities among different injection attack types, combined with surrogate classifiers and an evolutionary algorithm. This approach uncovers up to **5.78×** more WAF bypasses than grammar-based fuzzers.

In [32], an automated, data-driven approach to HTTP request tokenization using TF-IDF and One-Class SVM significantly improves detection rates while reducing false positives compared with conventional rule-based WAFs.

In [11], Dawadi *et al.* proposed a two-stage LSTM-based WAF that first filters volumetric HTTP flood DDoS attacks and then classifies XSS and SQL injection (SQLi) payloads. The system achieved an accuracy of **97.6%** for DDoS detection and **89.3%** for XSS/SQLi detection under high request rates.

In [36], Scano *et al.* applied machine learning to optimize **OWASP CRS** rule weights, improving true-positive rates by approximately **45%** at a **1% false-positive rate**, while simultaneously pruning **30%** of the rules without compromising performance.

AI-Powered Cybersecurity Agents and Decision Systems

The AI-driven cybersecurity domain is rapidly advancing toward fully autonomous defense agents capable of independently detecting, analyzing, and responding to cyber threats within seconds [31,42]. Hybrid AI models that integrate supervised learning, unsupervised learning, and reinforcement learning are widely explored, enabling adaptability to zero-day threats while achieving an optimal balance between precision and recall [39,38].

Human-in-the-loop simulation architectures combine human oversight with autonomous decision-making, enabling validation in simulated environments before operational deployment [20,16]. This capability is particularly critical in high-safety domains such as aerospace, where low latency and adaptability are essential [31].

Cross-layer intelligence aggregates information from multiple network layers, enabling the detection of complex, multi-stage attacks that isolated security systems may fail to identify [38,29]. Adaptive online learning enables cybersecurity agents to handle concept drift and maintain high detection accuracy over time [39,40].

Reinforcement learning is increasingly employed to optimize intrusion response strategies and resource allocation, balancing immediate threat mitigation with long-term system stability [42]. Furthermore, Explainable AI (XAI) modules improve user trust by providing transparent explanations of security decisions based on feature importance and contextual information [47].

CROSS-COMPARATIVE ANALYSIS AND INSIGHTS

***Corresponding Author:** Niharika Prasanna

Table 1: Cross-Comparative Analysis of Reviewed Works

Sl. No.	Category	Dataset(s)	Technique	Deployment Target	Accuracy	Explainable
1	Zero-day ML review	Various benchmarks	**Sup. ML** (DT, SVM, RF), **Unsup.** (AE, Clustering), **DL** (CNN, LSTM), **RL**, **Hybrid**, **FL**, Lightweight AI	General cyber defense	**Sup:** up to 98%; **Unsup:** 27–99%; **DL:** up to 94%; **RL:** ~90%; **Hybrid:** up to 100%	Medium–High (tree models, FL), Low (DL)
2	Autonomous Cyber Defense Agent	CybORG simulation	Hybrid: DRL + LLM chatbot (RAG + KG)	Network defense in simulation	Effective vs. 2 red-team strategies	Low–Medium
3	IoT zero-day detection	Mirai-infected IoT traffic	Unsupervised anomaly detection + Online One-Class SVM + FL	IoT devices	97% (known anomalies)	Medium
4	Autonomous comms security	Conceptual	ML anomaly detection + distributed consensus	Secure comm systems	Claimed improved detection	Medium
5	AutoML for Zero-Touch Networks	5G/6G case studies	AutoML (model selection, HPO, drift handling)	ZTN security	Maintains accuracy under drift	Medium
6	Robot CPS zero-day detection	UR10, Tiago, Jackal telemetry	CNN + LSTM + ensemble classifier	On-robot IDS	96%+	Medium
7	Cloud zero-day detection	AWS CIC 2018	CatBoost, XGBoost, NN, SVM, ensembles	Cloud IDS	Ensembles up to 99% (known), lower on zero-day	Medium
8	Space ACS simulation	Mission telemetry (sim)	AutoML detection + human-in-loop	Space systems	High (>95%)	Medium
9	AI & compliance review	Multiple case studies	AI anomaly detection, NLP	Enterprise security & compliance	Improved detection	Medium
10	Cybersecurity for IoT Healthcare	Custom IoT dataset	CNN, RNN	IoT medical devices	99%	Low
11	Blockchain IoT security	Simulated IoT	Blockchain + AI anomaly detection	IoT	High (>95%)	Medium
12	AI-based WAF	CSIC 2010, HTTP requests	ML classifiers (DT, RF, KNN, SVM)	WAF	99.70%	High
13	AI WAF deep learning	HTTP logs	CNN + LSTM	WAF	99.20%	Low
14	WAFFLED WAF bypass	Live HTTP to AWS, Azure, Cloudflare, ModSecurity	Grammar-based HTTP fuzzing	WAF testing	1207 bypasses found	N/A
15	Green Security	Various	Lightweight AI, TinyML	IoT security	Trade-off accuracy vs. energy	Medium
16	Industrial IoT security	SWaT dataset	Ensemble ML, anomaly detection	ICS/SCADA	~99%	Medium
17	Federated IDS	NSL-KDD CICIDS2017,	Federated SVM/RF	Distributed IDS	98% (NSL-KDD)	Medium

***Corresponding Author:** Niharika Prasanna

Sl. No.	Category	Dataset(s)	Technique	Deployment Target	Accuracy	Explainable
18	Malware detection	Malimg, Drebin	CNN, RF	Endpoint AV	94–99%	Medium
19	Adversarial ML defense	MNIST (security examples), CICIDS	Adversarial training	IDS, image recognition	Accuracy restored after attack	Low
20	IoT edge IDS	UNSW-NB15	Lightweight RF, DT	IoT edge	96%	High
21	PLC anomaly detection	SWaT, WADI	LSTM	ICS PLCs	95–98%	Low
22	IoT botnet detection	CTU-13, Bot-IoT	RF, XGBoost	IoT routers	99%	Medium
23	Traffic classification	CICFlowMeter features	CNN	ISP/Enterprise NIDS	98%	Low
24	Smart grid IDS	Custom SCADA logs	DNN + feature selection	Smart grid NIDS	97%	Medium
25	Cross-layer IDS (6G)	RF signal sets, CICIDS2017	AutoML + PLA + CLIDS	6G edge/cloud	>98%	Medium
26	Quantum-safe AI IDS	NSL-KDD	Hybrid quantum-classical ML	NIDS	94%	Medium
27	Blockchain IDS	UNSW-NB15	Blockchain + RF	IoT edge IDS	96%	Medium
28	TinyML IDS	NSL-KDD	Optimized DT, k-NN	IoT microcontrollers	94%	High
29	Autoencoder anomaly detection	KDD'99	Deep Autoencoder	NIDS	92%	Low
30	Transfer learning IDS	NSL-KDD, UNSW	TL from related domains	NIDS	70–75%	Medium
31	Adaptive ML NIDS	CICIDS2018	Adaptive RF + ADWIN drift detection	NIDS	Maintains ~95%	Medium
32	RL-based cyber defense	Simulated networks	Deep Q-Network	Network defense	>90%	Low
33	IoT intrusion detection	BoT-IoT, NSL-KDD	CNN + GRU	IoT gateways	98%	Low
34	ML-based spam filtering	Enron, SpamAssassin	Naive Bayes, SVM	Email servers	96–98%	High
35	AI for phishing detection	PhishTank, URL datasets	RF, XGBoost	Web gateways	97%	Medium
36	Insider threat detection	CERT Insider Threat	RNN, RF	Enterprise SIEM	94%	Medium
37	Cloud WAF with DL	CSIC 2010, custom HTTP logs	Bi-LSTM, CNN	Cloud WAF	98%	Low
38	Industrial anomaly detection	SWaT, gas pipeline data	CNN-LSTM hybrid	ICS monitoring	95–98%	Low
39	Vehicular IDS	VeReMi, CAN datasets	RF, DNN	Vehicle ECUs	97%	Medium
40	Cybersecurity in UAVs	UAVSim datasets	ML classifiers, CNN	UAV communications	94%	Medium

***Corresponding Author:** Niharika Prasanna

Sl. No.	Category	Dataset(s)	Technique	Deployment Target	Accuracy	Explainable
41	Threat intel fusion	Multiple OSINT feeds	NLP + ML fusion	Threat intelligence platform	92%	Medium
42	IoT anomaly detection (energy sector)	UNSW-NB15, power grid logs	LSTM Autoencoder	Smart grid IoT	96%	Low
43	Cross-platform malware detection	VirusShare, Drebin	CNN + opcode features	Multi-OS endpoints	95%	Medium
44	SDN-based IDS	SDNFlow, CICIDS2017	RF, SVM, DL	SDN controllers	96–99%	Medium
45	DNS anomaly detection	ISC, custom DNS datasets	Statistical + RF	DNS servers	95%	High
46	Blockchain-enabled access control	Simulated IoT	Blockchain + ML	IoT auth systems	>95%	Medium
47	Green security (TinyML)	Various IoT benchmarks	Optimized NN, DT	IoT edge	Accuracy–energy trade-off	Medium
48	Cybersecurity gamification	Training logs	Gamified RL agents	Cyber training simulations	Improved user performance	Medium

Key Cross-Paper Observations

- **Dominant datasets/benchmarks:** KDD'99/NSL-KDD and the CICIDS family continue to be widely used for NIDS research, while domain-specific studies employ specialized datasets (e.g., RoboMal for robotic cyber-physical systems, RF fingerprint datasets for Physical Layer Authentication (PLA), and CSIC/HTTPParams with live HTTP logs for Web Application Firewalls (WAFs)) [14,28].
- **Gaps in integration:** Very few studies attempt cross-system integration (e.g., NIDS + Endpoint AV + WAF + PLA). Most focus on a single security layer and evaluate performance within that domain. Cross-stack orchestration and information sharing remain significant research gaps [30].
- **Methodological trends:** The majority of existing approaches rely on supervised machine learning techniques such as Random Forest (RF), Support Vector Machine (SVM), Decision Tree (DT), and Neural Networks (NN). Emerging trends include AutoML, adaptive learning, and reinforcement learning [19].
- **Energy and computational trade-offs:** Several studies discuss the trade-off between detection performance and computational efficiency. The literature emphasizes balancing accuracy with latency, memory consumption, and energy usage, particularly in the context of "green security" and TinyML-based deployments [46].

OPEN CHALLENGES AND RESEARCH DIRECTIONS

Unified AI Defense Agents

Current cybersecurity solutions are largely siloed, focusing individually on Network Intrusion Detection Systems (NIDS), antivirus software, or Web Application Firewalls (WAFs). There is a growing need for multi-domain, general-purpose AI agents capable of correlating alerts, sharing threat intelligence, and automating responses across multiple layers of cybersecurity.

Energy- and Resource-Efficient Models

Many high-performance deep learning and ensemble models require substantial computational power and memory. Green security approaches, including TinyML, model compression, and lightweight architectures, remain underexplored but are essential for IoT, mobile, and edge computing environments.

Autonomous Updating and Drift Resilience

Most existing models require extensive offline retraining to adapt to emerging threats. Future research should focus on adaptive online learning models with self-updating capabilities that can automatically respond to concept drift without requiring manual intervention.

Federated Learning for Distributed Defense

Federated learning has demonstrated promising results for intrusion detection and IoT botnet detection in small-scale proof-of-concept studies. However, large-scale deployment remains challenging due to communication overhead, privacy-preserving aggregation mechanisms, and the handling of non-IID (non-independent and identically distributed) data across distributed nodes.

Explainability in Malware and NIDS Systems

Although deep learning models such as CNNs, LSTMs, and deep ensembles often achieve high detection accuracy, they generally lack interpretability. Explainable AI (XAI) techniques are essential for

***Corresponding Author:** Niharika Prasanna

regulatory compliance, improving user trust, and facilitating efficient incident response and forensic analysis.

Synergizing Isolated Solutions into Multi-Layered Defense Stacks

Physical, network, and application-layer security mechanisms should be integrated into unified cybersecurity frameworks. Cross-layer feature fusion can improve detection accuracy, enable policy-driven orchestration, and support continual learning across multiple security domains.

PLANNED FUTURE APPROACH

The literature review of 48 recent studies indicates that most AI-based cybersecurity solutions have been developed for specific application domains, including NIDS [44,37,36], antivirus and malware detection [12,9], and WAFs [31,38,10], with minimal cross-domain integration. Although many studies report detection accuracies exceeding 95%, the absence of coordinated, multi-layered security architectures leaves systems vulnerable to sophisticated multi-stage cyberattacks.

In our comparative analysis, the term **GreenNet** (or **Green Security**) refers to previous research on TinyML-based, energy-efficient cybersecurity, such as the work of Brudni *et al.* (2024). It is **not** introduced in this paper as a novel framework. Instead, it is included in the literature review to emphasize the importance of lightweight and energy-efficient cybersecurity solutions. The primary contribution of this work is the proposal of a Deep Reinforcement Learning (DRL)-based holistic cybersecurity architecture, which builds upon and extends existing research.

Previous studies have demonstrated the effectiveness of reinforcement learning for network defense [28,35], adaptive intrusion detection models [36], sandbox-based verification for malware analysis [12], and techniques for reducing false positives. However, no existing work has integrated these validated approaches into a unified, inter-domain cybersecurity framework.

To address these research gaps, we propose a Deep Reinforcement Learning (DRL)-based Holistic Cybersecurity System (Fig. 1). The proposed architecture consists of multiple decentralized security components, including Network Intrusion Detection and Prevention Systems (NIDPS), antivirus software (AV), Web Application Firewalls (WAFs), and malware detection modules, each independently analyzing incoming network traffic.

Suspicious packets are redirected to sandbox environments [12] that replicate the target systems to verify their behavior before classification. A Deep Reinforcement Learning framework [28,35] then integrates the outputs of all security modules together with sandbox analysis results to determine appropriate security actions in real time while continuously improving through experience. Confirmed malicious packets are safely discarded, whereas legitimate packets are forwarded to their intended destinations. All decisions are recorded to facilitate continual learning and reduce false negatives over time.

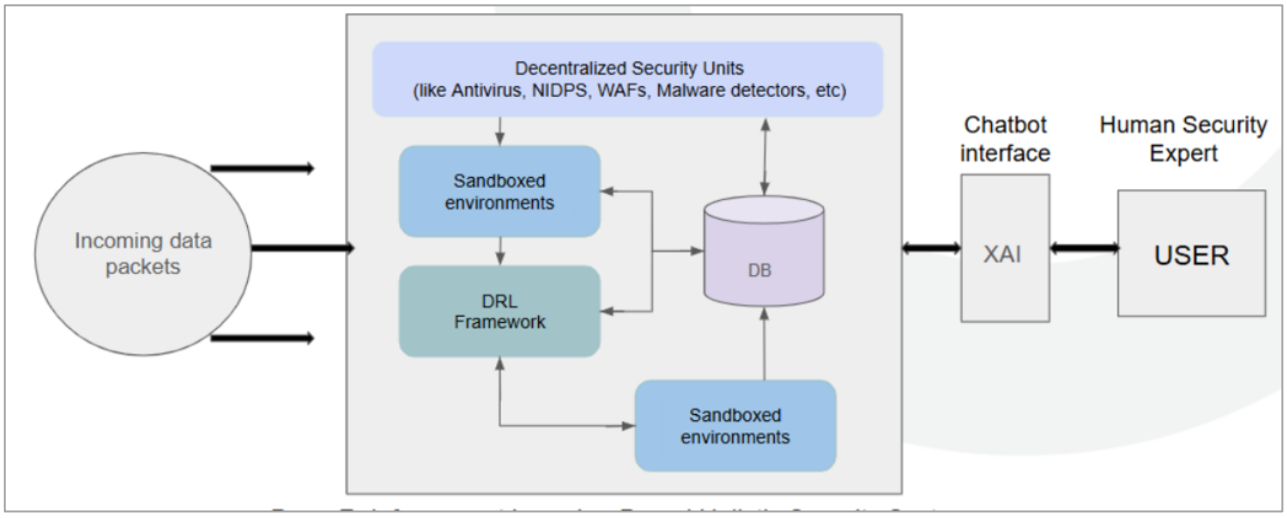

Fig. 1. Proposed architecture of the Deep Reinforcement Learning (DRL)-based holistic cybersecurity system.

The proposed high-level architecture builds upon:

- Decentralized analysis inspired by federated IDS research [30,44,43].
- Sandbox verification adapted from malware detection methodologies [12].
- Explainable AI mechanisms, including an XAI-enabled chatbot that provides contextual explanations and justifications for system decisions [31,26,15].

Although the proposed Deep Reinforcement Learning (DRL)-based holistic cybersecurity framework effectively integrates multiple defense layers, several practical challenges remain. Training and adapting DRL

***Corresponding Author:** Niharika Prasanna

agents are computationally intensive, while deployment in real-time, large-scale, or satellite-based environments may introduce latency and synchronization overhead. Furthermore, the energy requirements of continual learning and sandbox verification highlight the importance of developing lightweight, green-security optimizations. Future research will focus on improving computational efficiency, scalability, and energy consumption while preserving the adaptive and explainable characteristics of the proposed framework. Implementation details, experimental evaluation, and performance analysis will be presented in future work.

CONCLUSION

This review collected and categorized 48 recent studies on AI-powered cybersecurity across multiple domains, including Network Intrusion Detection Systems (NIDS), antivirus and malware detection, and Web Application Firewalls (WAFs). While each research area has demonstrated significant progress—with many studies achieving high detection accuracy through deep learning, reinforcement learning, and sandbox-based verification—there remains a considerable lack of integration across these domains. This fragmentation leaves cybersecurity infrastructures vulnerable to sophisticated, multi-stage, and adaptive cyberattacks.

Emerging research trends emphasize autonomous, adaptive, and data-driven cybersecurity solutions. Reinforcement learning enables dynamic decision-making, sandbox environments provide behavioral validation with high fidelity, and Explainable AI (XAI) enhances transparency and accountability. Collectively, these technologies have the potential to establish intelligent, automated, real-time, and trustworthy cybersecurity architectures.

This survey lays the foundation for our proposed Deep Reinforcement Learning-Based Holistic Cybersecurity System, an intelligent defense framework that integrates autonomy, adaptability, and explainability to address both current and emerging cyber threats while supporting the development of secure and resilient digital ecosystems.

REFERENCES

1. El Husseini, F., Noura, H., Salman, O., & Chehab, A. (2024). Advanced machine learning approaches for zero-day attack detection: A review. In *Proceedings of the 2024 8th Cyber Security in Networking Conference (CSNet)* (pp. 297–304).
2. Loevenich, J. F., Adler, E., Mercier, R., Velazquez, A., & Lopes, R. R. F. (2024). Design of an autonomous cyber defence agent using hybrid AI models. In *Proceedings of the 2024 International Conference on Military Communication and Information Systems (ICMCIS)* (pp. 1–10).
3. Ohtani, T., Yamamoto, R., & Ohzahata, S. (2024). Detecting zero-day attack with federated learning using autonomously extracted anomalies in IoT. In *Proceedings of the 2024 IEEE 21st Consumer Communications & Networking Conference (CCNC)* (pp. 356–359).
4. Gowrishankar, J., Chaudhary, P., & Sikka, R. (2024). Developing autonomous communications systems to enhance network security. In *Proceedings of the 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1–6).
5. Yang, L., El Rajab, M., Shami, A., & Muhaidat, S. (2024). Enabling AutoML for zero-touch network security: Use-case driven analysis. *IEEE Transactions on Network and Service Management.*
6. Kaur, U., Celik, Z. B., & Voyles, R. M. (2024). RoboCop: A robust zero-day cyber-physical attack detection framework for robots. In *Proceedings of the 2024 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)* (pp. 12457–12463).
7. Igugu, A. (2024). *Evaluating the effectiveness of AI and machine learning techniques for zero-day attacks detection in cloud environments* (Unpublished manuscript).
8. Tasdighi, A. (2024). *Simulation and testing of autonomous cybersecurity systems: Methodologies for simulating cyber-attacks in space to test effectiveness and human interactions*. SSRN.
9. Folorunso, A., Adewumi, T., Adewa, A., Okonkwo, R., & Olawumi, T. N. (2024). Impact of AI on cybersecurity and security compliance. *Global Journal of Engineering and Technology Advances, 21*(1), 167–184.
10. Yang, L., Naser, S., Shami, A., Muhaidat, S., Ong, L., & Debbah, M. (2025). Towards zero-touch networks: Cross-layer automated security solutions for 6G wireless networks. *IEEE Transactions on Communications.*
11. Toyin, O., *et al.* (2024). Intelligent network intrusion detection and prevention system (NIDPS): A machine learning and network security. In *Proceedings of the 2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON)* (pp. 1–6).
12. Patil, A. P., Premkumar, H., Hegde, P., *et al.* (2022). JARVIS: An intelligent network intrusion detection and prevention system. In *Proceedings of the 2022 IEEE Fourth International Conference on Advances in Electronics, Computers and Communications (ICAECC)* (pp. 1–6).
13. Shanthi, R., & Maruthi, R. (2023). A comparative study of intrusion detection and prevention systems for cloud environment. In *Proceedings of the 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 493–496).
14. Vadisetty, R., & Polamarasetti, A. (2024). Enhancing intrusion detection systems with deep learning and machine learning algorithms for real-time threat classification. In *Proceedings of the 2024*

***Corresponding Author:** Niharika Prasanna

Asian Conference on Intelligent Technologies (ACOIT) (pp. 1–6).
15. Nalini, N., Chaudhary, A., Surendran, S., Muthuraja, M., Ahmed, I., & Tj, N. (2023). Network intrusion detection system for feature extraction based on machine learning techniques. In *Proceedings of the 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 440–445).
16. Ullah, F., & Srivastava, G. (2024). Federated defense for malware detection and resilience against adversarial attacks. *IEEE Consumer Electronics Magazine.*
17. Xu, X., Zhang, Q., Wang, Y., Adebisi, B., Ohtsuki, T., & Gui, G. (2024). Advancing malware detection in network traffic with self-paced class incremental learning. *IEEE Internet of Things Journal.*
18. Dong, S., Shu, L., & Nie, S. (2024). Android malware detection method based on CNN and DNN hybrid mechanism. *IEEE Transactions on Industrial Informatics.*
19. Yang, C.-H., Maina, B. M., Cheng, S.-M., & Lee, H.-M. (2024). An adversarial attack on artificial intelligence malware detection in consumer Internet of Things. *IEEE Consumer Electronics Magazine.*
20. Liu, H., Gong, L., Mo, X., Dong, G., & Yu, J. (2024). Ltachecker: Lightweight Android malware detection based on Dalvik opcode sequences using attention temporal networks. *IEEE Internet of Things Journal.*
21. Jeon, J., Jeong, B., Baek, S., & Jeong, Y.-S. (2024). Static multi-feature-based malware detection using multi SPP-Net in smart IoT environments. *IEEE Transactions on Information Forensics and Security, 19*, 2487–2500.
22. Bussa, S., Prabaharan, G., Mishra, N., Seetha, J., Nair, V., *et al.* (2024). *Singularity AntiVirus: A novel approach to cybersecurity.* In *Proceedings of the 2024 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N)* (pp. 1636–1640).
23. Blancaflor, E. B., Magleo, J. R. T., Garcia, J. P. A. P., Navarro, J. R. D., & Lebosada, J. A. Q. (2024). *The usability assessment of antivirus software using the unified theory of acceptance and use of technology (UTAUT) model.* In *Proceedings of the 2024 17th International Conference on Advanced Computer Theory and Engineering (ICACTE)* (pp. 57–63).
24. Ryu, Y., Shin, K., Lee, J., Jung, D.-J., & Cho, H.-M. (2024). *Real-world antivirus evaluation methodology: Applying modern criteria for assessing antivirus functionality.* In *Proceedings of the 2024 International Conference on Information Networking (ICOIN)* (pp. 783–788).
25. Shahid, S. Z., Bangash, M. A., Hussain, M. R., & Arshad, S. (2024). *CyberCure: Malware defense system.* In *Proceedings of the 2024 4th International Conference on Innovations in Computer Science (ICONICS)* (pp. 1–7).
26. Brudni, S., Anidgar, S., Brodt, O., Mimran, D., Shabtai, A., & Elovici, Y. (2024). *Green security: A framework for measurement and optimization of energy consumption of cybersecurity solutions.* In *Proceedings of the 2024 IEEE 9th European Symposium on Security and Privacy (EuroS&P)* (pp. 676–696).
27. Wu, C., *et al.* (2024). *WAFBooster: Automatic boosting of WAF security against mutated malicious payloads. IEEE Transactions on Dependable and Secure Computing.*
28. Li, K., Yang, H., & Visser, W. (2022). *Evolutionary multi-task injection testing on web application firewalls. arXiv.* https://arxiv.org/abs/2206.05743
29. Riverol, A., Betarte, G., Martínez, R., & Pardo, A. (2024). *Capturing the security expert knowledge in feature selection for web application attack detection.* In *Proceedings of the 13th Latin-American Symposium on Dependable and Secure Computing* (pp. 153–158).
30. Dawadi, B. R., Adhikari, B., & Srivastava, D. K. (2023). Deep learning technique-enabled web application firewall for the detection of web attacks. *Sensors, 23*(4), 2073.
31. Scano, C., *et al.* (2024). *ModSec-Learn: Boosting ModSecurity with machine learning.* In *Proceedings of the International Symposium on Distributed Computing and Artificial Intelligence* (pp. 23–33).
32. dos Santos, C. H. M., & de Lima, S. M. L. (2024). XAI-driven antivirus in pattern identification of Citadel malware. *Journal of Computer Science, 82*, 102389.
33. Kolluri, V. (2024). Revolutionary research on the AI Sentry: An approach to overcome social engineering attacks using machine intelligence. *International Journal of Advanced Research in Interdisciplinary Science Endeavours, 1*(1), 53–58.
34. Kolluri, V. (2024). An extensive investigation into guardians of the digital realm: AI-driven antivirus and cyber threat intelligence. *International Journal of Advanced Research in Interdisciplinary Science Endeavours, 1*(2), 71–76.
35. *Analyzing machine learning algorithms for antivirus applications: A study on decision trees, support vector machines, and neural networks.* (2024). ResearchGate.
36. Yang, S., Yang, Y., Zhao, D., Xu, L., Li, X., Yu, F., & Hu, Y. (2025). Dynamic malware detection based on supervised contrastive learning. *Computers & Electrical Engineering, 123*, 110108.
37. Coscia, A., Dentamaro, V., Galantucci, S., Maci, A., & Pirlo, G. (2024). Automatic decision tree-based NIDPS ruleset generation for DoS/DDoS attacks. *Journal of Information Security and Applications, 82*, 103736.
38. Ayantayo, A., Kaur, A., Kour, A., Schmoor, X., Shah, F., Vickers, I., Kearney, P., & Abdelsamea, M. M. (2023). Network intrusion detection using feature fusion with deep learning. *Journal of Big Data, 10*(1), 167.

***Corresponding Author:** Niharika Prasanna

39. Isiaka, R., & Popoola, D. (2023). Development of an intrusion detection system in web applications using C-means and decision tree algorithm. *International Journal of Applied Science and Technology, 13*(1).
40. Alabrah, A. (2023). An efficient NIDPS with improved salp swarm feature optimization method. *Applied Sciences, 13*(12), 7002.
41. Fritsch, L., Jaber, A., & Yazidi, A. (2022). An overview of artificial intelligence used in malware. In E. Zouganeli, A. Yazidi, G. Mello, & P. Lind (Eds.), *Nordic Artificial Intelligence Research and Development (NAIS 2022)* (Communications in Computer and Information Science, Vol. 1650, pp. 41–56). Springer. https://doi.org/10.1007/978-3-031-17030-0_4
42. Chandran, S., Syam, S. R., Sankaran, S., Pandey, T., & Achuthan, K. (2025). From static to AI-driven detection: A comprehensive review of obfuscated malware techniques. *IEEE Access, 13*, 74335–74358. https://doi.org/10.1109/ACCESS.2025.3550781
43. Galli, A., La Gatta, V., Moscato, V., Postiglione, M., & Sperlì, G. (2024). Explainability in AI-based behavioral malware detection systems. *Computers & Security, 140*, 103842. https://doi.org/10.1016/j.cose.2024.103842
44. Ferdous, J., Islam, R., Mahboubi, A., & Islam, M. Z. (2024). AI-based ransomware detection: A comprehensive review. *IEEE Access, 12*, 136666–136695. https://doi.org/10.1109/ACCESS.2024.3461965
45. Durmuşkaya, M. E., & Bayraklı, S. (2025). Web application firewall based on machine learning models. *PeerJ Computer Science, 11*, e2975.
46. Román-Gallego, J.-Á., Pérez-Delgado, M.-L., Viñuela, M. L., & Vega-Hernández, M.-C. (2025). Artificial intelligence web application firewall for advanced detection of web injection attacks. *Expert Systems, 42*(1), e13505.

***Corresponding Author:** Niharika Prasanna