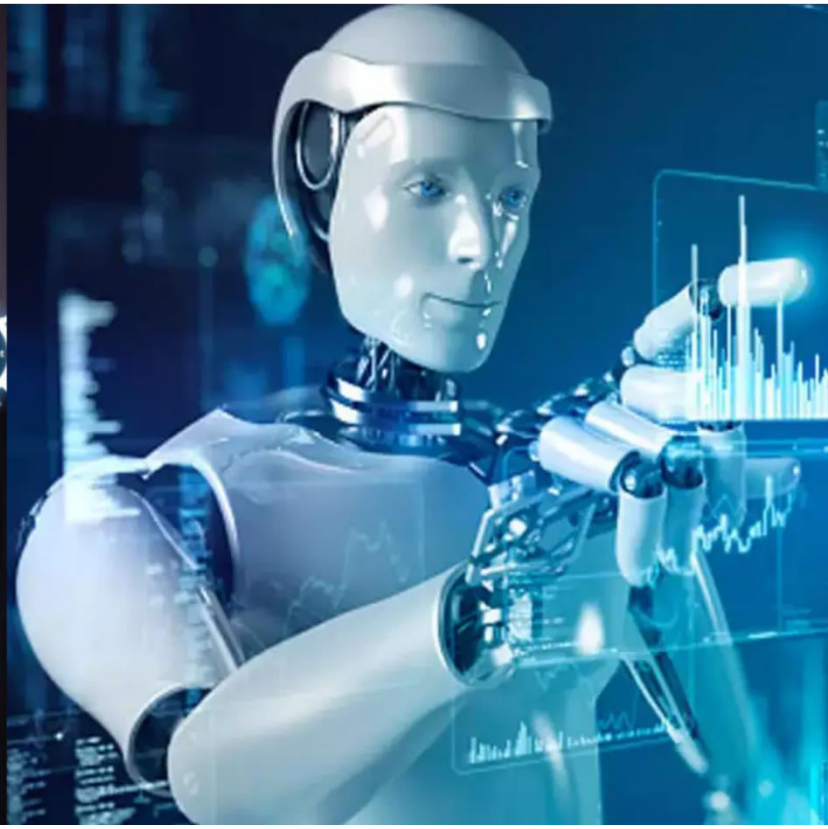
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503210|

AI-Driven Adaptive Firewall Framework for Enhanced Cybersecurity

Nagda Kamlesh Ganeshlal, Dr. Hetal R. Modi

Msc Cybersecurity Student, Bhagwan Mahavir College of Computer Applications, Surat, India

Asst. Professor, Bhagwan Mahavir College of Computer Application, Bhagwan Mahavir University, Surat, India

ABSTRACT: The increasing complexity of cyber threats has made traditional rule-based firewalls inadequate against attacks such as zero-day exploits and advanced persistent threats. This paper proposes an AI-Driven Adaptive Firewall Framework that enhances network security through intelligent threat detection and dynamic policy updates.

By integrating machine learning and deep learning for anomaly detection with reinforcement learning for automated rule optimization, the framework enables real-time adaptation to evolving threats. The study highlights that AI-based firewalls achieve higher detection accuracy, reduced false positives, and improved automation compared to conventional systems. Although challenges such as computational cost and data dependency remain, AI-driven adaptive firewalls offer a strong and scalable solution for modern cybersecurity.

KEYWORDS: Adaptive Firewall, Artificial Intelligence, Machine Learning, Reinforcement Learning, Intrusion Detection, Cybersecurity, Anomaly Detection.

I. INTRODUCTION

Today's cybersecurity landscape is characterized by an unprecedented level of complexity and sophistication, with cybercriminals using advanced techniques such as polymorphic malware, zero-day exploits, and social engineering tactics to infiltrate networks and compromise sensitive data. The rapidly evolving cybersecurity landscape demands innovative solutions that surpass the limitations of traditional defense systems' capabilities. Conventional firewalls often fail to protect against sophisticated threats such as zero-day a acks, polymorphic malware, and advanced persistent threats (APTs)[6].
In the current digital era, the rapid expansion of networks and the emergence of sophisticated cyberattacks demand more advanced methods for system protection[3]. AI-Augmented Firewall that leverages artificial intelligence to enhance real-time network security. By integrating AI for anomaly detection and dynamic policy adjustments, the firewall can adapt to evolving threats, offering stronger and more responsive protection compared to traditional firewalls [4]. Importance of intelligent, dynamic firewalls [1][7][21].

II. LITERATURE REVIEW

- **ML-Based Intrusion Detection:** Supervised learning (e.g. XGBoost, SVM, DT) for attack classification [1–3][19][13]; high accuracy (often >99%) and reduced false alarms [1][2][3][19].
- **Adaptive Learning & Retraining:** Dynamic retrainable firewalls using continual learning and microservice architectures [6][12]; emphasize real-time adaptation to new threats.
- **Reinforcement Learning (RL) Approaches:** RL for automated rule optimization (e.g. Q-learning, DRL) [7][10][20]; autonomously update policies, improve response to evolving attacks.
- **Deep Learning & Hybrid Models:** Use of DL (CNN, LSTM) for anomaly/log analysis and hybrid frameworks [7][21]; e.g. CNN-LSTM achieved top accuracy in log detection [21].
- **Specialized Firewall Extensions:** Advanced concepts like dual-layer WAF with ML [13], HPC-focused rule refinement [15], log-based analytics [21], LLM-enhanced policy generation [5], and microservices security [20].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503210|

- Cite key results: near-perfect detection [1][3][13], significant FP reduction [4][21], and improved scalability [5][7].

III. RESEARCH GAP IDENTIFICATION

- Many solutions achieve high accuracy on known datasets but lack testing on live networks.
- Insufficient integration of multiple AI techniques in a unified architecture.
- Scalability and real-time deployment challenges remain.
- Lack of explainability and handling of adversarial inputs in current models.
- Need for frameworks combining ML, RL, and possibly LLMs for dynamic rule synthesis.

IV. PROPOSED METHODOLOGY / FRAMEWORK

- Introduce a novel conceptual framework integrating modules: **Data Collection**, **AI Analytics (ML/DL)**, **RL Policy Engine**, and **Adaptive Firewall Controller**.
- network traffic is fed to a feature extraction module; an AI analytics component (using ensemble ML/DL models) detects anomalies [1–3][21]; detected threats inform an RL-based policy engine to update firewall rules [7][10]; an LLM-assisted interface generates human-readable policies [5]; continuous feedback loop allows dynamic retraining [6][12].
- Emphasize collaboration between supervised classifiers (for intrusion detection) and RL agents (for rule adaptation) in the framework.
- Highlight performance evaluation via simulation (e.g., NSL-KDD, CIC-IDS2017) and comparison benchmarks.

V. COMPARATIVE ANALYSIS TABLE

Approach/Techniques	Application	Key Results / Metrics
Dragonfly & Bat feature selection + DT/SVM/LR[1]	Intrusion detection (UNSW-NB15 dataset)	~100% accuracy (DT) and reduced false positives.
XGBoost classifier[2]	Real-time intrusion detection (CIC-IDS2017)	Superior accuracy and adaptability vs. rule-based systems.
ATRS (adaptive threat score) & RAA (risk access) [3]	Firewall decision-making	>99.5% detection accuracy with adaptive access control.
Deep RL (LSTM-CNN anomaly detector + MDP agent) [7]	Dynamic rule optimization & prevention	Improved accuracy, lower false positives and latency vs. static firewalls.
Deep Q-Learning RL (FireRL framework) [10][20]	Automated rule generation	Rapid adaptation, reduced false positives, robust against new attacks.
Dual-layer ML (DT + SVM) [13]	Web application firewall anomaly detection	99.88% detection accuracy, 100% precision, minimal false alarms.
Multiple ML (KNN, SVM, NN) on firewall logs [15]	HPC network firewall policy error detection	High accuracy in classifying firewall events; KNN/J48/NN excelled.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503210|

Approach/Techniques	Application	Key Results / Metrics
Shallow NN + Decision Tree (Internet Firewall-2019 data) [19]	Packet filtering decisions	99.8% accuracy (ODT), 98.5% (SNN) for allow/deny/drop.
Deep learning (CNN-LSTM) [21]	Firewall log analysis	Best accuracy (~86.3%) among DL models; reduced false positives, adaptable learning.
Deep RL (multibit trie optimization) [12]	Packet classification	Faster lookup and memory efficiency for scalable firewalls.

Table 1. Comparative overview of AI-driven firewall approaches from literature with core techniques and outcomes.

VI. RESULTS & DISCUSSION

- **Synthesis of Findings:** AI-driven firewalls consistently yield high threat detection rates [1–3][13][19]. Several studies report accuracies above 99% due to advanced ML/DL models.
- **False Positives:** Many proposed methods significantly lower false positives compared to static systems [1][4][21]. For instance, hybrid anomaly detectors and rule-update engines cut FP rates by learning patterns.
- **Adaptivity and Automation:** RL and dynamic frameworks show quick adaptation to new attacks [7][10]. Firewalls using RL agents updated rules in real-time, improving resilience (e.g., FireRL prototype reacted rapidly to threats).
- **Hybrid Strategies:** Combining multiple AI techniques (e.g. ML for detection and RL for policy) is notably effective [7][13]. The dual-layer WAF [13] and LLM-assisted policy generation [5] illustrate benefits of multi-model designs.
- **Resource and Complexity:** Some methods introduce computational overhead (deep models, continual retraining) that must be balanced against security gains. Studies highlight the need to optimize training latency and resource use.
- **Comparison with Traditional:** All surveyed papers indicate AI-enhanced systems outperform static firewalls in key metrics. However, real-world deployment details and standardized benchmarks are often missing.

VII. ADVANTAGES AND LIMITATIONS

Advantages:

- *Enhanced Detection:* Learning-based firewalls achieve superior accuracy, capturing complex patterns [1][21].
- *Reduced False Alarms:* AI models adapt to context, lowering false positive rates [1][4][21].
- *Dynamic Adaptation:* RL and retraining allow firewalls to evolve with threats [6][7][10].
- *Automation:* Rule generation and tuning can be automated, easing admin burden [10][13].

Limitations:

- *Computational Cost:* Training ML/DL models requires resources and may introduce latency [10][14].
- *Data Dependency:* High-quality, labeled data (e.g. CIC-IDS, UNSW-NB15) needed for training; real-world datasets can be scarce.
- *Complexity:* Integrating multiple AI modules adds system complexity and potential points of failure.
- *Explainability:* AI-driven decisions can lack transparency, challenging human trust.
- *Security of AI:* ML models themselves may be vulnerable to adversarial attacks or drift, necessitating further safeguards.

VIII. FUTURE SCOPE

- Explore **Federated Learning** for distributed firewall training without central data sharing.
- Investigate **Adversarial Robustness** to ensure ML models resist tampering.
- Integrate **Explainable AI (XAI)** to make firewall decisions interpretable for administrators.
- Develop **Lightweight Models** for deployment in resource-constrained environments (IoT, edge).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503210|

- **Real-World Validation:** Test AI firewalls in live networks and with evolving threat landscapes.
- **LLM and Knowledge Graphs:** Use large language models and threat intelligence graphs for automated policy suggestions [5].
- **User Privacy:** Ensure AI-based inspection respects privacy (e.g. through federated or anonymized learning).

IX. CONCLUSION

This survey confirms that integrating AI techniques into firewall systems markedly improves intrusion detection and adaptive defense capabilities. Supervised ML and DL models achieve very high detection accuracy, while reinforcement learning enables automated rule optimization. The proposed conceptual framework synthesizes these advances into a cohesive system. Nonetheless, challenges such as computational overhead, data requirements, and explainability must be addressed. Overall, AI-driven adaptive firewalls represent a promising direction for robust network security, offering dynamic, intelligent protection against modern threats.

REFERENCES

[1] Ali Al-Allawee, Sultan Aldossary, Radhwan M. Abdullah, and Lway F. Abdulrazak, "Intelligent Firewall for Attack Detection: Integrating Dragonfly and Bat Algorithms with Machine Learning," *Journal of Computing & Biomedical Informatics*, vol. 10, no. 1, 2025.
[2] H. U. Shinde, A. S. Naikwade, and S. S. Chiddarwar, "AI-Driven Intelligent Firewall for Real-Time Intrusion Detection Using XGBoost and CIC-IDS-2017 Dataset," *International Research Journal of Engineering and Technology*, vol. 9, no. 5, 2025.
[3] Mahesh S. Hale, Sandhya R. Wani, and Rubina Sheikh, "AI Enabled Firewall Using Two Metrics ATRS and RAA," *International Journal of Cybernetics and Computer Engineering*, Sep.–Oct. 2025.
[4] Parvathi S., Raj Shekhar Singh, and Simpal Kumari, "Dynamic AI-Augmented Firewall for Real-Time Threat Mitigation," *International Research Journal of Advanced Engineering and Technology*, 2025.
[5] Sujay Kanungo et al., "Reinforced Learning Based Firewall Architecture Leveraging LLMs," *International Journal of AI in Data Science and Machine Learning*, vol. 7, no. 1, 2026.
[6] Sina Ahmadi, "Adaptive Cybersecurity: Dynamically Retrainable Firewalls for Real-Time Network Protection," *arXiv* preprint 2501.09033, 2025.
[7] Taimoor Ahmad, "AI-Driven Dynamic Firewall Optimization Using Reinforcement Learning for Anomaly Detection and Prevention," *arXiv* preprint 2506.05356, 2025.
[8] Yasin Çarkçı, Alperen Sayar, Seyit Ertuğrul, Gökhan Karaca, and Aybar Toka, "ML-Driven System for Automated Threat Detection & Firewall Rule Management," *Veri Bilimi ve Uygulama Dergisi*, 2025.
[9] Akhila Reddy Yadulla, "Building Smarter Firewalls with AI," *International Journal of Computer Applications*, vol. 182, no. 37, 2022.
[10] Minghong Yang, Zhenhua Yang, and Qiwen Yang, "Adaptive Firewall Strategy Generation and Optimization Based on Reinforcement Learning," *Informatica* (Slovenia), vol. 49, no. 33, 2025.
[11] Parvathi S. et al., "AI-Augmented Firewall for Real-Time Threat Mitigation," *International Research Journal of Advanced Engineering and Technology*, 2025.
[12] Hasibul Jamil and Ning Weng, "Multibit Tries Packet Classification with Deep Reinforcement Learning," *arXiv* preprint 2205.08606, 2022.
[13] Ahmed Sameh and Sahar Selim, "Adaptive Dual-Layer Web Application Firewall (ADL-WAF) Leveraging Machine Learning for Enhanced Anomaly and Threat Detection," *arXiv* preprint 2511.12643, 2025.
[14] *IJRIAS Journal*, "AI-Driven Next-Generation Firewall Architecture," International Journal of Research in Innovation and Advanced Sciences, 2025.
[15] Jae-Kook Lee, Taeyoung Hong, and Gukhua Lee, "AI-Based Approach to Firewall Rule Refinement on High-Performance Computing Service Network," *Applied Sciences*, vol. 14, no. 11, 2024, p. 4373.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503210|

[16] Ashwin Kumar N.S. et al., "AI-Enhanced Firewall (AIEF)," *International Journal of Creative Research Thoughts*, vol. 13, no. 5, 2025.
[17] K. Ganga Parvathi et al., "Adaptive Firewall Simulation Model Integrating Packet Filtering and Anomaly Detection," *International Journal of Engineering & Advanced Technology*, vol. 9, no. 3, 2025.
[18] Martha O. Musa and Temitope V. Ime, "Improving Internet Firewall Using Machine Learning Techniques," *American Journal of Computer Science and Technology*, vol. 6, no. 1, 2023.
[19] Qasem Abu Al-Haija and Abdelraouf Ishtaiwi, "Machine Learning Based Model to Identify Firewall Decisions to Improve Cyber-Defense," *International Journal on Advanced Science, Engineering and Information Technology (IJASEIT)*, vol. 11, no. 4, 2021, pp. 1688–1695.
[20] Vijay Ramamoorthi, "Anomaly Detection and Automated Mitigation for Microservices Security with AI," *Applied Research in Artificial Intelligence and Computing*, vol. 3, no. 2, 2024.
[21] Yasmine Aboudrar, Muhammad Imran, and D. A. Yasin, "AI-Driven Firewall Log Analysis: Enhancing Threat Detection with Deep Learning Techniques," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 16, no. 7, 2025.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details