JOURNAL OF THE AMERICAN INSTITUTE
ISSN: 3066-3776
United States

# Enhanced Firewall Optimization in Network Design

**Riko Herwanto[1], Sushanty Saleh[2]**

Email Correspondent: rikoherwanto@darmajaya.ac.id

**Keywords:**
Firewall Optimization, Artificial Intelligence, Machine Learning, Network Security, Intrusion Detection, Dynamic Adaptability, Explainable AI, Cybersecurity.

**Abstract**

The escalating complexity and frequency of sophisticated cyber threats necessitate a fundamental shift from traditional, static firewall architectures toward intelligent, adaptive security solutions. This paper presents a comprehensive examination of enhanced firewall optimization strategies through the integration of artificial intelligence and machine learning within modern network design. The research systematically reviews contemporary advancements in firewall technologies, including next-generation firewalls, AI-driven intrusion detection systems, and dynamically retrainable security frameworks. A novel methodological framework is proposed that emphasizes network-centric design, incorporating advanced rule set optimization algorithms, real-time traffic analysis, and anomaly detection mechanisms powered by supervised, unsupervised, and reinforcement learning techniques. The system architecture adopts a modular, distributed approach leveraging containerization and microservices to ensure scalability, resilience, and seamless integration with existing network infrastructure. Experimental evaluation utilizing benchmark datasets (including UNSW-NB15, CICIDS2017, and NSL-KDD) demonstrates that AI-enhanced firewalls achieve superior detection accuracy exceeding 99%, significantly reduce false positive rates, and maintain minimal latency compared to conventional rule-based and signature-dependent systems. The incorporation of explainable AI frameworks such as SHAP and LIME further enhances model interpretability, fostering trust and enabling informed decision-making by security analysts. Despite these advancements, challenges persist regarding computational overhead, hyperparameter optimization, and reliance on labeled datasets, underscoring the need for future research into unsupervised learning, standardized experimental datasets, and techno-economic assessments. This paper concludes that AI-driven firewall optimization represents a paradigm shift in cybersecurity, offering proactive, adaptive, and transparent defense mechanisms essential for protecting complex network environments against evolving cyber threats.



## INTRODUCTION

As the foundational security layer in network architectures, firewalls are indispensable for monitoring and filtering network traffic based on predefined security policies (Lu & Yang, 2020). However, the increasing complexity and volume of modern network communications necessitate

[1] Department of Informatics Engineering, Faculty of Computer Science, Institut Informatika dan Bisnis Darmajaya, Indonesia, rikoherwanto@darmajaya.ac.id
[2] Department of Informatics Systems, Faculty of Computer Science, Institut Informatika dan Bisnis Darmajaya, Indonesia

sophisticated optimization techniques to mitigate inherent latency challenges arising from sequential packet classification processes (Coscia et al., 2023). This issue is further compounded by the dynamic nature of firewall rules in paradigms such as software-defined networking, where the control plane often shoulders significant computational and communication overhead (Caprolu et al., 2019). Consequently, an innovative, distributed architecture for firewall management, incorporating encrypted policies, is crucial to bolster fault tolerance and safeguard against sophisticated cyber threats (Allami et al., 2025). Such an architecture can leverage obfuscated blacklists or whitelists distributed across multiple servers to prevent external attacks targeting firewall data. Moreover, optimizing the generation and deployment of these firewall rules, especially in large-scale power systems, can significantly enhance proactive cyberattack defense by automating configuration and simulating data flows, thereby reducing manual errors and response times (Sahu et al., 2023).

This automation extends to Supervisory Control and Data Acquisition networks, where manual configuration errors can have catastrophic consequences for critical infrastructure systems like power generation and water distribution. Therefore, developing high-level approaches for configuring these firewalls can dramatically improve reliability and diminish the tediousness associated with manual deployments. Furthermore, the integration of bio-inspired, self-organizing protocols into decentralized firewall architectures offers autonomous management and optimization capabilities, ensuring resilience against evolving threats and dynamic service requirements (Duan & Al-Shaer, 2025).

Numerous studies have explored various facets of firewall optimization, including rule management, placement strategies, and integration with advanced networking paradigms to address the challenges of modern network security (Arthur et al., 2019; Smine, 2022). For instance, research has delved into the computational complexity of allowing rule ordering and greedy algorithms to optimize packet classification, highlighting how an increasing number of rules can lead to significant communication latency (Fuchino et al., 2023). This latency is further exacerbated by the static nature and lack of adaptability in traditional firewall architectures, which often struggle to respond effectively to real-time cyberattacks and suffer from inherent difficulties in obtaining a global view of all firewalls within a complex enterprise network (Duan & Al-Shaer, 2025). This limitation underscores the need for adaptive cybersecurity solutions, moving beyond static rule sets to dynamically retrainable firewalls that can leverage machine learning to analyze network traffic patterns and identify emergent threats in real-time (Ahmadi, 2025). These advanced systems necessitate architectures such as microservices and distributed frameworks to support real-time adaptability, drawing upon diverse data sources for continuous model retraining and dynamic threat identification through reinforcement and continual learning (Ahmadi, 2025). This dynamic adaptation provides significant improvements in detection accuracy and reduces false positives, offering a scalable solution for complex attack vectors in diverse settings (Ahmad, 2025).

This evolution marks a substantial shift from traditional firewalls, which largely depended on static, rule-based filtering, to more intelligent systems capable of anticipating and mitigating sophisticated cyber threats (Ahmadi, 2023; Lekkala, 2024). Modern firewalls, therefore, integrate advanced analytical capabilities, leveraging artificial intelligence and machine learning to analyze network traffic patterns, detect anomalies, and autonomously adapt security policies in response to evolving threat landscapes (Ahmadi, 2025). This paradigm shift is crucial given the increasing complexity of cyberattacks, which necessitate adaptive, machine learning-driven systems to identify and respond to emerging threats in real time rather than relying solely on predetermined rules. Next-generation firewalls, for example, incorporate deep packet inspection, application awareness, and integrated threat intelligence to enhance defense against sophisticated attacks (Srikanth, 2024). Moreover, the incorporation of dynamically retrainable firewalls, utilizing machine-learning models

to analyze network data and adjust settings, significantly improves the recognition of deviations and accelerates detection execution, thereby minimizing the impact of breaches. This contrasts sharply with conventional firewalls that often fail to adequately protect against sophisticated threats such as zero-day exploits, polymorphic malware, and advanced persistent threats (Ahmadi, 2025).

These security challenges are further exacerbated by the rapid advancement of network technologies, with 5G and AI integration presenting unprecedented difficulties for traditional intrusion detection systems and firewalls (Maasaoui et al., 2025). The proliferation of interconnected devices and the escalating sophistication of adversarial tactics demand robust and adaptive solutions, as evidenced by the successful implementation of reinforcement learning for dynamic firewall optimization and threat hunting in 5G environments (Alnfiai, 2025). Moreover, the growing complexity and scale of cyber threats, intensified by the expansion of cloud computing and the Internet of Things, further challenge conventional security mechanisms (Mohamed, 2025). Consequently, there is an urgent need for advanced cybersecurity paradigms that can dynamically adapt to new threats and autonomously manage security policies across heterogeneous network environments (Mohamed, 2025).

Traditional cybersecurity approaches, such as signature-based detection and rule-based firewalls, often prove inadequate in responding to the evolving and sophisticated nature of modern cyber threats, highlighting the limitations of static defense mechanisms (Oh et al., 2023). This is particularly evident when confronting zero-day exploits, polymorphic malware, and advanced adversarial machine learning attacks, which easily circumvent static configurations (Alnfiai, 2025). To address these challenges, advanced techniques integrating artificial intelligence and machine learning are being developed to create more adaptive and autonomous cybersecurity solutions (Klein & Romano, 2025). Artificial intelligence, specifically machine learning and deep learning, offers significant advancements in threat detection, prevention, and response by analyzing vast datasets in real-time to identify subtle patterns indicative of cyber threats and adapt to new attack strategies more efficiently than conventional methods (Agrawal et al., 2024; Salem et al., 2024). These AI-driven systems can autonomously learn from new threat intelligence and adjust firewall policies dynamically, providing a proactive defense against evolving cyber threats.

## METHOD

### Methodology for Enhanced Firewall Optimization

This section outlines a comprehensive methodology for developing an enhanced firewall optimization framework, focusing on the integration of artificial intelligence and machine learning techniques to achieve dynamic adaptability and proactive threat mitigation. The framework prioritizes real-time threat detection and policy enforcement through continuous learning and autonomous decision-making processes, thereby addressing the limitations of static rule-based systems.

### Framework for Network-Centric Firewall Design

This framework emphasizes a holistic approach, integrating firewall optimization directly into the network design from the outset, rather than treating it as a peripheral security component (Brody et al., 2025). This integration ensures that security policies are intrinsically woven into the network's operational fabric, facilitating seamless adaptation to evolving threats and compliance requirements. This proactive integration, driven by AI and machine learning, allows for continuous refinement of security posture based on real-time network telemetry and threat intelligence, significantly reducing the attack surface (KELVIN et al., 2024). This approach moves beyond reactive

defense mechanisms, enabling predictive threat modeling and automated policy adjustments across various network segments.

### Rule Set Optimization Algorithms

The effectiveness of this dynamic optimization hinges on advanced rule set algorithms that can autonomously analyze network traffic, identify anomalous patterns, and generate or modify firewall rules with minimal human intervention. These algorithms often leverage machine learning models, such as reinforcement learning and deep learning, to continually refine firewall configurations based on observed network behavior and emerging threat intelligence (Ita & Roshanaei, 2024). For instance, clustering techniques and anomaly detection models can analyze network logs and communication patterns to identify potential threats, which then inform the automated adjustment of firewall rules (Tallam, 2025).

### Traffic Analysis and Anomaly Detection

Advanced traffic analysis employs sophisticated machine learning algorithms to process vast streams of network data, identifying subtle deviations from established baselines that may indicate malicious activity (Priya et al., 2025). This includes leveraging techniques like deep packet inspection and behavioral analytics to discern zero-day exploits, polymorphic malware, and sophisticated persistent threats that bypass signature-based detection. Furthermore, AI-driven anomaly detection systems can differentiate between normal network operations and malicious incursions by continuously learning and adapting to new threat vectors, significantly improving threat identification accuracy (Becher & Torka, 2024). This proactive approach allows for immediate policy adjustments, thereby minimizing the window of vulnerability and enhancing overall network resilience against sophisticated cyberattacks (Hashmi et al., 2025). Such systems are particularly adept at handling encrypted traffic, where traditional methods often fail, by analyzing metadata and behavioral patterns to infer potential threats (Alvarado-Molina et al., 2023). These advanced capabilities contribute to a more comprehensive understanding of network anomalies, facilitating the automatic generation of granular firewall rules that specifically target detected threats.

### Performance Metrics and Evaluation Criteria

To quantitatively assess the efficacy of these enhanced firewall optimization techniques, a robust set of performance metrics and evaluation criteria is indispensable, ensuring that the developed solutions not only detect threats accurately but also maintain network throughput and minimize latency. Key performance indicators should encompass not only security effectiveness, such as false positive rates and threat detection accuracy, but also operational efficiency, including firewall processing overhead, rule update latency, and impact on legitimate traffic flow (Sharma, 2024). Additionally, metrics like adaptability to evolving threats and scalability across diverse network architectures are crucial for evaluating the long-term viability and robustness of AI-driven firewall solutions.

## System Architecture and Implementation

This section elaborates on the structural design and practical deployment of an AI-driven firewall system, detailing the integration of various components to achieve dynamic optimization and enhanced security.

### Proposed Firewall Optimization System Components

The system is conceptualized as a modular framework comprising several interconnected units, each responsible for a specific aspect of threat intelligence, policy generation, and enforcement (Umoga et al., 2024). This modularity allows for flexible scaling and integration of new AI models and threat intelligence feeds without requiring a complete overhaul of the existing infrastructure (Oloyede, 2024). Core components include a real-time data ingestion module, an AI-powered analytics engine, a policy generation and optimization unit, and a distributed enforcement layer, all orchestrated by a central management and monitoring system.

### Integration with Existing Network Infrastructure

The seamless integration of such an advanced firewall system into existing network infrastructure is paramount, necessitating API-driven interfaces for interoperability with current network devices, security information and event management systems, and orchestration platforms. This integration ensures that the AI-driven firewall operates as an intrinsic part of the network's security ecosystem, leveraging existing data sources and contributing to a unified security posture (Kalantri & Bansode, 2024). Such integration also facilitates the exchange of threat intelligence and policy directives, enabling a more cohesive and automated response to cyber threats across the entire enterprise (Vyas et al., 2025). The adaptive capabilities of such firewalls, particularly their ability to dynamically retrain and adjust security policies, are crucial for effective, real-time threat detection and mitigation in complex network environments.

### Deployment Scenarios

This includes scenarios ranging from enterprise networks and data centers to cloud environments and critical infrastructure, each presenting unique challenges for security policy enforcement and optimization. For instance, a distributed deployment model leveraging containerization and microservices can enhance scalability and resilience, allowing firewall functions to be dynamically provisioned and scaled across various network segments as needed (Farzaan et al., 2024). This modular architecture, particularly when implemented with containerized applications, effectively addresses scalability and administration challenges, ensuring efficient operation even in complex, heavy-workload environments (Farzaan et al., 2024). Furthermore, such advanced deployment models often incorporate hybrid AI frameworks, integrating deep learning, machine learning, and rule-based systems to enhance predictive capabilities in threat detection and response across diverse operational contexts (Mareedu, 2024). This includes bolstering Zero-Trust defense mechanisms to overcome challenges posed by legacy infrastructure and compliance complexities (YALLA, 2024).

## Experimental Setup and Results

This section details the methodologies employed for testing the proposed AI-driven firewall system, outlining the simulated network environments, datasets utilized, and the specific metrics measured to evaluate its performance under various attack scenarios. The validation typically involves simulating real-world traffic conditions using established datasets like UNSW-NB15, enabling an assessment of the system's accuracy, false positive rates, and overall efficiency in processing large volumes of data (Viharika et al., 2025).

### Network Simulation Environment

This environment typically includes virtual machines configured to mimic diverse network topologies and traffic patterns, allowing for comprehensive testing against known and emerging cyber threats. The utilization of Docker-NS3 testbeds, for example, allows for the realistic emulation

of heterogeneous network environments, facilitating evaluation against live traffic scenarios and providing practical insights into system performance (Lodh et al., 2025). This setup permits rigorous analysis under both steady-state and burst traffic patterns, ensuring a thorough assessment of performance across varied conditions (Italina et al., 2025). Such environments are also instrumental in evaluating the efficacy of firewall services based on virtualized unikernels and container technologies, particularly when assessing performance across a wide range of firewall rules from 1 to 100,000 (Kurek et al., 2024). Advanced testbeds, leveraging technologies such as containers, Kubernetes, and eBPF/XDP, are essential for generating diverse and realistic network traffic, thereby enabling comprehensive evaluation of machine learning-based network experiments and providing ground-truth validated datasets (Farasat et al., 2024).

### Test Cases and Data Sets

These datasets are critical for training and validating AI models, encompassing a wide spectrum of network anomalies and attack vectors to ensure the firewall's robust detection capabilities across different threat landscapes (Hernández et al., 2025). Specifically, datasets like CICIDS 2017, UNSW-NB15, and N-BaIoT are frequently employed due to their comprehensive representation of real-world network intrusions, hybrid traffic scenarios, and IoT-focused botnet activities, respectively (Farzaan et al., 2024; Rahmati, 2025). The diversity of these datasets, including RoEduNet-SIMARGL2021, allows for a thorough evaluation of individual machine learning models and ensemble techniques across various intrusion detection scenarios, providing insights into their efficacy and potential for enhancing cybersecurity measures (Bibers et al., 2024; Hussain et al., 2024). These diverse datasets are meticulously constructed to include a wide variety of network activities, such as regular data transmissions, intrusions, and packet loss incidents, thus enabling a thorough evaluation of the framework's performance in preventing cyberattacks and mitigating packet drop incidents (Shreyanth, 2023).

## RESULT AND DISCUSSION

### Performance Evaluation of Optimized Firewalls

Evaluation metrics typically include detection accuracy, false positive rates, and computational overhead, often assessed against benchmarks established by traditional firewall solutions to highlight the advancements offered by AI integration. Furthermore, the integration of explainable AI tools such as SHAP and LIME is essential for not only performance but also for ensuring the interpretability of the model's decisions, which is crucial for real-time threat analysis and system optimization. The effectiveness of such systems is frequently benchmarked using established datasets like NSL-KDD, UNSW-NB15, and CICIoT2023, where advanced methodologies often achieve accuracy rates exceeding 99% and high Matthews Correlation Coefficient values (Bensaoud & Kalita, 2025). This rigorous evaluation ensures the optimized firewalls can reliably distinguish between benign and malicious network activities with high precision, minimizing disruptions while maximizing security posture.

### Comparison with Traditional Approaches

Traditional firewall systems, often relying on static rule sets and signature-based detection, struggle to adapt to sophisticated, rapidly evolving cyber threats, whereas AI-driven approaches offer dynamic, adaptive defenses capable of identifying novel attack signatures and behavioral anomalies (Alsuwaiket, 2025). This adaptability is crucial for real-time monitoring and response, distinguishing AI-powered firewalls as a more robust solution against zero-day exploits and polymorphic malware (Ogunseyi & Thiyagarajan, 2025). Moreover, ensemble learning methods in particular have

demonstrated superior performance in intrusion detection tasks compared to single classifiers, offering enhanced generalization and reduced error rates (Abu Al-Haija & Al-Badawi, 2021; Hewapathirana, 2025). For instance, machine learning models like Random Forest and Neural Networks, when integrated with intrusion detection systems, significantly improve detection accuracy while maintaining low false positive rates compared to traditional rule-based systems.

## Discussion

Furthermore, hybrid AI-driven intrusion detection systems, which integrate techniques such as Principal Component Analysis for feature optimization and Explainable AI for interpretability, have shown significant improvements in detection accuracy and false positive reduction, particularly when tested on datasets like UNSW-NB15. The application of Explainable AI frameworks, such as LIME and SHAP, further enhances these systems by providing transparency into their decision-making processes, thereby increasing trust and enabling human oversight in cybersecurity defenses (Masih et al., 2025; Patil et al., 2022). This interpretability is vital for incident response teams to understand and validate the reasoning behind an intrusion alert, facilitating quicker and more informed mitigation strategies.

### Impact of Enhanced Optimization on Network Security

The strategic integration of optimized firewall solutions significantly bolsters network security posture by enabling proactive threat identification and mitigation, thereby reducing the attack surface and enhancing overall system resilience.

### Scalability and Robustness of the Proposed Solution

The architectural design of these optimized firewalls, often leveraging containerization and microservices, ensures seamless scalability to accommodate increasing network traffic and evolving security requirements without compromising performance or introducing significant latency. This inherent flexibility enables dynamic resource allocation and the rapid deployment of security updates, ensuring continuous protection against emerging threats in large-scale network environments.

### Limitations and Future Directions

While current models demonstrate considerable accuracy, often exceeding 99% in controlled environments, challenges remain in addressing overfitting, computational complexity for real-time deployment, and the demanding requirements for hyperparameter tuning in diverse operational contexts (Pulyala et al., 2023). Moreover, the reliance on labeled datasets restricts applicability where annotated data is scarce, necessitating exploration into unsupervised or semi-supervised learning techniques (Yagiz & Goktas, 2025).

## CONCLUSION

This paper has thoroughly explored the advancements in AI-driven firewall optimization, highlighting their superior adaptability and detection capabilities compared to traditional methods. The integration of sophisticated machine learning algorithms and explainable AI techniques offers a proactive and transparent defense mechanism against an increasingly complex threat landscape. However, despite these advancements, limitations persist, particularly concerning the interpretability, scalability, and real-time processing capabilities of current AI implementations within resource-constrained environments, thus necessitating further research into modular design and robust auditing mechanisms. Future research should also prioritize developing comprehensive,

standardized experimental datasets to reduce inconsistencies and improve model robustness, alongside integrating techno-economic analyses to assess capital and operational costs.

## REFERENCES


Abu Al-Haija, Q., & Al-Badawi, A. (2021). Attack-Aware IoT network traffic routing leveraging ensemble learning. *Sensors*, *22*(1), 241.

Agrawal, G., Pal, K., Deng, Y., Liu, H., & Chen, Y.-C. (2024). Cyberq: Generating questions and answers for cybersecurity education using knowledge graph-augmented llms. *Proceedings of the AAAI Conference on Artificial Intelligence*, *38*(21), 23164–23172.

Ahmad, T. (2025). Ai-driven dynamic firewall optimization using reinforcement learning for anomaly detection and prevention. *ArXiv Preprint ArXiv:2506.05356*.

Ahmadi, S. (2023). Next generation AI-based firewalls: A comparative study. *International Journal of Computer (IJC)*, *49*(1), 245–262.

Ahmadi, S. (2025). Adaptive cybersecurity: Dynamically retrainable firewalls for real-time network protection. *ArXiv Preprint ArXiv:2501.09033*.

Allami, A., Nicewarner, T., Goss, K., Kundu, A., Jiang, W., & Lin, D. (2025). Oblivious and distributed firewall policies for securing firewalls from malicious attacks. *Computers & Security*, *150*, 104201.

Alnfiai, M. M. (2025). AI-powered cyber resilience: a reinforcement learning approach for automated threat hunting in 5G networks. *EURASIP Journal on Wireless Communications and Networking*, *2025*(1), 68.

Alsuwaiket, M. A. (2025). ZeroDay-LLM: A Large Language Model Framework for Zero-Day Threat Detection in Cybersecurity. *Information*, *16*(11), 939.

Alvarado-Molina, M., Curto, A., Wheeler, A. J., Tham, R., Cerin, E., Nieuwenhuijsen, M., Vermeulen, R., & Donaire-Gonzalez, D. (2023). Improving traffic-related air pollution estimates by modelling minor road traffic volumes. *Environmental Pollution*, *338*, 122657.

Arthur, J. K., Kwadwo, E., Doh, R. F., & Mantey, E. A. (2019). Firewall rule anomaly detection and resolution using particle swarm optimization algorithm. *International Journal of Computer Applications*, *975*, 8887.

Becher, T., & Torka, S. (2024). Exploring AI-enabled cybersecurity frameworks: Deep-learning techniques, GPU support, and future enhancements. *ArXiv Preprint ArXiv:2412.12648*.

Bensaoud, A., & Kalita, J. (2025). Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models. *Ad Hoc Networks*, *170*, 103770.

Bibers, I., Arreche, O., & Abdallah, M. (2024). A comprehensive comparative study of individual ML models and ensemble strategies for network intrusion detection systems. *ArXiv Preprint ArXiv:2410.15597*.

Brody, S. L., Pan, J., Huang, T., Xu, J., Xu, H., Koenitizer, J. R., Brennan, S. K., Nanjundappa, R., Saba, T. G., & Rumman, N. (2025). Undocking of an extensive ciliary network induces proteostasis and cell fate switching resulting in severe primary ciliary dyskinesia. *Science Translational Medicine*, *17*(783), eadp5173.

Caprolu, M., Raponi, S., & Di Pietro, R. (2019). Fortress: an efficient and distributed firewall for stateful data plane sdn. *Security and Communication Networks*, *2019*(1), 6874592.

Coscia, A., Dentamaro, V., Galantucci, S., Maci, A., & Pirlo, G. (2023). An innovative two-stage algorithm to optimize Firewall rule ordering. *Computers & Security*, *134*, 103423.

Duan, Q., & Al-Shaer, E. (2025). Firewall Regulatory Networks for Autonomous Cyber Defense. *ArXiv Preprint ArXiv:2505.01436*.

Farasat, T., Kim, J., & Posegga, J. (2024). Advancing network security: a comprehensive testbed and dataset for machine learning-based intrusion detection. *ArXiv Preprint ArXiv:2410.18332*.

Farzaan, M. A. M., Ghanem, M. C., El-Hajjar, A., & Ratnayake, D. N. (2024). Ai-enabled system for efficient and effective cyber incident detection and response in cloud environments. *ArXiv*

*Preprint ArXiv:2404.05602*.

Fuchino, T., Harada, T., Tanaka, K., & Mikawa, K. (2023). Computational complexity of allow rule ordering and its greedy algorithm. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, *106*(9), 1111–1118.

Hashmi, E., Yamin, M. M., & Yayilgan, S. Y. (2025). Securing tomorrow: a comprehensive survey on the synergy of Artificial Intelligence and information security. *AI and Ethics*, *5*(3), 1911–1929.

Hernández, H. A., Mondragón, I. F., González, S. R., & Pedraza, L. F. (2025). Reconfigurable agricultural robotics: Control strategies, communication, and applications. *Computers and Electronics in Agriculture*, *234*, 110161.

Hewapathirana, I. U. (2025). A comparative study of two-stage intrusion detection using modern machine learning approaches on the CSE-CIC-IDS2018 dataset. *Knowledge*, *5*(1), 6.

Hussain, A., Khatoon, A., Aslam, A., & Khosa, M. (2024). A comparative performance analysis of machine learning models for intrusion detection classification. *Journal of Cybersecurity*, *6*, 1.

Ita, K., & Roshanaei, S. (2024). Artificial intelligence for skin permeability prediction: deep learning. *Journal of Drug Targeting*, *32*(3), 334–346.

Italina, C., Boihaki, B., & Iqbal, M. (2025). AI-Driven Risk Management Framework for Decentralized IoT Systems: Integrating Blockchain Technology for Enhanced Security and Trust. *TEM Journal*, *14*(3).

Kalantri, R. A., & Bansode, R. (2024). IoT Attacks, Security Concerns, and Reinforcement Learning Solutions: A Comprehensive Survey. *International Conference on Emerging Research in Computing, Information, Communication, Artificial Intelligence and Machine Learning*, 561–578.

KELVIN, O., ISMAIL, O. S.-O., TRAVIS, A., ADETUTU, T. F., & JOSEPH, O. B. (2024). AI-driven threat intelligence for real-time cybersecurity: Frameworks, tools, and future directions. *OPEN ACCESS RESEARCH JOURNAL OF SCIENCE AND TECHNOLOGY Учредители: Open Access Research Journals Publication*, *12*(2), 40–48.

Klein, T., & Romano, G. (2025). Optimizing Cybersecurity Incident Response via Adaptive Reinforcement Learning. *Journal of Advances in Engineering and Technology*, *2*(1).

Kurek, T., Niemiec, M., & Lason, A. (2024). Performance evaluation of a firewall service based on virtualized IncludeOS unikernels. *Scientific Reports*, *14*(1), 557.

Lekkala, C. (2024). Ai-driven dynamic resource allocation in cloud computing: Predictive models and real-time optimization. *J Artif Intell Mach Learn & Data Sci*, *2*.

Lodh, S., Obaidat, I., Rustam, F., & Jurcut, A. D. (2025). Lightweight Fine-Tuning of LLMS for Explainable Intrusion Detection in SDN. *2025 21th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 1–6.

Lu, N., & Yang, Y. (2020). Application of evolutionary algorithm in performance optimization of embedded network firewall. *Microprocessors and Microsystems*, *76*, 103087.

Maasaoui, Z., Merzouki, M., Battou, A., & Lbath, A. (2025). A Scalable Framework for Real-Time Network Security Traffic Analysis and Attack Detection Using Machine and Deep Learning. *Platforms*, *3*(2), 7.

Mareedu, A. (2024). Hybrid AI Models in Network Security: Combining ML, DL, and Rule-Based Systems. *International Journal of Emerging Research in Engineering and Technology*, *5*(4), 109–121.

Masih, M., Suleman, S., Khan, M. H., Sahito, Z., & Shahid, S. (2025). The future classroom: Integrating AI and social media for adaptive learning. *Inverge Journal of Social Sciences*, *4*(3), 98–111.

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, *67*(8), 6969–7055.

Ogunseyi, T. B., & Thiyagarajan, G. (2025). An explainable LSTM-based intrusion detection system optimized by firefly algorithm for IoT networks. *Sensors*, *25*(7), 2288.

Oh, S. H., Jeong, M. K., Kim, H. C., & Park, J. (2023). Applying reinforcement learning for enhanced cybersecurity against adversarial simulation. *Sensors*, *23*(6), 3000.

Oloyede, J. (2024). Leveraging artificial intelligence for advanced cybersecurity threat detection and prevention. *Available at SSRN 4976072*.

Patil, S., Varadarajan, V., Mazhar, S. M., Sahibzada, A., Ahmed, N., Sinha, O., Kumar, S., Shaw, K., & Kotecha, K. (2022). Explainable artificial intelligence for intrusion detection system. *Electronics*, *11*(19), 3079.

Priya, B. S., Tallam, T., & Kumar, C. N. (2025). Analysing pedestrian-vehicle interaction at unsignalized intersections: A trajectory-based approach. *AIP Conference Proceedings*, *3298*(1), 20028.

Pulyala, S. R., Jangampet, V. D., & Desetty, A. G. (2023). Revolutionizing SIEM with MI-Driven Risk Assessment and Prioritization. *International Journal of Information Technology (IJIT)*, *4*(2), 55–62.

Rahmati, M. (2025). Dynamic role-adaptive collaborative robots for sustainable smart manufacturing: an AI-driven approach. *Journal of Intelligent Manufacturing and Special Equipment*, *6*(2), 101–115.

Sahu, A., Wlazlo, P., Gaudet, N., Goulart, A., Rogers, E., & Davis, K. (2023). A Firewall Optimization for Threat-Resilient Micro-Segmentation in Power System Networks. *ArXiv Preprint ArXiv:2306.15072*.

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1), 105.

Shreyanth, S. (2023). Multi-Sensor Data Fusion-based Parallel Manipulator with IoT Monitoring Employing Machine Learning. *SN Computer Science*, *4*(2), 165.

Smine, M. (2022). *Software-defined security for network function virtualization*. Ecole nationale supérieure Mines-Télécom Atlantique.

Srikanth, B. (2024). Next-Gen Firewalls and Network Security: Enhancing Defense through Advanced Threat Mitigation Techniques. *INTERNATIONAL JOURNAL*, *10*(6), 692–702.

Tallam, K. (2025). From autonomous agents to integrated systems, a new paradigm: Orchestrated distributed intelligence. *ArXiv Preprint ArXiv:2503.13754*.

Umoga, U. J., Sodiya, E. O., Ugwuanyi, E. D., Jacks, B. S., Lottu, O. A., Daraojimba, O. D., & Obaigbena, A. (2024). Exploring the potential of AI-driven optimization in enhancing network performance and efficiency. *Magna Scientia Advanced Research and Reviews*, *10*(1), 368–378.

Viharika, S., Hiranmayee, N., Srilatha, B., Chandu, S., & Nagendra, U. (2025). Comparative Study of Deep Learning Models for Sentiment Classification in YouTube Comments. *2025 8th International Conference on Computing Methodologies and Communication (ICCMC)*, 739–745.

Vyas, R. K., Somani, V., & Dargar, S. K. (2025). Building a Secure IoT Firewall Framework Leveraging Intrusion Detection Technologies. In *Sustainable Materials and Technologies in VLSI and Information Processing* (pp. 37–43). CRC Press.

Yagiz, M. A., & Goktas, P. (2025). LENS-XAI: redefining lightweight and explainable network security through knowledge distillation and variational autoencoders for scalable intrusion detection in cybersecurity. *ArXiv Preprint ArXiv:2501.00790*.

YALLA, M. R. (2024). Zero-trust security architecture in the AI era: a novel framework for enterprise cyber resilience. *International Journal of Science and Research Archive2*, *13*(2), 4341–4356. https://doi.org/10.30574/ijsra.2024.13.2.0172