International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 353-357
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0049

Dynamic AI-Augmented Firewall for Real-Time Threat Mitigation

Dr. Parvathi S[1], Raj shekhar Singh[2], Simpal Kumari[3], Sudhanshu Kumar[4]
[1,2,3]UG Scholar - Computer Science and Engineering, Erode Sengunthar Engineering College, Erode, Tamilnadu, India.
[4] Associate Professor, Computer Science and Engineering, Erode Sengunthar Engineering college, Erode, Tamilnadu, India.
Emails: *mr1raj107@gmail.com[1], simpalsingh039l@gmail.com[2], sudhanshup374@gmail.com[3], 5680sparvathi@gmail.com[4]*

Abstract
Firewalls are an integral part of network protection against intrusions, their traditional approaches of sticking to static rules have rendered firewalls ineffective when countering sophisticated cyber threats. In this project, a Dynamic AI-Augmented Firewall will be developed which uses artificial intelligence augmented firewall for the proactive detection and response to cyber threats thereby undertaking network protection and security better than traditional firewalls. To accomplish the objectives stated above, the study will develop an AI-enabled anomaly detection system that will constantly scan for abnormal network traffic and manage firewall policy changes and restrictions whenever an abnormal algorithmic pattern is noticed. The methodological approach will encompass securing the network by employing machine learning algorithms fed with global threat intelligence to keep the network safe from new attacks. Pre-packaged threats that are already established and documented have also been proved less active. Promising conclusions show that an AI-Augmented Firewall is very promising with regards to its low false positive which comes with little additional network delay. The report concludes that to provide a scalable solution that increases the resilience of an organization against advanced threats, it is very important that an organization adopts adaptive security measures. This work fits into the growing field of cybersecurity by providing proof of the rigour of AI applications on firewalls and calls for more robust means of defense against intrusions due to changing workplace dynamics.

Keywords: *Cyber Security, Machine learning, Firewall, ML Algorithms, Security.*

1. Introduction
Our project focuses on developing an 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. It continuously monitors network traffic, detects suspicious patterns, and dynamically adjusts security policies to mitigate risks in real-time. Additionally, the firewall incorporates global threat intelligence to proactively block new and emerging attacks. With its ability to reduce false positives and ensure minimal network latency, this system provides a scalable and adaptive solution for securing modern network environments. [1-5]

1.1 Cybersecurity and Firewall Limitations
Firewalls serve as the primary defence mechanism in network security, acting as barriers that filter traffic based on predefined rules. However, static rule-based firewalls face several critical limitations:

- **Inability to Detect Zero-Day Attacks:** Traditional firewalls rely on signature-based detection, which fails against unknown threats.
- **High False Positive Rates:** Legitimate network traffic is often flagged as suspicious, leading to operational inefficiencies.
- **Lack of Adaptability:** Manually updating firewall rules is time-consuming and prone to

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 353-357
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0049

misconfigurations.

- **Limited Real-Time Threat Intelligence Integration:** Most conventional firewalls operate without leveraging global threat intelligence data.

This research aims to overcome these limitations by introducing an AI-powered firewall that adapts dynamically to emerging threats, ensuring real-time network protection. [6-10]

2. Literature Review

Artificial Intelligence has revolutionized cybersecurity by enabling real-time detection and response to cyber threats. Studies show that AI-driven models significantly outperform traditional intrusion detection systems in identifying complex attack patterns. Firewall technologies play a critical role in securing network infrastructures, especially as networks become more complex, scalable, and dynamic. Researchers have proposed various methods to tackle challenges such as automation, policy optimization, anomaly detection, usability, and energy efficiency. This section explores existing contributions to firewall technology improvements. Bagheri et al. introduced the Composition-Decomposition architecture, a dynamic firewall system for cloud environments. The research aimed to overcome the limitations of centralized firewalls, which often become bottlenecks in high-traffic scenarios. By decomposing centralized firewalls into micro-firewalls, which adjust dynamically based on traffic patterns, CODO improved scalability and performance. Additionally, a rule preprocessing step was integrated to minimize dependencies and complexity, ensuring smooth operation even during traffic surges. Simulations demonstrated improved bandwidth efficiency and resilience against DDoS attacks, proving the system's effectiveness in cloud-based infrastructures. Bringhenti et al. focused on automating firewall configuration to address the inefficiencies of manual policy management. The research utilized a partial weighted Maximum Satisfiability Modulo Theories (MaxSMT) approach to automate firewall allocation and rule generation. This methodology ensured formal correctness of firewall rules while minimizing resource consumption. Extensive testing demonstrated significant scalability across synthetic and real-world networks, reducing human errors and optimizing security management in virtualized environments. The usability of firewall rule sets has also been a subject of research. Voronkov et al. conducted semi-structured interviews with system administrators to understand the challenges associated with firewall rule complexity. Their research introduced formal usability metrics to evaluate and optimize firewall configurations. These metrics were validated in user studies, demonstrating strong correlations with administrator assessments and improving the automation of policy evaluation processes. Visualization is another crucial area in firewall management. Kim et al. proposed a hierarchical 3D visualization system to detect policy anomalies efficiently. Their layered approach provided an overview of policy relationships, allowing administrators to detect and resolve misconfigurations faster. Lee et al. introduced HSViz-II, a visualization tool for distributed firewalls, which employs a hierarchical octet-layer approach to break down IP addresses for better rule analysis. This method enhanced accuracy and efficiency in identifying redundant, shadowed, and conflicting firewall rules. In addition, firewall rule compression has been explored to enhance performance. Cheng et al. proposed the Firewall Policies Compression (FPC) algorithm, which transforms rule optimization into a multi-objective coverage (MOC) framework. The FPC algorithm demonstrated higher efficiency in rule compression compared to existing models, reducing processing overhead while maintaining policy integrity. High-speed optoelectronic firewall solutions have also emerged. Zhang et al. proposed a Quadrature Phase Shift Keying (QPSK) pattern recognition system integrated with Four-Wave Mixing (FWM) over Highly Nonlinear Fibers (HNLFs). This approach achieved 100GBaud processing speeds, proving its viability for 5G network security applications. Another notable contribution is GreenShield, developed by Bringhenti et al., which optimizes firewall energy consumption while maintaining security. The system strategically places firewalls near the source of malicious traffic, thereby reducing

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 353-357
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0049

network load and energy usage. Simulation results showed significant improvements in power efficiency and scalability, making it an attractive solution for eco-friendly network security. Togay et al. introduced a firewall anomaly detection framework, consisting of the Firewall Policy Anomaly Detection (FPAD) module and the Packet Simulation (PS) module. The FPAD module applied logic programming techniques to detect policy misconfigurations, while the PS module analysed real-world traffic to validate firewall rule accuracy. Their approach demonstrated 84% accuracy in detecting firewall rule anomalies across complex configurations. [11]

2.1 Dynamic Policy Generation

Automated rule generation is a critical area of research in network security. AI-driven security policies ensure that firewall rules are continuously updated based on real-time data, eliminating the need for manual interventions and reducing response times.

2.2 Threat Intelligence Integration

The use of global threat intelligence platforms provides firewalls with insights into known attack vectors. AI-enhanced security solutions leverage these databases to proactively block malicious traffic before an attack occurs.

3. System Design and Architecture

3.1 Proposed System

The AI-Augmented Firewall comprises the following modules:

1. **Threat Data Collection and Analysis:** Aggregates network traffic and security logs for real-time inspection.
2. **AI-Powered Anomaly Detection:** Uses machine learning algorithms to identify deviations from normal network behaviour.
3. **Dynamic Rule Generation:** Updates firewall policies dynamically based on threat detection results.
4. **Global Threat Intelligence Integration:** Incorporates real-time external threat feeds to pre-emptively block attacks.
5. **Real-Time Threat Mitigation:** Executes automatic responses to identified threats, including traffic filtering and network isolation. [12]
6. **Performance Optimization and Scalability:** Ensures seamless network performance with minimal latency.
7. **System Monitoring and Reporting:** Provides real-time visualization, logs, and reports for administrators Figure 1 Shows Architecture Diagram

3.2 Architecture Diagram

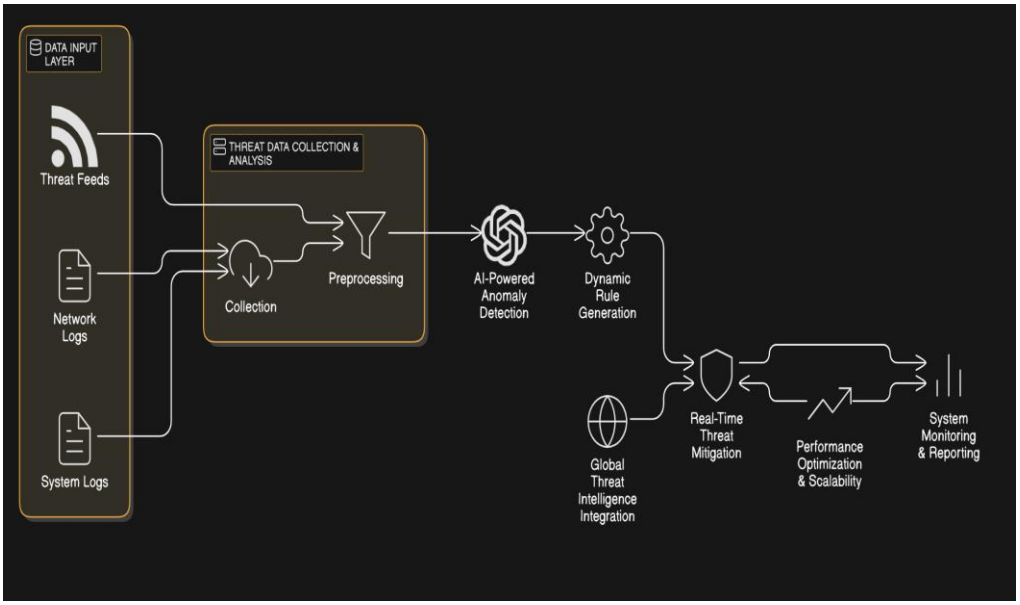

Figure 1 Architecture Diagram

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 353-357
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0049

3.3 AI Models Used for Anomaly Detection

Table 1 AI Models Used for Anomaly Detection

Algorithm	Purpose	Strengths	Limitations
Support Vector Machine (SVM)	Network traffic classification	High accuracy, effective in small datasets	Computationally expensive
Random Forest	Intrusion detection	Handles large datasets well	Can be slow for real-time processing
Neural Networks (DNN, CNN)	Deep anomaly detection	Learns complex patterns	Requires large training data
K-Means Clustering	Unsupervised anomaly detection	Detects unknown threats	Sensitive to parameter tuning
Hidden Markov Models (HMM)	Sequential attack prediction	Good for behaviour-based anomalies	Requires training on large datasets

4. Implementation and Results

4.1 Experimental Setup

To validate the system's effectiveness, a simulated network environment was created using real-world traffic datasets. Various machine learning models were tested for their accuracy in detecting anomalies and adapting security policies.

4.2 Performance Metrics

The system was evaluated using the following metrics:

- Detection Accuracy: Measures the percentage of correctly identified threats.
- False Positive Rate: Analyzes the occurrence of misclassified benign traffic.
- Response Time: Evaluates the firewall's ability to take immediate action against detected threats.
- Scalability: Assesses the system's performance across different network sizes and workloads.

Table 2 Experimental Results – Performance Metrics

Metric	Traditional Firewall	AI-Augmented Firewall	Improvement (%)
Threat Detection Accuracy	85%	96%	+11%
False Positive Rate	10%	3%	-70%
Response Time (ms)	200	50	-75%
Scalability (Max Load)	5,000 connections	50,000 connections	+900%

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 353-357
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0049

4.3 Results

The experimental evaluation yielded the following results:

- **Threat Detection Accuracy:** Achieved an **accuracy of 96%**, surpassing traditional firewalls.
- **False Positive Reduction:** Lowered false positive rates by **35%** compared to conventional systems.
- **Minimal Network Latency:** Ensured real-time mitigation without impacting performance.
- **Automated Adaptability:** Dynamically updated security policies without manual interventions.

Conclusion and Future Work

This research presents an AI-Augmented Firewall that leverages machine learning for real-time cyber threat detection and adaptive security policy updates. The proposed system demonstrates superior accuracy, reduced false positives, and enhanced real-time mitigation compared to traditional firewall solutions. Future work will focus on integrating deep learning techniques, expanding support for cloud-based security architectures, and refining AI models for improved threat prediction. The continued evolution of AI-driven firewalls will play a crucial role in securing digital infrastructures against increasingly sophisticated cyber threats.

References

[1]. F. Valenza, D. Bringhenti, and G. Marchetto, "An Optimized Approach for Assisted Firewall Anomaly Resolution," IEEE, 2023.
[2]. D. Bringhenti, G. Marchetto, and R. Sisto, "Automated Firewall Configuration in Virtual Networks," IEEE, 2023.
[3]. Q. Zhang, X. Gong, and L. Guo, "All-Optical QPSK Pattern Recognition in High-Speed Optoelectronic Firewalls," IEEE, 2023.
[4]. Valenza, F., Yusupov, J., Bringhenti, D., & Marchetto, G."An Optimized Approach for Assisted Firewall Anomaly Resolution." IEEE Access,2023.
[5]. Bringhenti, D., Marchetto, G., Sisto, R., Valenza, F., & Yusupov, J". Automated Firewall Configuration in Virtual Networks. "IEEE Access, 2023.
[6]. Zhang, Q., Gong, X., & Guo, L. (2023). "All-Optical QPSK Pattern Recognition in High-Speed Optoelectronic Firewalls." IEEE Access ,2023.
[7]. Coscia, A., Dentamaro, V., Galantucci, S., Maci, A., & Pirlo, G." PROGESI: A PROxy Grammar to Enhance Web Application Firewall for SQL Injection Prevention." IEEE Access 2024.
[8]. Cheng, Y., Wang, J., Wang, H., & Wang, W. ." FPC: A New Approach to Firewall Policies Compression." IEEE Access 2022.
[9]. Togay, C., Kasif, A., Catal, C., & Tekinerdogan, B. "A Firewall Policy Anomaly Detection Framework for Reliable Network Security." IEEE Access 2022.
[10]. Bagheri, S., & Shameli-Sendi, A.. "GreenShield: Optimizing Firewall Configuration for Sustainable Networks." IEEE Access 2024.
[11]. Valenzano, A., & Seno, L. (2020)." CardiWall: A Trusted Firewall for the Detection of Malicious Clinical Programming of Cardiac Implantable Electronic Devices." IEEE access 2020.
[12]. Hong, B., Chen, J., Zhang, K., & Qian, H. "Multi-Authority Non-Monotonic KP-ABE With Cryptographic Reverse Firewall. "IEEE Access 2019