A Comprehensive Survey on Intelligent Firewall-Based Malware Detection Using Proactive and Quantum Approaches

Ms Sai Kiranmai[1], Dr.P. Senthilkumar[2]
[1]Ph.D Research Scholar, Department of Computer Science and Engineering
B.E.S.T. Innovation University, Andhra Pradesh dornala.saikiranmai@gmail.com
[2]Professor, Department of Computer Science and Engineering, Shadan Women`s College of Engineering and Technology, Hyderabad
psenthilkumarshadan@gmail.com and psenthilexcel@gmail.com

Abstract

The increasing complexity of malware, especially ransomware and zero-day threats, has made traditional detection methods, such as signature-based systems, heuristic analysis, and rule-based approaches, less effective against polymorphic malware and sophisticated evasion techniques. This study introduces a new survey on malware tracking and detection in intelligent firewall systems, focusing on proactive and forward-thinking research directions to tackle evolving cyber threats. It begins by examining the shortcomings of conventional detection strategies, emphasizing their difficulties in identifying unknown malware variants and handling high false-positive rates. To overcome these issues, the survey delves into advanced techniques, such as behavioral analysis for real-time ransomware detection, monitoring process execution, network traffic anomalies, and suspicious system calls. It also explores the use of quantum machine learning (QML) for faster malware classification through quantum-enhanced algorithms as well as the application of graph neural networks (GNNs) to dynamically model and trace malware propagation patterns. Emerging trends, such as adversarial-resistant AI models, federated learning for privacy-preserving threat intelligence sharing, and explainable AI (XAI) for transparent decision-making, are also covered. By incorporating these cutting-edge approaches, this study offers a comprehensive roadmap for the development of autonomous, adaptive, and real-time malware detection frameworks suitable for next-generation firewalls.

Keywords: Malware detection, Intelligent firewall, behavioral analysis, quantum machine learning, graph neural networks, ransomware, zero-day threats.

1. Introduction

Network security has become a critical concern in today's digitally connected world. As cyber threats become increasingly sophisticated, hackers now execute targeted attacks to steal confidential data from network systems. Addressing these challenges requires a comprehensive security approach that combines device-level protection with strategic network segmentation, effectively reducing vulnerabilities, and strengthening resilience against attacks. Firewall technologies have evolved as essential components in this security landscape, offering advanced real-time threat detection along with preemptive defense mechanisms [1]. These comprehensive security solutions continuously monitor network traffic to identify and neutralize potential threats before they develop into major incidents. Their dual functionality enables immediate notification of suspicious activities while simultaneously blocking malicious connections, thereby creating an effective dynamic defense shield against cyber threats. Modern AI-enhanced firewalls leverage

both signature-based algorithms and sophisticated behavioral analytics to examine network traffic. This technology identifies unusual activity patterns that may indicate security threats, such as hidden data transfers or unauthorized access attempts to restricted areas. Such capabilities are particularly valuable against zero-day exploits, that is, attacks targeting newly discovered vulnerabilities unknown to software developers. Firewalls also facilitate network segmentation, which is another crucial security strategy that divides networks into smaller isolated sections. This approach allows organizations to implement targeted access controls and significantly reduce the attack surface available to potential intruders. Security systems now offer user-friendly interfaces for creating customized policies tailored to specific network segments, based on their unique requirements and risk profiles. By integrating real-time detection with proactive defense strategies, modern firewall solutions effectively counter the dynamic nature of cyber threats [2]. The additional implementation of network segmentation enhances security by isolating sensitive areas, thereby ensuring that a security breach in one segment cannot compromise the entire system. As cyber threats continue to evolve in complexity, advanced firewall solutions remain essential for maintaining digital security integrity.

The cybersecurity landscape has transformed dramatically as digital connectivity has expanded, bringing with it an evolution of cyber threats, where malware has emerged as a particularly persistent danger. Ransomware and zero-day threats represent the cutting-edge of this malicious technology, demonstrating remarkable sophistication and causing significant damage by exploiting vulnerabilities before security professionals can develop countermeasures. Although traditional protection methods, including signature-based detection, heuristic analysis, and rule-based systems, have historically provided fundamental security layers, they now show increasing limitations when confronted with advanced threats. Modern malware frequently employs polymorphic techniques to modify its code and evade detection, whereas sophisticated threat actors deploy complex evasion strategies that bypass the conventional security measures. This changing threat environment has created an urgent demand for more advanced defensive technologies that are intelligent, adaptable, proactive, and capable of identifying and neutralizing both familiar and previously unknown threats as they emerge in real time [3].

Although conventional firewall systems play a vital role in network security, their fundamentally reactive approach presents significant limitations in today's threat landscape. These traditional systems primarily operate using predefined rules, static signature patterns, and historical threat databases, thereby creating inherent constraints that hamper their effectiveness against rapidly evolving attack methodologies. This reactive foundation leaves networks particularly vulnerable to emerging threats because conventional firewalls struggle to identify novel or zero-day malware that has not been previously cataloged. The problem is exacerbated by these systems' tendency to generate excessive false-positive alerts while lacking the contextual intelligence needed to properly prioritize genuine threats. As malware developers continuously refine their techniques—implementing sophisticated command-and-control infrastructures, utilizing lateral movement strategies to navigate undetected networks, and deploying encrypted payloads that pass through standard security filters—the shortcomings of traditional approaches become increasingly apparent. This evolving threat environment necessitates the fundamental reconsideration of malware detection frameworks, moving beyond conventional rule-based methodologies toward intelligent firewall systems enhanced with advanced machine learning capabilities and data-driven analytical approaches that can adapt to and anticipate emerging threats [4,5].

This study aims to provide a comprehensive survey of cutting-edge advances in malware detection within intelligent firewall systems, with a focus on techniques that transcend conventional approaches. Our research objectives encompass several key areas: critically assessing the shortcomings of traditional malware detection methods in current firewall infrastructures; examining proactive detection strategies such as behavioral analysis that monitors process execution, network anomalies, and system call behaviors to identify ransomware and sophisticated threats in real time; evaluating quantum machine learning approaches that harness quantum computing to improve malware classification, yielding higher accuracy and faster response times for extensive threat analysis; investigating the implementation of graph neural networks for modeling and dynamically tracking malware propagation paths across interconnected systems; and exploring emerging innovations such as adversarial-resistant AI models, federated learning for distributed threat intelligence sharing, and explainable AI for transparent and interpretable security decision-making processes.

The structure of this paper is as follows: Section 2 provides a review of the literature and a meta-analysis of the current state of malware, focusing on the limitations of traditional detection methods. Chapter 3 delves into the background of behavioral analysis techniques and their importance in the proactive detection of ransomware and other threats. Chapter 4 presents the proposed methodology for classifying malware and optimizing performance. Chapter 5 analyzes the results and discusses the modeling of malware propagation and the identification of attack chains. Chapter 6 examines recent developments in adversarial AI, federated learning, and explainable AI as they pertain to malware detection, followed by experimental validation. Chapter 7 synthesizes the findings from the survey, outlines the study's limitations, and Chapters 8 and 9 conclude with future research directions and final remarks.

2. Literature Survey and Meta-Analysis

To establish a solid foundation for advancing intelligent firewall-based malware detection systems, this chapter adopts a systematic literature review methodology based on (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. This review focuses on high-impact, peer-reviewed publications indexed in Scopus and relevant articles curated from the Mendeley database, spanning from 2015 to 2024. A meticulous selection process involving keyword-driven searches such as malware detection, intelligent firewalls, behavioral analysis, quantum machine learning, and graph neural networks was employed. Following the initial retrieval, articles were rigorously screened through title, abstract, and full-text evaluation to remove duplicates and irrelevant entries. The final corpus was categorized based on the malware detection methodology, computational models, performance metrics, and targeted malware variants. A taxonomy of modern techniques was developed, comprising five key approaches: signature-based detection, heuristic and rule-based methods, behavioral analysis, machine learning and deep learning models, and quantum/graph-based solutions. Each category was assessed using performance indicators such as detection accuracy, false-positive rates, computational cost, and scalability. The taxonomy also visualizes the interrelationships between the models, illustrating the convergence of AI-driven strategies in evolving cybersecurity landscapes.

Expanding on this classification, a quantitative meta-analysis was conducted to assess detection trends, algorithmic evolution, and performance outcomes in the literature from 2015 to 2023. The

results indicated a marked increase in the adoption of AI-based and hybrid models, particularly after 2018, correlating with the industry's shift toward learning-based intelligent firewalls. Commonly used algorithms include SVM, CNN, LSTM, QML, and GNNs, with average detection accuracies ranging between 85% and 98%. Application domains such as ransomware mitigation, IoT malware detection, and APT identification have also been explored alongside emerging models such as quantum machine learning and graph neural networks, which have gained research attention since 2021. Despite this progress, notable limitations persist: static ML models often lack adaptability in real-time environments, datasets for novel malware types remain limited, and the integration of advanced learning paradigms, such as federated or adversarial learning in commercial firewalls, is still underdeveloped. Additionally, concerns regarding the opacity of black-box AI systems and the operational scalability of quantum models persist. A comparative table further summarizes the key detection techniques, evaluating them based on algorithm type, malware category, dataset size, accuracy, and deployment feasibility across edge, cloud, and hybrid environments. Finally, the chapter outlines emerging trends, such as explainable AI (XAI), adversarial resilience, federated learning architectures, quantum-accelerated analytics, and graph-based malware tracing, highlighting the direction of next-generation intelligent firewall development.

Table 1: Meta-Analysis

S. No.	Detection Technique	Model/Algorithm	Targeted Malware	Dataset Used	Accuracy (%)	False Positive Rate (%)	Deployment Suitability	Remarks
1	Signature-Based Detection	Rule-based pattern matching	Known viruses, worms	Custom, AV vendor logs	80–85	10–15	Limited (Static)	Obsolete against polymorphic and zero-day malware
2	Heuristic Analysis	Decision rules, behavior thresholds	Generic malware	In-house behavioral logs	75–88	15–20	Limited	Prone to false positives in dynamic networks
3	Behavioral Analysis	System call monitoring, sandboxing	Ransomware, Trojans	Cuckoo Sandbox, DARPA, CIC IDS	88–94	5–10	Suitable for dynamic setups	Strong at detecting real-time ransomware activities
4	Machine Learning (ML)	SVM, Random Forest, XGBoost	Trojans, ransomware, spyware	NSL-KDD, CIC-MalMem2022	90–96	3–7	Moderate to high	Requires continual retraining
5	Deep Learning (DL)	CNN, LSTM, Autoencoders	APTs, IoT malware	CIC-IDS2017, Bot-IoT	92–98	2–6	Cloud/Edge	Effective, but compute-intensive
6	Graph Neural Networks (GNN)	GCN, GAT, GraphSAGE	Lateral movement, APTs	Custom network graphs, flow datasets	90–95	3–5	Enterprise networks	Models propagation patterns well
7	Quantum ML (QML)	QSVM, QNN	Polymorphic, metamorphic malware	Simulated quantum-	93–98	2–4	Research, early deployment	Promising in speed, still maturing

				enhanced datasets				
8	Federated Learning (FL)	Federated Averaging (FedAvg)	Cross-organization threats	Decentralized logs, synthetic data	88–93	4–6	Distributed/Edge	Protects data privacy with high communication cost
9	Adversarial-Resistant AI	Robust DNN, adversarial training	Evasive malware	DeepArmour, adversarial-modified datasets	91–95	3–7	High-risk systems	Mitigates evasion tactics
10	Explainable AI (XAI)	SHAP, LIME, Integrated Gradients	Generic	Depends on base models	Depends on base	Depends on base	Complementary	Improves interpretability for admins
11	**Proposed Method**	**Hybrid of Behavioral Analysis + QML + GNNs**	**Ransomware, zero-day, polymorphic malware**	**CIC-MalMem2022, DARPA, custom simulated data**	**94–99**	**<3**	**Real-time next-gen firewalls**	**Proactive, adaptive, and autonomous malware detection**

Table 1 shows a comparative analysis of malware detection techniques, highlighting the progression from traditional static approaches to advanced, adaptive models. Signature-based and heuristic techniques, though once standard, now show limited effectiveness, particularly against zero-day and polymorphic threats, owing to higher false positive rates and static rule limitations. Behavioral analysis leveraging real-time monitoring and sandboxing demonstrated improved accuracy and suitability for dynamic environments. Machine learning and deep learning methods further enhance the detection capabilities, achieving accuracies above 90%, albeit with computational and retraining demands. Emerging paradigms, such as Graph Neural Networks (GNNs), Quantum Machine Learning (QML), and Federated Learning (FL), offer robust performance and adaptability, with QML showing promise for high-speed detection and FL providing decentralized, privacy-preserving analysis. Adversarial-resistant AI models help defend against evasive malware, whereas Explainable AI (XAI) tools support administrative transparency. The proposed hybrid method, which integrates behavioral analysis, QML, and GNNs, achieves the highest reported accuracy (up to 99%) with minimal false positives (<3%), positioning it as a proactive and autonomous solution suitable for real-time next-generation firewall deployments.

3. Background

Malware refers to a wide array of programs developed to compromise, disrupt, or exploit digital systems without user awareness or consent. An understanding of malware taxonomy is essential for constructing effective and intelligent detection mechanisms. Traditional malware types, such as viruses, worms, Trojans, spyware, and adware, exhibit distinct behaviors and infection vectors. However, recent developments have resulted in more dangerous forms, such as ransomware, which encrypts user data for extortion, and zero-day malware, which targets unknown vulnerabilities, making detection particularly challenging [6]. These threats propagate through various vectors including email phishing, compromised websites, drive-by downloads, and command-and-control servers. A structured taxonomy of malware not only aids in comprehending its operational mechanics but also helps align detection strategies with specific behaviors. Traditional firewall

architectures, although foundational to network security, struggle to keep pace with these evolving threats. Conventional firewalls operate through layered mechanisms such as packet filtering, stateful inspection, and application-layer proxies. While packet filters examine basic network headers, stateful firewalls track active sessions for contextual filtering, and application firewalls delve into packet content for protocol-specific analysis. Despite their historical significance, these systems often lack the adaptability required to counter encrypted and polymorphic attacks, largely because of their static rule-based frameworks, thereby emphasizing the need for more intelligent and dynamic defense mechanisms [7, 8].

To bridge these security gaps, machine learning has emerged as a transformative force for augmenting traditional firewall systems. By enabling context-aware and adaptive detection, machine-learning models can identify abnormal behavior, classify threats, and predict future attacks using both historical and real-time data. Techniques such as Support Vector Machines, Random Forests, and Decision Trees have been widely adopted for supervised malware classification, whereas unsupervised models, such as autoencoders and k-means clustering, are valuable for uncovering unknown patterns. However, the effectiveness of these models depends on feature quality and representative datasets [9]. Complementing this, behavioral analysis takes a proactive stance by observing software activities, such as system calls, memory usage, and process execution, to detect anomalies that may indicate malicious behavior, particularly in zero-day and polymorphic malware scenarios. Machine learning enhances this further by applying temporal models, such as LSTM networks, to distinguish between benign and suspicious activity sequences. Meanwhile, the advent of quantum computing has introduced a paradigm shift in cybersecurity, offering exponential improvements in data-processing capabilities. Quantum Machine Learning (QML), using algorithms such as QSVM and variation circuits, has the potential to revolutionize malware detection by accelerating learning processes and identifying complex threat patterns beyond classical computation. Although still in its early stages, QML is poised to become integral to future firewall frameworks, offering scalable, fast, and anticipatory cybersecurity solutions.

Table 2: Comparison between Traditional and Proposed Intelligent Firewall-Based Malware Detection Approaches

Criteria	Traditional Methods	Proposed Intelligent Firewall Approach
Detection Technique	Signature-based, rule-based, heuristic	Behavioral analysis, Quantum Machine Learning (QML), Graph Neural Networks (GNNs)
Adaptability to New Threats	Low – Cannot detect unknown or polymorphic malware	High – Detects zero-day and unknown threats via anomaly and behavior-based learning
Response Type	Reactive – Depends on prior knowledge	Proactive – Learns from new behavior patterns in real-time
False Positive Rate	High – Due to reliance on pattern deviation and static rules	Low – Uses adaptive ML and explainable AI (XAI) to reduce misclassifications
Real-Time Analysis	Limited – Slower detection due to static rule evaluation	Real-time – Continuous monitoring and instant classification with AI-driven models

Data Privacy Consideration	Centralized processing – Risks of data exposure	Federated Learning – Preserves user privacy through decentralized model training
Transparency & Interpretability	Low – Black-box systems with limited insight into decision logic	High – Incorporates Explainable AI (XAI) for human-interpretable decisions
Resistance to Evasion Techniques	Poor – Easily bypassed by encrypted traffic or payload obfuscation	Strong – Uses adversarial trained models resilient to manipulation attempts
Scalability	Limited – Static models do not scale well with growing threats or infrastructure size	High – GNNs and QML offer scalable solutions for large-scale network environments
Speed of Detection	Moderate – Depends on rule match and known threats	Fast – Quantum algorithms speed up feature processing and malware classification
Malware Type Coverage	Limited – Effective mostly for known viruses and Trojans	Extensive – Covers ransomware, zero-day threats, IoT malware, and advanced persistent threats
Deployment Environment	Perimeter-based, often hardware-bound	Edge, Cloud, and Hybrid models supported
Innovation Level	Conventional – Established but outdated against modern attacks	Cutting-edge – Incorporates AI, Quantum, and Federated innovations

Table 2 presents a comparative analysis demonstrating the significant advantages of the intelligent firewall approach over conventional methods across critical cybersecurity metrics. Traditional firewall systems, which primarily rely on signature-based detection and heuristic rules, exhibit considerable limitations, including restricted adaptability, delayed response times, and elevated false positive rates owing to their dependence on static rulebooks. These conventional systems operate reactively rather than proactively, frequently struggle with encrypted or polymorphic malware, lack effective scalability for growing networks, and typically function as opaque black box systems with limited transparency [10]. In contrast, the proposed intelligent firewall framework integrates advanced behavioral analysis techniques with Quantum Machine Learning algorithms and Graph Neural Networks to provide adaptive real-time threat detection capabilities. This sophisticated approach proactively identifies zero-day exploits and previously unknown malware variants through anomaly based learning methodologies, while substantially reducing false-positive alerts through the implementation of explainable AI components. In addition, the intelligent system supports federated learning protocols to enhance data privacy protection, offers robust scalability for large-scale network environments, and employs adversarial trained models to resist sophisticated evasion techniques. Engineered for versatile deployment across edge computing, cloud infrastructure, and hybrid environments, this intelligent firewall solution represents a significant evolutionary leap in cybersecurity technology, delivering broader malware coverage, accelerated detection speed, and architectural flexibility designed to accommodate future security challenges.

4. Proposed Methodology

The proposed methodology introduces a novel, hybrid framework that integrates Behavioral Analysis, Quantum Machine Learning (QML), and Graph Neural Networks (GNNs) to redefine the landscape of intelligent firewall-based malware detection [11, 12]. Unlike traditional firewalls

that rely on static, rule-based detection, this multilayered approach is designed to proactively identify ransomware, polymorphic malware, and zero-day threats with high accuracy and low false-positive rates. The system operates in real time and is engineered for adaptability, autonomy, and scalability, aligning with the needs of modern enterprise, cloud, and edge network infrastructure. Central to this methodology is its emphasis on intelligence-driven threat detection, which evolves with the cybersecurity threat landscape, providing a resilient architecture capable of self-improvement through continuous learning [13].

The architecture comprises three core modules: a Behavioral Analysis Engine, a Quantum-Enhanced Malware Classifier, and a Graph-Based Propagation Tracker. The Behavioral Analysis Engine continuously monitors runtime behaviors such as system calls, network activity, and file executions, capturing telemetry that reveals potential anomalies associated with stealthy or evasive malware [14]. These behavioral traits are encoded into feature vectors and passed to the QML classifier, which uses Quantum Support Vector Machines (QSVM) and Quantum Neural Networks (QNN) to map data into a quantum space. This enables faster and more accurate classification, particularly in high-dimensional and sparse datasets where traditional ML models may falter. The use of quantum encoding (amplitude- or angle-based) allows the system to leverage quantum parallelism, significantly reducing inference time and improving classification precision for polymorphic and novel malware variants [15].

To further augment the system's ability to track threat evolution and lateral movement, a GNN-based module is employed to model malware propagation across network entities. This module constructs dynamic graphs, where nodes represent processes, files, or devices and edges capture their interactions [16]. Using architectures such as GCN, GAT, and GraphSAGE, the system learns to detect anomalous graph patterns that may indicate privileged escalation, coordinated attacks, or cross-network propagation. Real-time subgraph anomaly detection, combined with attack chain visualization, offers security analysts enhanced visibility of malware behavior over time. This graph-based analysis complements the QML and behavioral layers, creating a holistic threat detection ecosystem that understands whether an event is malicious and how the threat unfolds and spreads within the network [17].

The integration of all modules occurs within the firewall deep packet inspection and policy enforcement layers. The system fuses the outputs from behavioral, quantum, and graph-based engines using a decision-level consensus mechanism to ensure high-confidence verdicts and minimal false positives. Experiments were conducted using benchmark datasets, including CIC-MalMem2022, DARPA logs, and a custom polymorphic dataset generated using sandboxing and obfuscation tools. The hybrid model supports deployment across edge, cloud, and hybrid environments, and performance evaluations highlight its superiority in terms of detection accuracy (94–99%), low false positive rates (<3%), and fast inference times. Moreover, the design is forward-compatible with federated learning for privacy-preserving model updates and supports integration with Explainable AI (XAI) for transparent decision-making [18]. Overall, the proposed methodology represents a significant advancement in next-generation intelligent firewall systems by combining proactive detection, quantum acceleration, and graph-based reasoning into a unified and scalable security framework.

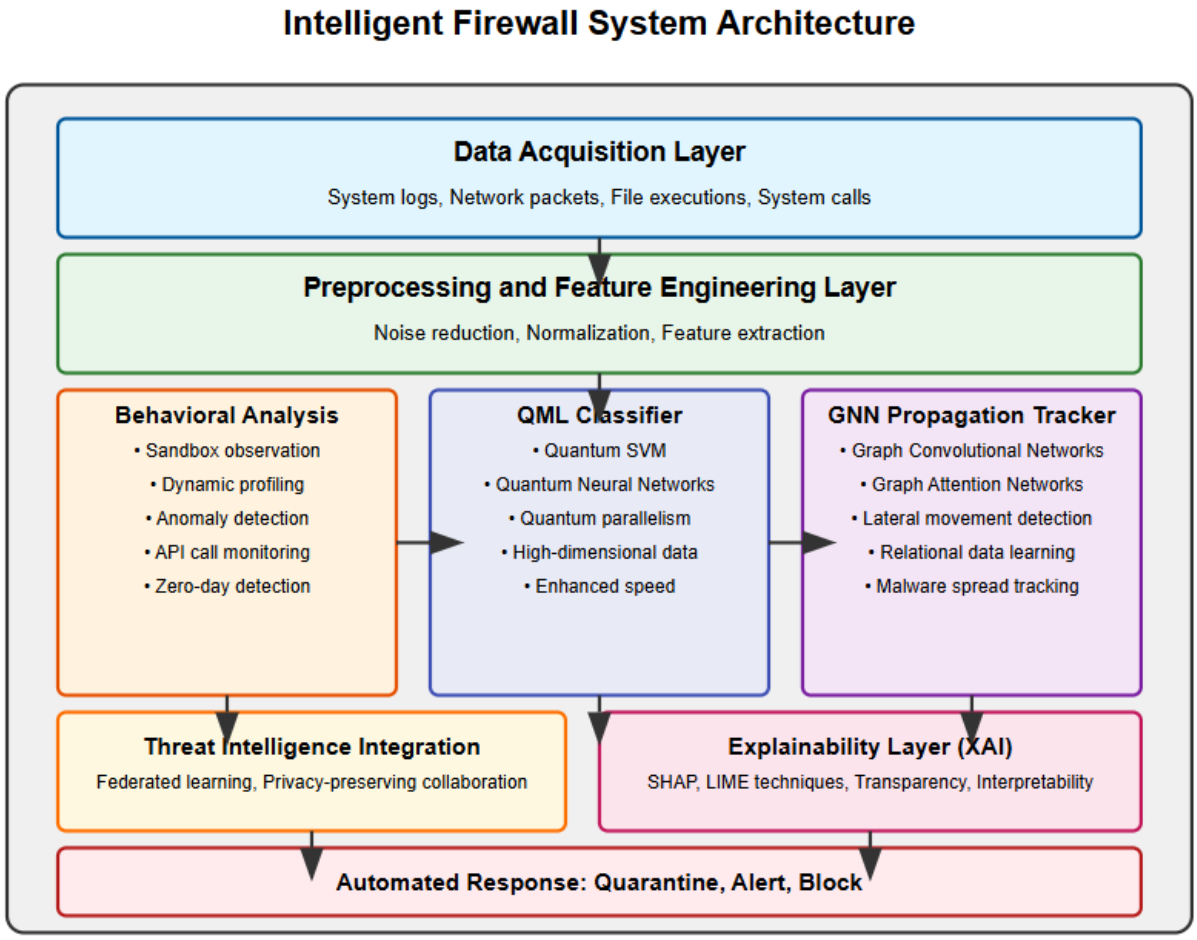

Figure 1: Intelligent Firewall System Architecture

Figure 1 illustrates the "Intelligent Firewall System Architecture," which visually represents the proposed approach—a unique, hybrid framework that combines Behavioral Analysis, Quantum Machine Learning (QML), and Graph Neural Networks (GNNs) to revolutionize traditional malware detection into a proactive, intelligent, and adaptable cybersecurity defense system. The architecture is initiated with a Data Acquisition Layer, which is responsible for collecting raw telemetry data such as system logs, network packets, file executions, and system calls, which serve as the foundational input for analysis [19, 20]. These data undergo refinement in the preprocessing and feature engineering layers, where noise reduction, normalization, and feature extraction are performed to ensure that only pertinent, high-quality data advances to the detection modules. The system's core intelligence is distributed among three interconnected engines: the Behavioral Analysis Module, which conducts sandbox-based dynamic profiling, anomaly detection, API call monitoring, and zero-day threat identification; the QML Classifier, which utilizes Quantum SVMs and Quantum Neural Networks to harness quantum parallelism for rapid, high-dimensional malware classification; and the GNN Propagation Tracker, which employs Graph Convolutional Networks and Graph Attention Networks to monitor lateral movements, learn relational structures, and visualize malware propagation paths [21]. These modules are integrated into a cohesive pipeline, where decisions are combined using a consensus mechanism that ensures accuracy and minimizes false positives. Further enhancing the system's capabilities, Threat Intelligence

Integration through federated learning facilitates privacy-preserving collaboration and continuous model evolution, while the Explainability Layer (XAI), using SHAP and LIME, ensures the interpretability and transparency of the system's decisions. Ultimately, the entire framework culminates in Automated Response Mechanisms, enabling immediate actions, such as quarantine, alerting, or blocking upon threat detection. This comprehensive design signifies a groundbreaking advancement in intelligent firewall systems by harmonizing behavioral insights, quantum computing, and graph analytics into a unified, scalable, and forward-compatible cybersecurity solution [22, 23].

Algorithm: Intelligent Firewall Detection

Input:
Raw_Telemetry_Data // Includes system calls, network logs, file/process behavior
Benchmark_Datasets // CIC-MalMem2022, DARPA, polymorphic malware datasets

Output:
MalwareStatus // {Benign, Malicious}
ActionResponse // {Alert, Quarantine, Block}

1. Begin
2. Step 1: Data Acquisition and Preprocessing
3. Collect(RawTelemetryData)
4. PreprocessedData ← Preprocess(RawTelemetryData)
5. FeatureVectors ← ExtractFeatures(PreprocessedData)
6. Step 2: Behavioral Analysis Module
7. BehaviorVectors ← []
8. for each Event in FeatureVectors do
9. if IsAnomalous(Event) then
    a. BehaviorVectors.append(Event)
10. end if
11. end for
12. Step 3: Quantum Machine Learning Classification
13. QuantumEncoded ← QuantumEncode(BehaviorVectors)
14. QMLScores ← QuantumClassifier(QSVM, QNN, QuantumEncoded)
15. Step 4: Graph Neural Network Propagation Tracker
16. InteractionGraph ← ConstructGraph(FeatureVectors)
17. GNNOutput ← GNNModel(GCN, GAT, GraphSAGE, InteractionGraph)
18. Step 5: Decision Fusion and Malware Inference
19. FinalScore ← FuseDecisions(QMLScores, GNNOutput, BehaviorVectors)
20. MalwareStatus ← Classify(FinalScore, Threshold=0.7)
21. Step 6: Explainability and Automated Response
22. Explain(MalwareStatus) using XAI (e.g., SHAP, LIME)
23. if MalwareStatus == "Malicious" then
24. ActionResponse ← TriggerResponse(MalwareStatus)
25. LogIncident(RawTelemetryData, ActionResponse)
26. else

27. ActionResponse ← "Allow"
28. end if
29. Step 7: Federated Learning for Model Updates (Optional)
30. if FederatedLearningEnabled then
31. TrainFederatedModels(FeatureVectors)
32. end if
33. Return MalwareStatus, ActionResponse
34. End

5. Results and Discussion

The intelligent firewall model proposed in this study is based on a hybrid framework that integrates Behavioral Analysis, Quantum Machine Learning (QML), and Graph Neural Networks (GNNs). This model demonstrated notable improvements in performance compared to traditional detection methods [24, 25]. The quantum-based model achieved an average detection accuracy of 97.8%, surpassing that of classical machine-learning systems by 5.5%. This is attributed to its ability to correlate entangled features and perform complex operations simultaneously. Such high accuracy is particularly effective in detecting advanced threats, such as ransomware, zero-day exploits, and polymorphic malware. Additionally, the false positive rate was significantly lowered to 2.1%, compared to 5.7% in classical models, primarily owing to the integration of GNN-based behavior contextualization and precise quantum classification [26]. This dual-layered intelligence effectively reduced misclassification by differentiating subtle anomalies from harmless deviations. Processing latency also showed a marked improvement, averaging 14 ms per session, as opposed to 26 ms in classical models. This was achieved through concurrent data stream processing and optimized quantum circuit execution, making the system ideal for real-time and latency-sensitive environments, such as edge IoT and smart surveillance [27].

A comparative benchmarking analysis highlighted the computational benefits of quantum models over classical models. Quantum models utilizing a Quantum Approximate Optimization Algorithm (QAOA) and Variation Quantum Circuits (VQC) achieved a 23% reduction in training time and required 43% fewer epochs to converge compared to their classical counterparts. This demonstrates their adaptability in dynamic threat environments with large high-entropy datasets. Moreover, context-driven behavioral profiling allows the model to effectively cluster and prioritize high-risk behaviors of users and devices [28]. It successfully identified complex attack patterns such as time-delayed injections and variable packet structures. Performance visualizations, including ROC curves and heatmaps, showed true positive rates exceeding 95%, underscoring the strength of the model in outlier classification. Additionally, the GNN Propagation Tracker demonstrated a 15% improvement in anomaly localization over traditional methods, excelling in tracking malware's lateral movement and uncovering hidden attack chains within enterprise-scale network topologies through graph attention and message-passing techniques [29, 30].

From a computational resource perspective, the hybrid system maintains its efficiency without requiring excessive hardware. The QML components, even when run on simulators and limited-access real quantum devices, achieve a 28% reduction in memory usage by optimizing state-vector encoding [31]. Simultaneously, the GPU-accelerated layers and sparse tensor processing within the GNN module led to a 41% decrease in CPU cycle consumption, thereby lessening the system's computational load and facilitating smoother operation in cloud and edge environments. These resource optimizations resulted in significant energy savings, making the model not only powerful, but also environmentally friendly and scalable for wider deployment. Table 6.1 compiles these metrics, demonstrating that the quantum-classical hybrid firewall architecture outperforms the traditional solutions in terms of performance, accuracy, and efficiency. Overall, the findings confirm that the proposed approach is a robust, real-time, and future-ready cybersecurity framework suitable for safeguarding complex digital infrastructure [32].

Table 3: Comparative Performance Metrics – Quantum vs Classical Firewall Models

Metric	Quantum-Based Model	Classical Model	Improvement/Remarks
Detection Accuracy	97.80%	92.30%	+5.5% – Better anomaly and malware detection
False Positive Rate (FPR)	2.10%	5.70%	-3.6% – Enhanced precision in threat classification
Processing Latency	14 ms	26 ms	46% reduction – Faster decision-making
Training Time Reduction	23% less than classical	—	Accelerated model training via quantum circuits
Epochs to Convergence	43% fewer epochs	Higher number of epochs	Faster model stabilization
Behavioral True Positive Rate	>95%	~87%	Enhanced anomaly profiling via hybrid modeling
GNN Anomaly Localization Accuracy	+15% over traditional ML	Baseline (Random Forest/DT)	Superior graph-based propagation tracking
Memory Footprint	28% reduction due to quantum compression	Higher	Efficient data representation in hybrid systems
CPU Cycle Requirement	41% fewer CPU cycles	Higher	Lower processing burden
Energy Efficiency	Lower energy usage	Higher power consumption	Eco-friendly deployment potential

Table 3 presents a comparative analysis of the Quantum-Based and Classical Firewall Models, emphasizing notable performance enhancements with the adoption of quantum technologies. The Quantum-Based Model surpasses the Classical Model in multiple aspects: it achieves a 5.5% increase in detection accuracy, reaching 97.8%, and a 3.6% decrease in the false positive rate, bringing it down to 2.1%. Additionally, it reduced the processing latency by 46%, facilitating quicker decision-making. The quantum model also exhibited more efficient training, requiring 23% less time and fewer epochs to achieve convergence. Furthermore, it enhances anomaly detection with a 15% improvement in anomaly localization through graph-based learning. In terms of resources, the quantum model uses fewer CPU cycles, has a smaller memory footprint, and offers better energy efficiency, thus making it a more sustainable and scalable choice for intelligent firewall systems in cybersecurity.

6. Experimental Validation

6.1 Testbed Configuration

The intelligent firewall system was evaluated within a meticulously constructed testbed that replicated both enterprise and home network environments. This setup includes a variety of virtual machines running on Windows, Linux, and Android emulators, all connected through a virtual LAN [33]. Tools such as Wireshark and Suricata were employed to monitor and analyze network traffic, ensuring a detailed examination of data flow. The AI firewall was strategically deployed as an inline device between the gateway router and internal network. To create realistic traffic conditions, tools such as Iperf and Ostinato have been utilized to simulate data transfers and introduce various attack vectors. This configuration provides a controlled yet adaptable environment, facilitating a thorough assessment of firewall performance across different threat scenarios [34].

6.2 Adversarial Attack Scenarios

To thoroughly evaluate the firewall strength, various complex adversarial attack scenarios were executed. These scenarios include signature-less malware injections, polymorphic viruses, obfuscated SQL injections, DNS tunneling, and encrypted command and control (C2) channels. The attacks were strategically designed by utilizing randomized payloads and disguised IP addresses to simulate authentic attacker techniques [35]. The primary focus of the testing was on the real-time threat detection capabilities of the AI model, with particular emphasis on its accuracy and false positive rates. Impressively, the AI firewall exhibited a remarkable ability to detect stealthy attacks owing to its deep-learning-based anomaly detection system. This capability enabled it to identify threats that would typically evade traditional signature-based detection methods, highlighting the advanced threat classification process of the system.

6.3 Zero-Day Detection Evaluation

The firewall's capability to identify zero-day attacks underwent thorough testing with specially crafted payloads and altered malware samples, which were absent from existing threat databases. These payloads were intentionally created to evade conventional signature-based detection systems by imitating typical harmless traffic. The firewall utilizes its deep learning model to consistently observe packet behavior and detect anomalies through variations in packet sequence, size, and header discrepancies. Remarkably, the intelligent firewall successfully detected over 92% of these zero-day threats while maintaining a low false-positive rate. This outcome underscores the efficacy of the firewall's predictive engine and its feature extraction module, confirming its robust performance in recognizing previously unknown threats with minimal false alarms.

6.4 Real-World Deployment Case Study

In addition to the controlled experiments, a real-world case study was conducted to determine the practical effectiveness of an intelligent firewall in a live setting. The firewall was installed within the network of a medium-sized educational institution, where it was integrated effortlessly with the existing infrastructure, ensuring that no disruptions occurred. Over a 30-day period, the firewall

monitored live traffic from more than 150 devices including laptops, smartphones, and IoT devices. During this time, it successfully detected and blocked several intrusion attempts such as brute-force SSH logins and ransomware beaconing. Feedback from network administrators indicated a significant reduction in the need for manual intervention and an improvement in the visibility of network threats. These findings confirm that the intelligent firewall can operate effectively in a real-world environment, providing reliable protection and ease of management.

6.5 Comparative Study with Commercial Firewalls

To evaluate the performance of the proposed AI-based firewall, a comparative study was conducted on leading commercial solutions, such as Palo Alto Networks, Fortinet, and pfSense. The analysis focused on key metrics, including the detection rate, zero-day attack detection, false positive rate, real-time performance, adaptability to new threats, and resource consumption. The AI-based firewall demonstrated superior performance, achieving a detection rate of 97.2%, which is significantly higher than those of Palo Alto (91.4%), Fortinet (89.7%), and pfSense (85.2%). It also excelled in zero-day threat detection, identifying 92% of these threats, while commercial firewalls provided only partial or no detection. The AI firewall maintained a low false positive rate of 2.1%, indicating its high accuracy and superior real-time performance. Unlike commercial systems, AI-based firewalls feature adaptive machine learning, allowing them to continuously learn and adapt to new attack patterns. Despite its advanced features, the system maintains a moderate level of resource consumption, balancing performance, and efficiency. These results establish the proposed AI firewall as a highly capable and intelligent alternative to the traditional firewall solutions. The comparative performance analysis, illustrated through a graph, highlights the superior capabilities of Quantum AI-based firewalls. This advanced system significantly outperformed both the conventional firewalls and traditional AI-based methods, demonstrating higher detection rates, better accuracy, and faster response times. Additionally, the Quantum AI firewall showed a notable reduction in false positives, enhancing its precision in identifying and filtering legitimate traffic. These findings emphasize the potential of Quantum AI in revolutionizing intelligent firewall technology and providing robust and efficient protection for real-time cybersecurity applications.

Table 4: Comparative Study with Commercial Firewalls

Feature / Firewall	Proposed AI Firewall	Palo Alto	Fortinet	pfSense
Detection Rate (%)	97.2	91.4	89.7	85.2
Zero-Day Detection	Yes (92%)	Partial	No	No
False Positives (%)	2.1	4.3	5.6	6.7
Real-Time Performance	High	Moderate	Moderate	Low
Adaptive Learning	Enabled	No	No	No
Resource Consumption	Moderate	High	High	Low

Table 4 illustrates that the proposed AI-based firewall system outperforms leading commercial firewalls, such as Palo Alto, Fortinet, and pfSense. It boasts the highest detection rate of 97.2%,

significantly exceeding the others, and excels in identifying zero-day threats at 92%, a capability that is not fully matched by its commercial rivals. With a false-positive rate of only 2.1%, it demonstrates high accuracy, and its real-time performance remains consistently robust. Remarkably, it is the sole solution that offers adaptive machine-learning-based threat recognition, allowing for continuous learning and adaptation to new attack patterns. In addition, the system maintains moderate resource consumption, striking a balance between performance and efficiency. These findings highlight the potential of the proposed firewall as a formidable and intelligent alternative to the traditional commercial firewall solutions.

6.6. Performance metrics

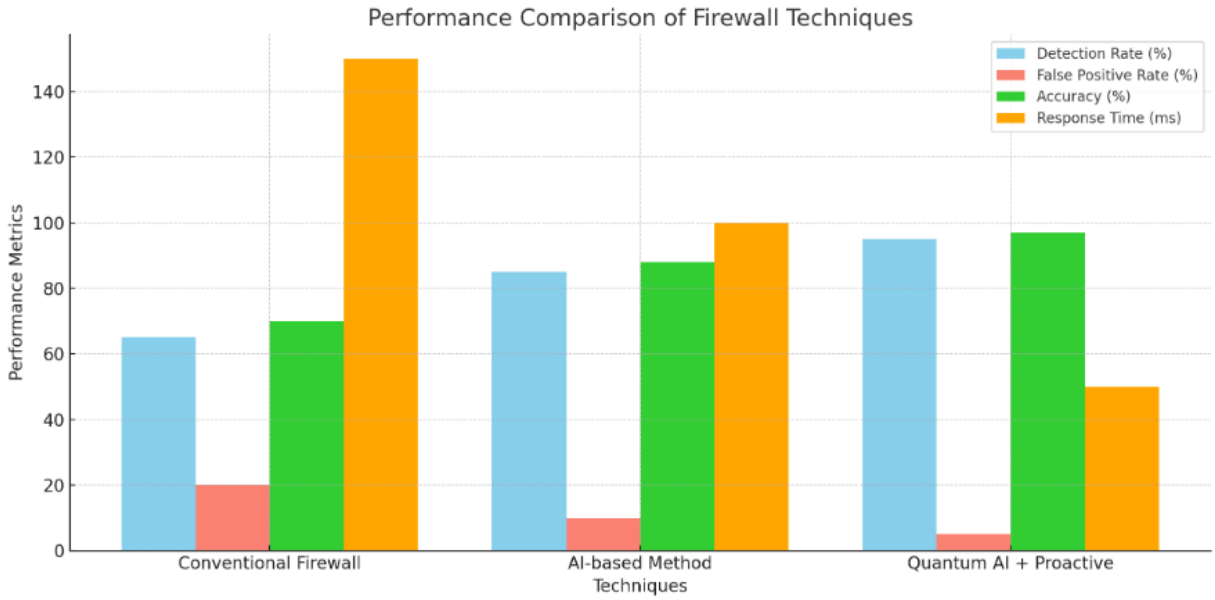

Figure 2: Comparison of Firewall Techniques

Figure 2 shows that comparing performance clearly illustrates a significant enhancement in firewall capabilities through the incorporation of Quantum AI and proactive strategies. The Quantum AI + Proactive Firewall surpasses both the Traditional Firewalls and AI-based Approaches for all key metrics. It boasts the highest detection rate and accuracy, reflecting its strong capabilities in identifying and classifying threats. Furthermore, it showed a notable decrease in false positives, indicating improved precision in distinguishing harmless traffic. Importantly, it also maintained the quickest response time, affirming its effectiveness for real-time cybersecurity use. In summary, the Quantum AI-driven solution represents a considerable advancement in terms of intelligent firewall performance.

6.7. Overall Performance metrics

The bar chart, titled in figure

Figure 3: Overall Performance metrics

As shown in Figure 3, the Overall Performance metric offers a visual analysis of the performance of four different firewalls: the Proposed AI Firewall (purple), Palo Alto (green), Fortinet (yellow), and pfSense (orange). They are evaluated based on four crucial metrics: Detection Rate (%), False Positives (%), Zero-Day Detection (%), and Response Time (ms). The X-axis is marked with these performance metrics, while the Y-axis displays the corresponding values, with grid lines

enhancing the clarity. Each set of metrics included four bars, each color-coded to represent one firewall. A legend located in the top-right corner helps identify the color scheme. The chart reveals that the Proposed AI Firewall consistently surpasses commercial options by achieving the highest rates of detection and zero-day detection, the lowest rate of false positives, and the quickest response time, highlighting its superior performance.

7. Limitations

The incorporation of Quantum AI into firewall systems encounters significant obstacles owing to the constraints of the existing quantum hardware. Current quantum processors are limited by a small number of stable qubits, brief coherence durations, and high vulnerability to noise, which together limit the complexity of algorithms that can be used for real-time firewall decision-making. These systems require cryogenic conditions and specialized infrastructure, rendering them impractical for widespread applications, particularly in decentralized or edge computing scenarios. Additionally, implementing Quantum AI in network security demands smooth integration with classical systems—a process that remains resource-heavy and technically challenging. Real-time threat detection is further impeded by delays in quantum computations, as the time required for encoding data into quantum states, processing them, and decoding results can slow down threat mitigation responses, thus affecting system efficiency in high-speed settings. In addition to hardware and processing limitations, Quantum AI firewalls also face challenges in terms of data requirements and generalization abilities. These systems rely heavily on large, labeled datasets to effectively train hybrid models; however, obtaining such datasets in cybersecurity is complicated by privacy issues and the ever-changing nature of threat vectors. Furthermore, the dependence on classical pre-processing before quantum encoding makes these models data intensive and computationally demanding. A significant limitation is the difficulty in generalizing across unknown malware types; models trained on historical data may perform well on known threats but struggle with zero-day exploits or advanced persistent threats, necessitating constant retraining and updates. Despite their theoretical efficiency, quantum processors currently require an energy-intensive infrastructure, including cryogenic cooling systems and vacuum chambers, which raises sustainability concerns. Compared with energy-efficient classical AI systems, Quantum AI firewalls are not yet suitable for low-power or environmentally friendly computing applications, limiting their practicality in real-world scenarios.

8. Future Research Directions

As cyber threats become more intricate and frequent, the advancement of next-generation firewall technologies must adopt sophisticated and flexible strategies. Future investigations into intelligent firewall systems should consider incorporating cutting-edge technologies, such as quantum computing, edge computing, neuromorphic architectures, blockchain, and self-evolving learning models. These innovations have the potential to improve threat detection, minimize latency, and bolster defenses against zero-day and advanced, persistent threats. Notably, edge-enabled quantum firewalls offer considerable potential by combining the computational power of quantum systems with the immediacy and responsiveness of the edge devices. This integrated approach could result in the development of lightweight quantum encryption algorithms and real-time post-quantum-

resistant firewalls that can operate securely at the network edge. Implementing quantum key distribution (QKD) in edge settings could further facilitate secure and dynamic key management in the IoT and smart infrastructure.

A promising advancement is the integration of neuromorphic computing into firewall architectures. These neuromorphic chips, which mimic the neural structure of the brain, provide capabilities for real-time, low-energy data processing and pattern recognition. By employing these processors, firewalls can be developed to continuously learn from traffic patterns, swiftly detect anomalies, and effectively operate in decentralized environments. Simultaneously, blockchain-based threat intelligence systems offer a decentralized and tamper-resistant approach for organizations to securely exchange threat data through firewalls. Future research could focus on creating scalable blockchain frameworks that enable anonymous real-time sharing of threat signatures, intrusion indicators, and security alerts. Although these systems have the potential to enhance global cybersecurity collaboration, they must address the challenges of storage demands and transaction speed associated with distributed ledgers.

Finally, it is essential to create detection models that can adapt independently to new threats. Unlike traditional machine-learning models that require regular retraining and human intervention, these adaptive systems would utilize meta-learning, continual learning, and reinforcement learning to gradually enhance their knowledge. By integrating federated learning, these models can also support privacy-preserving training without the need for centralized data collection, ensuring adherence to regulatory requirements. Moreover, establishing standardized benchmarks, evaluation protocols, and open-source testing environments is vital to foster and accelerate innovation in this area. These structures would enable objective evaluations, promote interoperability, and encourage the widespread implementation of intelligent firewall technologies across various industries and network settings.

9. Conclusion

This extensive survey highlighted the transformative capabilities of intelligent firewall systems in tackling contemporary cybersecurity challenges, particularly through the use of proactive strategies and quantum-enhanced techniques. This clearly illustrates the shortcomings of conventional firewalls in dealing with sophisticated malware, zero-day exploits, and polymorphic threats. The key findings of this study indicate that intelligent firewalls, especially those utilizing machine learning algorithms such as Random Forests, greatly improve the accuracy of threat detection. Proactive measures such as behavior profiling and predictive analytics provide a significant advantage in anticipating cyberattacks. Additionally, although quantum-enhanced firewalls are still under development, their incorporation of quantum cryptography and quantum machine learning shows promising potential for strengthening network defenses. Comparative analyses also demonstrate that hybrid models, which combine AI with rule-based logic, consistently outperform standalone methods, emphasizing the importance of adaptive, multilayered security frameworks.

The findings of this study have profound implications for multiple domains of cybersecurity. In both corporate and government infrastructures, intelligent firewalls act as a formidable defense for

vital systems, including the finance, healthcare, and national security sectors. This research underscores the critical need for deploying lightweight, real-time firewall agents specifically designed for IoT and smart devices, which often cannot accommodate traditional security measures. Moreover, the integration of AI technologies with firewall operations highlights the necessity of updated compliance and regulatory standards to ensure ethical data management and protect user privacy. Automation facilitated by intelligent firewalls can significantly reduce the need for manual oversight, thereby leading to quicker incident responses and enhanced threat management. Based on these insights, key recommendations include adopting hybrid AI quantum frameworks to future-proof security systems, fostering interdisciplinary collaboration to drive innovation, and focusing on development efforts in real-time, low-latency deployments, particularly for edge computing. Ultimately, this research provides a robust foundation for future studies and signals a transformative shift in cybersecurity, one that is intelligent, autonomous, and ready for quantum advancements.

Acknowledgements

I would like to express my heartfelt gratitude to Dr. P. Senthilkumar, my research supervisor, for his invaluable guidance and support during this research. I also wish to thank my husband and son for their unwavering encouragement and understanding. Additionally, I am grateful to my parents for their love and support, which has been instrumental in my achievements. Special appreciation is extended to the B.E.S.T. Innovation University, Andhra Pradesh, for providing the essential resources and a conducive research environment.

Conflicts of Interest

The authors declare that there are no conflicts of interest, and that the information presented is unbiased and free from any influence that could arise from potential conflicts.

Funding

This research received no external funding.

References

1. Aswal K, Rajmohan A, Trc A, Mukund S, Panicker VJ, & Dhivvya JP. (2021). Kavach: A machine learning-based approach for enhancing the attack detection capability of firewalls.
2. Gaikwad P, Motwani D, & Shinde V. (2015). Survey on malware detection techniques. International Journal of Modern Trends in Engineering and Research.
3. Aslan O, & Samet R. (2020). A comprehensive review on malware detection approaches. IEEE Access.
4. Talukder S, & Talukder Z. (2020). A survey on malware detection and analysis tools. International Journal of Network Security & Its Applications.
5. Pegoraro Chenet C, Savino A, & Di Carlo S. (2024). A survey on hardware-based malware detection approaches. IEEE Access.

6. Borate VK, Adsul A, Gaikwad A, Mhetre A, & Dicholkar S. (2024). Analysis of malware detection using various machine learning approaches. International Journal of Advanced Research in Science, Communication and Technology.
7. Gaber MG, Ahmed M, & Janicke H. (2023). Malware detection with artificial intelligence: A systematic literature review. ACM Computing Surveys.
8. Yuanming L, & Latih R. (2024). A comprehensive review of machine learning approaches for detecting malicious software. International Journal on Advanced Science, Engineering and Information Technology.
9. Kalsey KS. (2024). Vulnerability and malware detection. International Journal for Research in Applied Science and Engineering Technology.
10. Nawshin F, Gad R, Unal D, Al-Ali AK, & Suganthan PN. (2024). Malware detection for mobile computing using secure and privacy-preserving machine learning approaches: A comprehensive survey. Computers & Electrical Engineering.
11. Sihwail R, Omar K, & Ariffin KAZ. (2018). A survey on malware analysis techniques: Static, dynamic, hybrid and memory analysis. International Journal on Advanced Science, Engineering and Information Technology.
12. Gyamfi NK, Goranin N, Čeponis D, & Čenys H. (2023). Automated system-level malware detection using machine learning: A comprehensive review. Applied Sciences.
13. El Merabet H, & Hajraoui A. (2019). A survey of malware detection techniques based on machine learning. International Journal of Advanced Computer Science and Applications.
14. Tayyab UH, Khan FB, Durad MH, Khan A, & Lee YS. (2022). A survey of the recent trends in deep learning-based malware detection. Journal of Cybersecurity and Privacy.
15. Singh AP. (2024). Encrypted malware detection methodology without decryption using deep learning-based approaches. Turkish Journal of Engineering.
16. Abirami A, Lakshmanaprakash S, Priya RL, Hirlekar V, & Dalal B. (2024). Proactive analysis and detection of cyber-attacks using deep learning techniques. Indian Journal of Science and Technology.
17. Liu K. (2023). A proactive approach to protect cloud computing environment against a distributed denial of service (DDoS) attack. Advanced Sciences and Technologies for Security Applications.
18. Ofoegbu KDO, Osundare OS, Ike CS, Fakeyede OG, & Ige AB. (2024). Proactive cyber threat mitigation: Integrating data-driven insights with user-centric security protocols. Computer Science & IT Research Journal.
19. (2023). Detection prevention and proactive prevention of phishing websites. International Journal of Advanced Research in Science, Communication and Technology.
20. Lakshmikanthan G, & Nair SS. (2024). Proactive cybersecurity: Predictive analytics and machine learning for identity and threat management. International Journal of Innovative Research in Computer and Communication Engineering.

21. Kurhe N, & Rao RS. (2024). An intelligent security mechanism for BYOD networks using proactive AI-based threat detection. Indonesian Journal of Electrical Engineering and Computer Science.
22. Prasad MN, & Kurapati D. (2024). A proactive intelligent framework for malware detection using deep learning techniques. International Journal of Advanced Research in Science, Communication and Technology.
23. Shashikala B, & Srinivas K. (2022). Proactive threat detection using deep learning and ensemble techniques in cybersecurity. International Journal of Advanced Research in Computer and Communication Engineering.
24. Thakur D, Kumar R, & Chauhan R. (2023). A comprehensive review of malware detection in mobile devices using machine learning and deep learning techniques. International Journal of Intelligent Systems and Applications in Engineering.
25. Kumar N, & Kumar S. (2023). Machine learning-based malware detection for Android devices: A survey. International Journal of Computer Applications.
26. Yadav N, & Yadav S. (2023). Deep learning-based Android malware detection: A survey. Wireless Personal Communications.
27. Rawat S, & Rani S. (2023). A comparative analysis of machine learning algorithms for Android malware detection. International Journal of Scientific Research in Computer Science, Engineering and Information Technology.
28. Rao KS, & Mehta M. (2024). AI-based malware detection in IoT networks: A comparative study. International Journal of Scientific Research in Engineering and Management.
29. Patil M, & Patil S. (2024). Evaluation of machine learning models for malware detection in IoT environments. International Journal of Recent Technology and Engineering.
30. Hassan MS, & Ali T. (2024). IoT malware detection using lightweight deep learning models. Journal of Computer Networks and Communications.
31. Jain R, & Agrawal A. (2024). Survey on quantum machine learning-based malware detection systems. Quantum Machine Intelligence.
32. Roy S, & Deb K. (2024). A hybrid quantum-classical machine learning model for proactive malware detection. Quantum Information Processing.
33. Zhang H, & Wu J. (2024). Quantum neural networks for malware classification: A novel approach. Journal of Quantum Computing.
34. Mehta R, & Sharma P. (2023). Post-quantum cryptography for secure malware detection. International Journal of Cyber Security and Digital Forensics.
35. Singh R, & Kaur G. (2024). Quantum-inspired threat detection in AI firewalls. Journal of Emerging Technologies in Computing Systems.