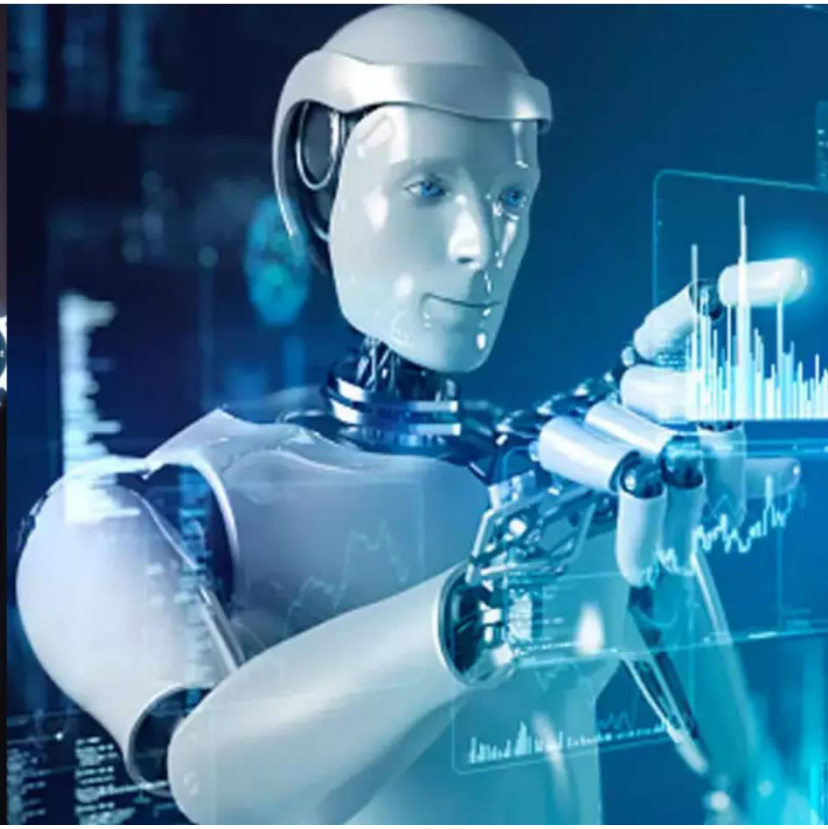
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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

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

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



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

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

Impact Factor 8.699

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

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503360|

Performance Optimization of Firewall Systems Using Intelligent Traffic Analysis

Smit K. Patel, Dr. Hetal R. Modi

Student, Bhagwan Mahavir Collage of Computer Application, Bhagwan Mahavir University, Surat, Gujarat, India

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

ABSTRACT: With the rapid growth of digital communication, network security has become a major concern for organizations and individuals. Firewalls are one of the most important components used to protect networks from unauthorized access and cyber threats [9]. Traditional firewall systems are effective in filtering known threats, but they struggle to detect advanced and zero-day attacks [11]. This research focuses on improving the performance of firewall systems using intelligent traffic analysis techniques. The integration of machine learning helps in identifying abnormal patterns in network traffic [10]. The proposed system enhances detection accuracy and reduces false positive rates [7]. It also improves system efficiency by minimizing latency and increasing throughput. Experimental analysis shows that the intelligent firewall system performs better than traditional firewalls. This study highlights the importance of adaptive security mechanisms in modern networks. The results demonstrate that optimized firewall systems are essential for protecting complex network infrastructures.[4]

KEYWORDS: Firewall Security, Network Protection, Machine Learning, Intrusion Detection, Traffic Analysis, Cyber Security, NGFW

I. INTRODUCTION

In the modern digital era, the use of the internet has increased significantly, leading to a rise in cyber threats and attacks. Organizations rely heavily on network systems, making security a critical requirement. Firewalls act as a barrier between trusted and untrusted networks, controlling incoming and outgoing traffic [9]. Traditional firewalls operate based on predefined rules, which limits their ability to detect unknown threats. Cyber-attacks such as malware, phishing, and distributed denial-of-service attacks have become more advanced [11]. Therefore, there is a need for intelligent firewall systems that can analyze network traffic in real time. Machine learning techniques provide the ability to detect patterns and anomalies in data [10]. This research focuses on enhancing firewall performance using intelligent traffic analysis. The aim is to develop a system that improves detection accuracy while maintaining high performance. The study also evaluates the effectiveness of the proposed system compared to traditional methods [6].

II. LITERATURE REVIEW

Various studies have been conducted in the field of network security and firewall systems. Traditional firewalls such as packet filtering firewalls were among the first security mechanisms used to control network traffic [9]. These firewalls inspect packets based on IP addresses, ports, and protocols. However, they lack the ability to understand the context of the data. Stateful inspection firewalls improved this by tracking the state of network connections. Proxy firewalls added an additional layer of security by acting as intermediaries between users and external networks.

With the advancement of technology, Next Generation Firewalls (NGFW) were introduced [1][3]. These firewalls include features such as intrusion detection systems, application awareness, and deep packet inspection. Studies have shown that NGFWs provide better protection against modern cyber threats [4][5]. However, they also introduce challenges such as increased latency and higher computational requirements.

Recent research focuses on integrating machine learning techniques into firewall systems [6][10]. Machine learning algorithms can analyze large volumes of network traffic and identify abnormal patterns. These systems are capable of

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

Impact Factor 8.699

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

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503360|

detecting unknown and zero-day attacks [7][8]. Researchers have used algorithms such as decision trees, neural networks, and support vector machines for intrusion detection.

Cloud-based firewall systems have also gained popularity due to their scalability and flexibility [19]. However, they face issues such as latency and data privacy concerns. Hybrid firewall systems that combine traditional and intelligent techniques have shown promising results [14][18].

Despite these advancements, challenges such as false positives, performance degradation, and complexity still exist. This research aims to address these issues by proposing an optimized firewall system using intelligent traffic analysis [12].

III. RESEARCH GAP

Although significant progress has been made in firewall technologies, several gaps still exist in the current systems. Traditional firewalls are not capable of detecting advanced cyber threats such as zero-day attacks [11]. They rely on predefined rules, which limits their effectiveness in dynamic environments. Next Generation Firewalls provide enhanced security but often suffer from performance issues [3].

One major gap is the high false positive rate in existing systems [7]. This leads to unnecessary alerts and reduces system efficiency. Another issue is the lack of real-time adaptability in firewall systems. Most systems are not capable of updating their rules dynamically based on changing network conditions [4].

Machine learning-based firewalls require large datasets for training, which may not always be available [9]. They also consume significant computational resources, making them difficult to implement in resource-constrained environments.Cloud firewall systems face challenges related to latency and data privacy [11]. In high-traffic networks, firewall performance tends to degrade, affecting overall system performance.

There is also a lack of integration between firewall systems and intelligent traffic analysis techniques [13]. Existing systems do not fully utilize the potential of machine learning for improving firewall performance.This research aims to bridge these gaps by developing an optimized firewall system that combines traditional security mechanisms with intelligent traffic analysis [19][5]. The goal is to improve detection accuracy while maintaining high performance and scalability.

IV. RESEARCH METHODOLOGY

The research methodology involves designing and evaluating an intelligent firewall system. The first step is to create a network environment for testing. Network traffic data is collected using tools such as Wireshark. This data includes both normal and malicious traffic [4][13][16].

The collected data is then pre-processed to remove noise and irrelevant information. Feature extraction techniques are applied to identify important characteristics of the data [6]. Machine learning algorithms are used to train the model for detecting anomalies [9].

The firewall system is implemented using FortiGate firewall technology. Attack simulation is performed using Kali Linux to generate various types of cyber-attacks [15][17]. The system is tested under different network conditions to evaluate its performance [11].

Performance metrics such as accuracy, detection rate, false positive rate, latency, and throughput are used to measure the effectiveness of the system. The results are compared with traditional firewall systems to analyze improvements [18][20].

The proposed system integrates intelligent traffic analysis with firewall filtering mechanisms. The goal is to create a system that can detect threats in real time while maintaining high performance [6].

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

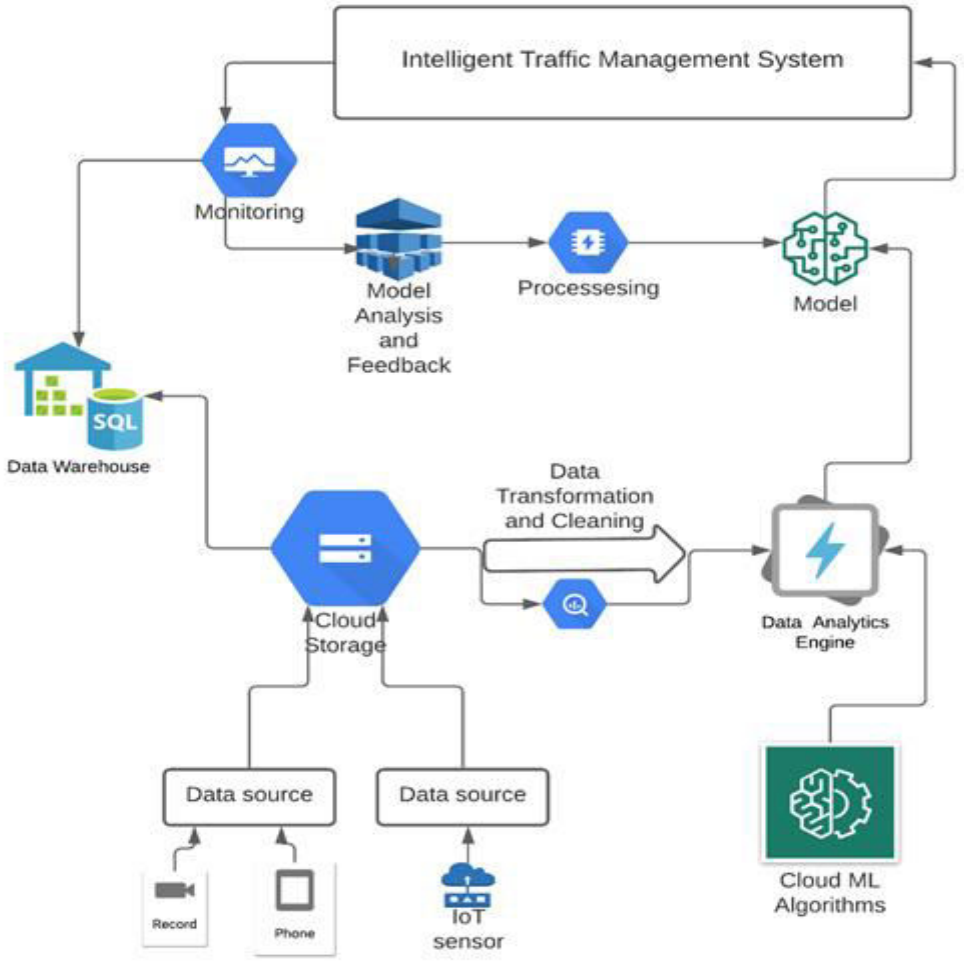
Impact Factor 8.699

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

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503360|

V. INTELLIGENT TRAFFIC MANAGEMENT SYSTEM ARCHITECTURE



The diagram represents an intelligent traffic management system integrated with advanced data analytics and machine learning techniques. The system begins with multiple data sources, including mobile devices, sensors, and recorded inputs [11] .

These sources generate large volumes of raw data continuously. The collected data is transmitted to the cloud storage system. Cloud storage acts as a centralized repository for handling large-scale data efficiently [1]. The stored data is then forwarded to the data transformation and cleaning module. This module removes noise, redundancy, and inconsistencies from the data. Data pre-processing ensures that the dataset is suitable for analysis [18][19].

After pre-processing, the cleaned data is passed to the data analytics engine. The analytics engine performs detailed examination and pattern recognition [3]. It identifies trends, anomalies, and traffic behaviours within the data [8]. The processed data is then utilized by cloud-based machine learning algorithms. These algorithms are responsible for intelligent decision-making [13]. Machine learning models are trained using historical and real-time data. The trained models predict traffic patterns and detect anomalies [4].

The system includes a processing module that manages computational operations. This module ensures efficient handling of large data streams. The model component generates insights based on analysed data [12]. These insights are further used for optimization and decision support [9].

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

Impact Factor 8.699

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

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503360|

The monitoring component continuously tracks system performance [20]. It ensures that all modules are functioning correctly. Monitoring also helps in identifying system inefficiencies [11][17].

A feedback mechanism is integrated into the system [1]. This mechanism allows continuous improvement of the machine learning models [8]. Feedback is generated based on system outputs and real-time conditions. The feedback is sent back to the model for retraining and optimization [16].

The data warehouse stores structured and processed data. It supports long-term storage and historical analysis. The warehouse improves decision-making by providing reliable datasets [9].The intelligent traffic management system coordinates all components. It ensures smooth data flow between modules [5]. The system adapts dynamically to changing traffic conditions [14].

Overall, the architecture enables real-time traffic analysis and optimization [10]. It enhances system efficiency and reduces latency. The integration of cloud computing and machine learning improves scalability [7][8]. The system provides accurate predictions and proactive decision-making. This architecture is suitable for modern intelligent network environments [18].

VI. FIREWALL SYSTEMS BENEFITS

The proposed firewall system offers several advantages over traditional systems. It improves the detection accuracy of cyber threats [15]. The integration of machine learning allows the system to identify unknown attacks [8].

The system reduces false positive rates, leading to better efficiency [18]. It enhances network performance by minimizing latency. The intelligent traffic analysis helps in understanding network behaviour [12].

The system is scalable and can be used in different network environments. It provides real-time threat detection and response. The use of advanced technologies improves overall security [14][19].
The proposed system also supports adaptive learning, allowing it to improve over time. It can handle high volumes of network traffic effectively [8]. The system provides better protection against modern cyber threats.[20]

VII. CHALLENGES

Despite its advantages, the proposed system faces several challenges. One of the main challenges is the complexity of integrating machine learning with firewall systems [8].

The system requires high computational resources, which may not be available in all environments [11]. Data collection and pre-processing can be time-consuming. The accuracy of the model depends on the quality of the training data [10].

Another challenge is maintaining system performance under heavy network traffic. The system may experience delays due to processing large volumes of data [13].

Security of the machine learning model is also a concern. Attackers may try to manipulate the model. The system must be protected against such threats [7].Implementing the system in real-world environments can be difficult. It requires proper configuration and management [1].

Challenges	Description	Impact	Solution
Real-Time Processing	Processing high-speed data in real time is complex [3]	Delay in detecting threats [16]	Use high-performance computing and real-time analytics tools [15]

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

Impact Factor 8.699

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

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503360|

Data Privacy	Sensitive network data may be exposed during processing [3]	Risk of data breaches and privacy violations [11]	Apply encryption and secure data handling protocols [4]
Integration Issues	Combining firewall systems with machine learning is complex [16]	Difficult implementation and system instability [11]	Adopt modular and scalable architecture [14]
Data Storage Limitation	Large-scale data storage becomes challenging [20]	Risk of data loss or inefficiency [10]	Use distributed storage systems [6]
Algorithm Efficiency	inefficient algorithms slow down processing [15]	Reduced system performance [9]	Use optimized and efficient algorithms [14]
Maintenance Complexity	Continuous system updates and maintenance are required [6]	Increased downtime risk [20]	Use automated monitoring and maintenance tools [8]
Monitoring Complexity	Continuous monitoring of system performance is difficult [1]	Delayed detection of system failures [8]	system failures Implement automated monitoring tools [18]
Compatibility Issues	Difficulty in integrating with existing systems [19]	System conflicts and failures [13]	Use standardized protocols [4]
Network Congestion	Heavy traffic load affects system performance [2]	Packet loss and increased latency [9]	Use load balancing techniques [19]
Implementation Cost	Advanced firewall systems are expensive [3]	Not affordable for small organizations [18]	Use hybrid and cost-effective solutions [12]
Dynamic Threats	Cyber threats continuously evolve [5]	Existing system may become outdated [6]	Implement adaptive and self-learning models [8]
Resource Consumption	High CPU and memory usage by advanced systems [14]	Increased operational cost [10]	Optimize resource utilization [5]

VIII. CONCLUSION

This research presents an optimized firewall system using intelligent traffic analysis [9]. The study highlights the limitations of traditional firewall systems and the need for advanced security mechanisms [14].

The proposed system integrates machine learning techniques to improve detection accuracy and reduce false positives. Experimental results show that the system performs better than traditional firewalls [11].

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

Impact Factor 8.699

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

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503360|

The research demonstrates the importance of adaptive security systems in modern networks. The proposed system provides a reliable solution for protecting network infrastructure [20].

Future work can focus on improving the efficiency of machine learning models. Advanced techniques such as deep learning can be explored. The system can also be extended to cloud environments [8].Overall, the research contributes to the development of intelligent firewall systems for enhanced cybersecurity.

REFERENCES

[1] Kaneriya Smit. P (2025). Next-generation firewall (NGFW) technologies and their application in enterprise security. International Journal of Sciences and Innovation Engineering DOI: https://doi.org/10.70849/IJSCI.
[2] Ahmed Abdel-Aziz (2021), Intrusion Detection and Response – Leveraging Next Generation Firewall Technology
[3] Ashay Mohile (2023), Next-Generation Firewalls: A Performance-Driven Approach to Contextual Threat Prevention, Senior Technical Marketing Engineer, Palo Alto Networks, California, USA, DOI: 10.15680/IJCTECE.2023.0601003
[4] Mr. Apoorva Karambelkar, Mr. Shivam Gupta, Ms. Vidhi Agarwal, Mrs. Sonia Behra (2025). Next Generation Firewall using IPS & IDS. Ijraset Journal for Research in Applied Science and Engineering Technology. DOI Link: https://doi.org/10.22214/ijraset.2025.68804
[5] Jenny Heino, Antti Hakkala & Seppo Virtanen (2022). Study of methods for endpoint aware inspection in a next generation firewall
[6] Sina Ahmadi (2023), Next Generation AI-Based Firewalls: A Comparative Study. International Journal of Computer
[7] Taimoor Ahmad (2025). AI-Driven Dynamic Firewall Optimization Using Reinforcement Learning for Anomaly Detection and Prevention. https://doi.org/10.48550/arXiv.2506.05356
[8] Trishna Panse, Kailash Chandra Bandhu (2025). Evaluating Next-Generation Firewalls Using Machine Learning-Based Hybrid Feature Selection for Threat Detection and Risk Mitigation. doi=10.5220/0014275000004928
[9] Dr. S.G. Bhirud, Vijay Katkar (2010). Novel Architecture for Intrusion-Tolerant Distributed Intrusion Detection System using Packet Filter Firewall and State Transition Tables. International Journal of Computer Applications. 8, 11 (October 2010), 29-32. DOI=10.5120/1248-1631
[10] Mouhammd Alkasassbeh (2017), An empirical evaluation for the intrusion detection features based on machine learning and feature selection methods. arXiv:1712.09623
[11] Ehsan Saboori, Shafigh Parsazad, Yasaman Sanatkhani (2012) Automatic firewall rules generator for anomaly detection systems with Apriori algorithm. arXiv:1209.0852
[12] Mansoor Farooq, Rafi Khan, Mubashir Hassan Khan (2023). Stout Implementation of Firewall and Network Segmentation for Securing IoT Devices. Indian Journal of Science and Technology. DOI: 10.17485/IJST/v16i33.1262
[13] Babu R Dawadi, Bibek Adhikari, Devesh K Srivastava (2023). Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks. Sensors (Basel). 2023 Feb 12;23(4):2073. doi: 10.3390/s23042073
[14] Zalte S.S., Patil P.N, Deshmukh S.N(2021). Distributed Firewall with Dynamic Intrusion Detection Module. international journal of advanced research in engineering and technology. DOI: 10.34218/IJARET.12.4.2021.046
[15] Arya Mahendrata Diningrat (2025). Evaluation of Firewall and Intrusion Detection System (IDS) Technology Implementation in Improving Network Security.
[16] Yasin ÇARKÇI, Alperen SAYAR, Seyıt ERTUĞRUL, Görkem DEMİRCAN Boran ERTUĞRUL (2025). A Machine Learning-Driven System for Automated Threat Detection and Firewall Rule Management Using Dark Web Intelligence.
[17] Minghong Yang, Zhenhua Yang, Qiwen Yang (2025). Adaptive Firewall Strategy Generation and Optimization Based on Reinforcement Learning. doi.org/10.31449/inf. v49i33.9363
[18] . Hajar Esmaeil As-Suhbani, S.D. Khamitkar (2019). Classification of Firewall Logs Using Supervised Machine Learning Algorithms. International Journal of Computer Sciences and Engineering DOI: 10.26438/ijcse/v7i8.301304
[19] . Himanshu Sharma (2021), Next-Generation Firewall in the Cloud: Advanced Firewall Solutions to the Cloud. ESP Journal of Engineering & Technology Advancements. DOI: 10.56472/25832646/ESP-V1I1P112
[20] Jae-Kook Lee, Taeyoung Hong, Gukhua Lee (). AI-Based Approach to Firewall Rule Refinement on High-Performance Computing Service Network. National Supercomputing Center, Korea Institute of Science and Technology Information, 245 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details