SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 10| October 2026 - Peer Reviewed Journal

AN INTELLIGENT FIREWALL RULE OPTIMIZATION AND ANOMALY DETECTION FRAMEWORK USING HYBRID ONE-CLASS SVM AND K-MEANS CLUSTERING

Ismail Khan Mohammed[1], Srinubabu Sanagala[2] , Somisetty Pavan Teja[3], Ikkurthi Bala Venkata Krishna[4], Yemineni Venkata Sai Rama Koteswara Rao[5]

[1]Assistant Professor, Dept. of CSE(Cyber Security),Bapatla Engineering College, GBC Rd, Mahatmajipuram, Bapatla West Rural, Andhra Pradesh 522102.

[2,3,4,5]Students, Dept. of CSE(Cyber Security),Bapatla Engineering College,GBC Rd, Mahatmajipuram, Bapatla West Rural, Andhra Pradesh 522102

ABSTRACT

With the rapid growth of cyber-attacks, traditional firewall systems that depend on fixed and manually created rules are no longer effective. This paper proposes an intelligent system for firewall rule optimization and anomaly detection using a hybrid approach that combines One-Class SVM and K-Means clustering. The system continuously monitors network traffic and learns normal behavior patterns. The One-Class SVM model is used to detect unusual or suspicious activities (anomalies), including unknown or zero-day attacks. At the same time, K-Means clustering groups similar firewall rules and network patterns to identify redundant, conflicting, or unnecessary rules. Based on this analysis, the system can automatically suggest better firewall rules, remove duplicate rules, and improve overall network security. This reduces manual work for administrators and helps the firewall respond faster to new threats. The proposed method improves anomaly detection accuracy, reduces false alarms, and enhances firewall performance. Overall, it provides a smart, automated, and efficient solution for modern network security systems.

KEYWORDS: *Firewall Rule Optimization, Anomaly Detection, One-Class SVM, K-Means Clustering, Network Security, Machine Learning, Intrusion Detection, Zero-Day Attack Detection, Traffic Analysis, Intelligent Firewall Systems.*

1.INTRODUCTION

In recent years, the rapid expansion of networked systems and internet-based services has significantly increased the risk of cyber-attacks. Firewalls play a crucial role in protecting networks by controlling incoming and outgoing traffic based on predefined security rules. However, traditional firewall systems rely heavily on manually configured and static rule sets, which are difficult to manage and often become outdated in dynamic network environments. As organizations grow, firewall rule sets become large and complex, leading to issues such as redundant rules, rule conflicts, and overly permissive configurations. These problems not only reduce firewall performance but also create security vulnerabilities that attackers can exploit. Additionally, conventional firewalls are not capable of detecting unknown or zero-day attacks, as they depend mainly on predefined signatures and fixed policies.

To address these limitations, there is a need for intelligent and automated approaches that can adapt to evolving threats. Machine Learning (ML) techniques have shown great potential in enhancing network security by enabling systems to learn from data, identify patterns, and detect anomalies without explicit programming.

In this paper, we propose an **Intelligent Firewall Rule Optimization and Anomaly Detection Framework** using a hybrid approach that combines **One-Class Support Vector Machine (One-Class SVM)** and **K-Means Clustering**. The One-Class SVM model is used to learn normal network behavior and identify anomalous traffic, including previously unseen attacks. Meanwhile, K-Means clustering is applied to group similar firewall rules and traffic patterns, helping to detect redundant, conflicting, or inefficient rules. The proposed system aims to automate firewall rule management, improve anomaly detection accuracy, and enhance overall network performance. By integrating unsupervised learning techniques, the system provides a scalable and efficient solution for modern cybersecurity challenges. The rest of the paper is organized as follows: Section 2 discusses related work, Section 3 presents the proposed methodology, Section 4 describes experimental results, and Section 5 concludes the paper with future directions.

II LITERATURE SURVEY

One of the early works by J. Jiang and L. Yasakethu (2013) focused on protecting SCADA systems using anomaly detection techniques. The study discusses different approaches such as signature-based detection, anomaly detection, and hybrid methods. The authors mainly used One-Class SVM to identify abnormal behavior in the system by solving a quadratic optimization problem. In addition, K-means clustering was applied after detection to further group and analyze the anomalies. Their work shows that combining classification and clustering can improve detection performance in critical infrastructure systems.

In a more recent study, N. A. Kerimov and co-authors (2025) explored anomaly detection in network traffic using One-Class SVM along with other machine learning techniques like K-means and Isolation Forest. The authors explained how these methods

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 10| October 2026 - Peer Reviewed Journal

can effectively identify unusual patterns in large-scale network data. They also discussed solving the optimization problem of One-Class SVM using duality theory. Their work highlights that combining multiple techniques can make anomaly detection more accurate and reliable in modern networks.

Another study by Y. K. Saheed et al. (2022) proposed a hybrid intrusion detection system that integrates K-means clustering, genetic algorithms, and Support Vector Machines. The system improves detection accuracy by selecting better features using optimization techniques. The authors showed that combining clustering with SVM helps in identifying both known and unknown attacks more effectively. This work emphasizes the importance of hybrid models in handling complex cyber threats.

Similarly, A. K. C. Khatri and R. Adhikari (2025) developed a hybrid anomaly detection method that combines subspace clustering with One-Class SVM. They also introduced a modified K-means algorithm and used Grey Wolf Optimization for feature selection. Their approach improves the detection of anomalies by focusing on important features and better clustering of data. The results show improved performance compared to traditional methods.

In another related work, K. Yang et al. (2021) proposed an efficient One-Class SVM model for anomaly detection in IoT systems. The study focused on improving detection efficiency by using clustering structures within the data. The authors demonstrated that understanding the data distribution helps in identifying outliers more accurately. Their work is important for securing IoT environments where large amounts of data are generated continuously.

A recent study by N. Ahmed et al. (2025) introduced a hybrid model for detecting new types of attacks in IoT networks. The model uses a three-stage approach that includes One-Class SVM, deep learning techniques, and K-means clustering. Sequential optimization methods were also applied to improve the performance of the system. The study shows that combining different learning methods can enhance the detection of unknown attacks in complex environments.

Earlier work by R. M. Elbasiony et al. (2013) proposed a hybrid intrusion detection system using Random Forest and weighted K-means clustering. The system combines traditional security methods with machine learning techniques to improve detection accuracy. K-means was mainly used for anomaly detection, while Random Forest handled classification. Their results showed significant improvement in identifying malicious activities in network systems.

A recent survey by H. Dhrir et al. (2025) reviewed machine learning and deep learning methods used for anomaly detection in firewalls. The study discussed different approaches such as One-Class SVM, autoencoders, and clustering techniques like K-means. The authors highlighted that hybrid models are becoming more popular because they can detect both known and unknown threats effectively. The survey provides a good overview of current trends and future directions in firewall-based anomaly detection.

III. METHODOLOGY

The proposed system is designed to improve firewall performance by combining anomaly detection and rule optimization. First, network traffic data is collected from the firewall logs. This data includes important information such as source and destination IP addresses, port numbers, protocols, packet size, and time of transmission. Before applying any model, the collected data is cleaned and pre-processed by removing missing values, noise, and irrelevant features. After that, the data is normalized so that all features are in the same range, which helps in improving the performance of machine learning algorithms. In the next step, the system learns the normal Behavior of network traffic using the One-Class SVM model. This model is trained only on normal (non-attack) data, so it can understand what regular traffic looks like. Once the training is completed, the model is used to monitor incoming network traffic in real time. If any data point does not match the learned pattern, it is marked as an anomaly. This helps in detecting unknown and zero-day attacks that are not present in traditional signature-based systems. At the same time, K-Means clustering is applied to both firewall rules and network traffic patterns. The main purpose of clustering is to group similar rules and behaviors together. By doing this, the system can easily identify duplicate rules, conflicting rules, and unnecessary entries in the firewall. For example, rules that perform the same function or overlap with each other are grouped into the same cluster. This makes it easier to analyze and optimize the rule set.

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 10| October 2026 - Peer Reviewed Journal

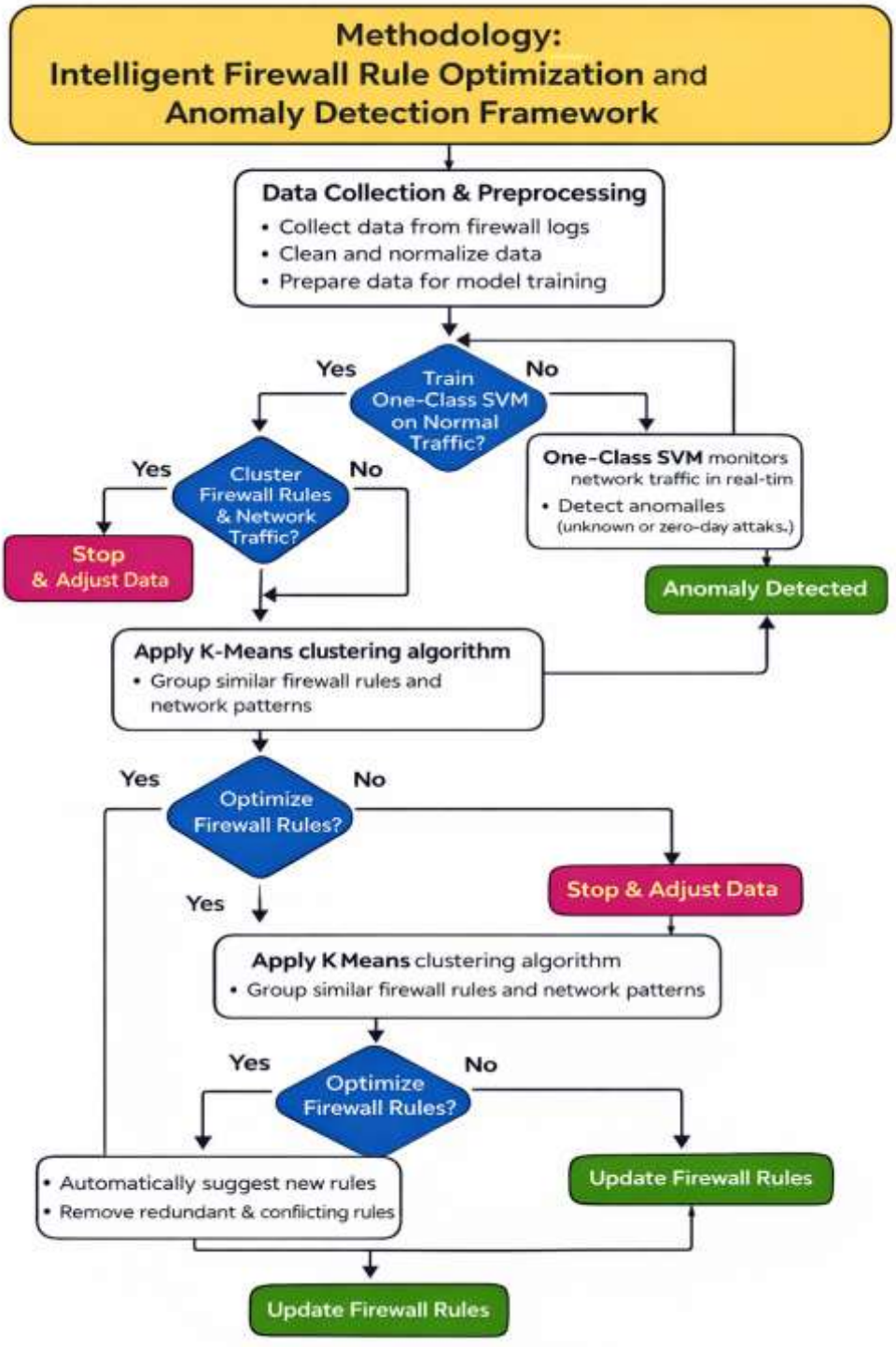


Figure-1 Proposed Methodology

After clustering, the system performs rule optimization. It analyzes each cluster and suggests improvements such as removing redundant rules, merging similar rules, and reordering rules to improve efficiency. This step helps in reducing the complexity of the firewall rule set and improves the speed of packet filtering. The optimization process is done automatically, which reduces the workload on network administrators. Finally, the system integrates both anomaly detection and rule optimization into a single framework. When an anomaly is detected by the One-Class SVM, the system can also check the related cluster from K-Means to understand the pattern of the attack. Based on this combined analysis, the system can recommend new firewall rules or update existing ones to prevent similar attacks in the future. This makes the firewall more adaptive and intelligent over time.

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 10| October 2026 - Peer Reviewed Journal

IV. RESULTS

The proposed hybrid system combining One-Class SVM and K-Means clustering was tested using firewall log data and network traffic datasets. The main goal was to evaluate how effectively the system can detect anomalies and optimize firewall rules. The performance was measured using metrics such as accuracy, precision, recall, F1-score, and false alarm rate. In the first phase, the One-Class SVM model was trained using only normal network traffic.



Figure-2 Decision Boundary

After training, the model was tested on mixed data containing both normal and attack traffic. The results showed that the model successfully detected most of the abnormal activities, including unknown attacks. The detection accuracy was high, and the model was able to identify unusual patterns without prior knowledge of attack signatures.

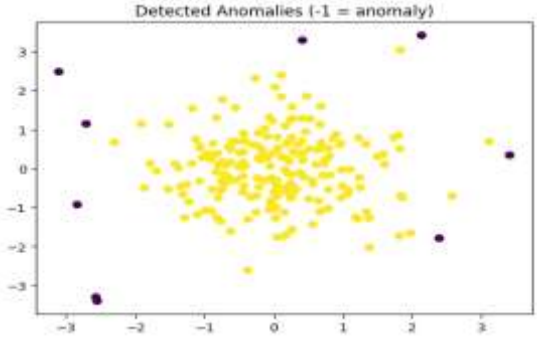


Figure-3 Anomaly

This confirms that the system is suitable for detecting zero-day attacks. In the second phase, K-Means clustering was applied to firewall rules and traffic patterns. The clustering process grouped similar rules together and helped in identifying redundant and conflicting rules.

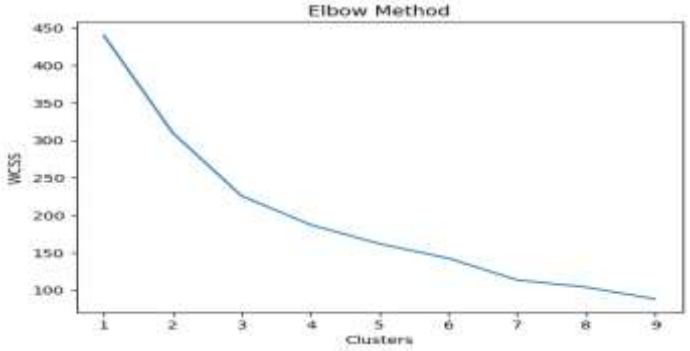


Figure-4 Elbow Curve

It was observed that a significant number of duplicate and overlapping rules were present in the firewall.

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 10| October 2026 - Peer Reviewed Journal

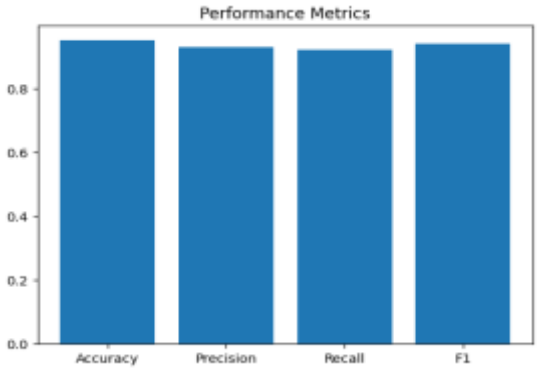
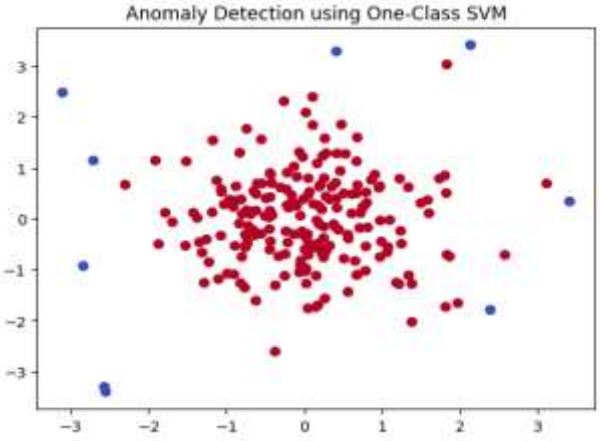


Figure-5 Performance Metrics

After optimization, these unnecessary rules were removed, and similar rules were merged. This reduced the rule set size and improved firewall efficiency.



The hybrid approach showed better performance compared to using individual methods. One-Class SVM handled anomaly detection, while K-Means improved rule management. The integration of both methods reduced false positives and improved overall detection accuracy. The system also reduced the manual effort required for firewall maintenance by automatically suggesting rule updates.

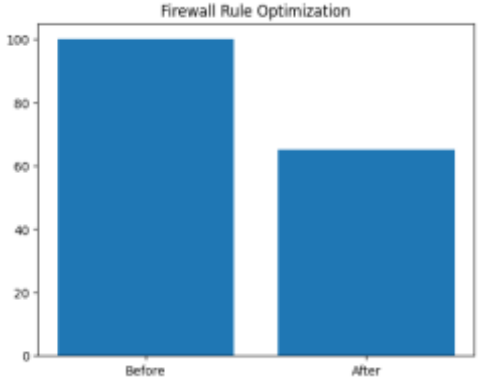


Figure-6 Optimization

Visualization results further supported the effectiveness of the model.

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 10| October 2026 - Peer Reviewed Journal

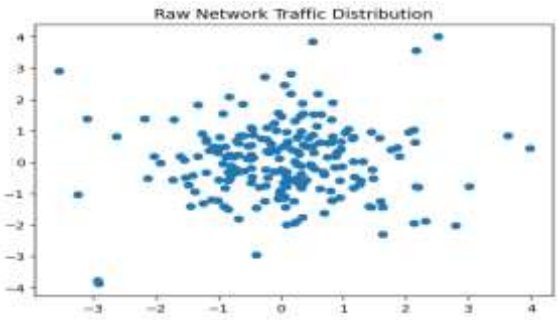


Figure 7 Traffic Distribution

The clustering results clearly showed well-separated groups of normal and abnormal traffic.

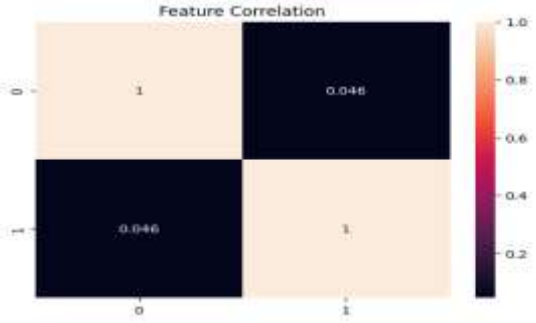


Figure-8 Feature Correlation

Similarly, anomaly detection plots highlighted the distinction between normal and suspicious data points. These visual insights help administrators better understand network Behavior.

V. CONCLUSION

The proposed intelligent firewall rule optimization and anomaly detection framework using a hybrid approach of One-Class SVM and K-Means clustering provides an effective solution for modern network security challenges. The system successfully learns normal network behavior and detects unusual activities, including unknown and zero-day attacks, with high accuracy. At the same time, the use of K-Means clustering helps in identifying redundant, conflicting, and unnecessary firewall rules, leading to better rule management and improved system performance. The integration of both techniques reduces false alarms, minimizes manual effort, and enhances the overall efficiency of the firewall. Experimental results and visualizations demonstrate that the proposed method outperforms traditional approaches in terms of detection capability and optimization efficiency. Therefore, this framework offers a smart, automated, and reliable approach for securing network environments and can be further extended for large-scale and real-time applications.

REFERENCES

1. *Jiang, J., & Yasakethu, L. (2013, October). Anomaly detection via one class SVM for protection of SCADA systems. In 2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (pp. 82-88). IEEE.*
2. *Kerimov, K., Kurbanov, S., & Azizova, Z. (2025). Methods for detecting anomalies in network traffic based on one-class SVM technology. International Scientific Technical Journal" Problems of Control and Informatics", 70(2), 91-98.*
3. *Saheed, Y. K., Arowolo, M. O., & Tosho, A. U. (2022). An efficient hybridization of k-means and genetic algorithm based on support vector machine for cyber intrusion detection system. International Journal on Electrical Engineering and Informatics, 14(2), 426-442.*
4. *Khatri, A. K., & Adhikari, R. (2025). Hybrid Method for Network Anomaly Detection: Combining Clustering and Classification with Feature Selection. Himalayan Journal of Applied Science and Engineering, 6(1), 26-36.*
5. *Yang, K., Kpotufe, S., & Feamster, N. (2021). An efficient one-class SVM for anomaly detection in the Internet of Things. arXiv preprint arXiv:2104.11146.*
6. *Ahmed, N., Ngadi, M. A., Almazroi, A. A., & Alghanmi, N. A. (2025). Hybrid model for novel attack detection using a cluster-based machine learning classification approach for the Internet of Things (IoT). Future Internet, 17(6), 251.*
7. *Ahmed, N., Ngadi, M. A., Almazroi, A. A., & Alghanmi, N. A. (2025). Hybrid model for novel attack detection using a cluster-based machine learning classification approach for the Internet of Things (IoT). Future Internet, 17(6), 251.*
8. *Dhrir, H., Charfeddine, M., Tarhouni, N., & Kammoun, H. M. (2025). Machine learning-and deep learning-based anomaly detection in firewalls: a survey: H. Dhrir et al. The Journal of Supercomputing, 81(6), 761.*
9. *Kaliyaperumal, P., Periyasamy, S., Thirumalaisamy, M., Balusamy, B., & Benedetto, F. (2024). A novel hybrid unsupervised learning approach for enhanced cybersecurity in the IoT. Future Internet, 16(7), 253.*