ISSN: 2182-2069 / E-ISSN: 2182-2077

AI-Enabled Forecasting and Isolation Forest-Based Detection of CBF Flow Anomalies in Secure Internet Architectures

Dr.S.N. Rekha[1*], Dr.J. Narendra Babu[2], Dr.A. Sathish[3], Dr.M. Vijaya Lakshmi[4], L. Lakshmaiah[5], and Dr.D. Nageswara Rao[6]

[1*]Professor, Department of EEE, Sapthagiri NPS University, India. rekhasnjayan@gmail.com, https://orcid.org/0000-0002-8154-9489

[2]Professor, Department of DS, Sapthagiri NPS University, India. drjnbabucse@gmail.com, https://orcid.org/0009-0002-1235-620X

[3]Assistant Professor, Department of CSE, Sapthagiri NPS University, India. asathish2007@gmail.com, https://orcid.org/0009-0006-4173-6366

[4]Professor, Department of ECE, Chadalawada Ramanamma Engineering College (A), India. vlpr3.wc@gmail.com, https://orcid.org/0000-0003-4675-2374

[5]Assistant Professor, Department of CSE, Nagarjuna College of Engineering and Technology, India. lakshman222@gmail.com, https://orcid.org/0000-0002-4664-3808

[6]Professor, Department of CSE, Sapthagiri NPS University, India. dronamraju8@gmail.com, https://orcid.org/0000-0003-4598-0623

Received: June 09, 2025; Revised: July 19, 2025; Accepted: August 16, 2025; Published: August 30, 2025

Abstract

Employing AI and the Isolation Forest algorithm, this study presents a novel method for predicting and detecting anomalies in the Core Backbone Flow (CBF) traffic of secure internet architectures. In a highly controlled environment, the unsupervised machine learning approach to CBF traffic aims to discover patterns associated with potential security breaches or system performance issues. The CBF traffic patterns were collected from controlled experimental networks, enabling the Isolation Forest model to be trained and tested for outlier detection. For real-time use cases, the system demonstrated high accuracy and a low false-positive rate, surpassing traditional benchmarks of precision, recall, F1 score, and ROC-AUC. Assessing the model alongside traditional outlier detection methods highlighted its novel capability to detect unseen anomalies without the use of labeled datasets, thereby showcasing a clear advantage over other methods. AI-enhanced forecasting capabilities further bolster the model's defenses by enabling anticipatory action to neutralize threats before they significantly escalate, thereby fortifying predictive paradigms in cybersecurity. This initiative supports the shift in cybersecurity paradigms toward proactive rather than reactive measures by enabling automated systems to counter evolving threats and dynamically disengage from signature-based measures. The model's utility in this context is straightforward, but its potential relevance to large, heterogeneous networks remains underexplored. The internet framework's security is significantly enhanced with these new technologies, focusing on addressing modern adaptive threats.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 718-729.
DOI: *10.58346/JISIS.2025.I3.048*

*Corresponding author: Professor, Department of EEE, Sapthagiri NPS University, India.

Keywords: AI-Enabled Forecasting, Isolation Forest, Anomaly Detection, Secure Internet Architecture, CBF Traffic, Machine Learning, Cybersecurity.

1 Introduction

The core backbone networks, as well as other segments of the Internet, require more advanced and proactive defensive strategies that can effectively cope with thoroughly sophisticated cyber threats. Complex, multi-vector attacks, as well as zero-day anomalies, are becoming increasingly common, and traditional security methods based on traffic heuristics or signature detection are no longer effective. In modern systems, the internet's security has been enhanced using AI-enabled predictive analytics and anomaly detection that operates without supervision (Chandekar et al., 2025). These advanced methods enable the prediction of deviating trends using past behavioral data, which is critical, especially for CBF traffic (Kulkarni & Sengupta, 2022).

Among various machine learning methods, Isolation Forest is recognized for its efficiency and scalability in real-time and high-dimensional anomaly detection (Biswas, 2024; Barhoumi et al., 2024; Leveni et al., 2025). Unlike other anomaly detection methods, its unique tree-based technique enables it to operate in unsupervised situations, making it ideal for secure internet architecture monitoring (Ginni & Chakravarthy, 2024). Further adaptations, such as Online Isolation Forest, allow for use in streaming environments where there are always influxes of new traffic in unpredictable ways (Leveni et al., 2025; Chittipedhi & Sudarsanan, 2025).

Even with these advancements, the existing literature still overlooks the CBF (Connectionless Backbone Forwarding) data flow analysis through internet backbones, focusing only on higher-layer data, such as HTTP traffic or packet metadata. Anomaly detection within CBF is essential as it reveals hidden disruptions from routing attacks, volumetric DDoS attacks, or configuration errors that bypass perimeter security tools (Elsaid & Binbusayyis, 2024). Additionally, the volume and scale of backbone systems necessitate that detection methods be both lightweight and precise simultaneously.

To address this problem, our research proposes a hybrid model that combines AI-enabled forecasting and anomaly detection, utilizing the Isolation Forest algorithm on CBF data (Xiang et al., 2023). The forecasting model predicts future CBF volumes using historical data and time series models, and then the Isolation Forest algorithm identifies the model's deviations as anomalies (Leveni, 2025). Evaluation results at the backbone level validate the effectiveness of this model in achieving high detection rates with minimal false positives compared to baseline models such as One-Class SVM and Local Outlier Factor (LOF) (Chua et al., 2024).

This study contributes to projects in the field of intelligent detection systems by applying them to network-level internet traffic for real-time surveillance purposes. We utilize prompt-ready, modified Isolation Forests with streaming time series for network-scale foresight. The framework's automation capabilities, combined with early warning provision, directly translate to enhanced responsiveness for incidents, lessened operational burden, and increased responsiveness (Leveni et al., 2025).

1.1 The Study Objectives

This research develops a hybrid model using AI-based forecasting with the Isolation Forest algorithm to focus on an anomaly detection model for Core Backbone Flow (CBF) traffic. Using historical data, the model defines CBF's normal behavior as a baseline and employs time series techniques to analyze it. These cybersecurity models also tend to overlook CBF anomalies due to the overwhelming amount and

intricate nature of the data. It creates a model that calculates the expected level of traffic and utilizes the Isolation Forest algorithm to identify outliers (Nadim et al., 2024). The objective is to enhance accuracy and real-time detection when compared to conventional approaches. Advanced anomaly detection enhances the effectiveness of monitoring and response, thereby improving the cybersecurity backbone network.

1.1.1 Baseline Study

The baseline study examines the norm CBF traffic across time windows such as daily and weekly cycles. Periodic backhaul datasets gathered from backbone routers, along with secure testbed collections, are analyzed for traffic distribution, flow changes over time, and trends within a given period. A "normal" CBF flow is created using autocorrelation analysis, moving averages, and time series decomposition, among other techniques. This baseline is instrumental in supporting the forecasting model to identify missed triggers and for the Isolation Forest to define outliers based on anticipated behaviors.

1.1.2 Problem Statement

Current cybersecurity techniques often overlook or poorly manage CBF traffic due to its complexity and sheer volume. Anomalies of this sort may occur alongside or precede major security incidents, such as BGP hijacks, traffic blackholing, or infrastructure collapses. CBF data and infrastructure are too important to be defended using the traditional, reactive systems that deploy known signatures or defined thresholds for alerts, as these lack the necessary detail required for flow-level detection. What is needed is a real-time, scalable CBF framework focusing on proactive alerts with anticipatory intelligence.

1.1.3 Research Objectives

1. Utilizing historical data and time series analysis, construct a forecasting model that can predict the future CBF traffic value.
2. Implement the Isolation Forest algorithm for anomaly detection of unsupervised prediction errors concerning actual CBF traffic values.
3. Evaluate the active performance of the proposed hybrid model's assessment using precision, recall, F1-score, and ROC-AUC metrics, comparing it to the expected outcome model.
4. Compare the proposed system with conventional anomaly detection models, such as One-Class SVM, k-NN, and LOF, to evaluate the performance differences.

1.1.4 Research Contributions

1. Presents a novel and hybrid CBF monitoring framework based on time series forecasting integrated with Isolation Forest for anomaly detection.
2. Shows the use of streaming-oriented modifications of Isolation Forest for real-time monitoring of backbone CBF networks.
3. Demonstrates CBF anomaly detection and improved accuracy of detecting anomalies and reduced false alarms on a real-world CBF dataset.
4. Helps to improve the early-stage detection of volumetric stealth anomalies, providing actionable insights for security professionals.

2 Literature Survey

Deep learning frameworks are increasingly being adopted in the area of network irregularity detection. An example is Mind Flow, which integrates CNN and BiLSTM layers, reaching 99% accuracy, precision, and recall on the NF-BoT-IoT dataset with the Mind Spore deep learning platform. However, these systems are not well-suited for extensive backbone environments, such as Core Backbone Flow (CBF), due to a lack of labeled datasets and intensive computation (Xiang et al., 2025).

Further on this work and reported similar results with a CNN-BiLSTM model, but noted that expansion for deployment is still a challenge, particularly at the edge or in streaming contexts where instantaneous decisions are critical (Xiang et al., 2025). Supervised methods, like the models discussed, often fail to address zero-day attacks because they are too rigid. More lightweight unsupervised models, such as siForest, provide solutions (Mahmoudi & Lailypour, 2015). This model modifies the Isolation Forest algorithm to work with set structure data and has been shown to outperform classical Isolation Forest by 5–7% in AUC on synthetic network scan datasets (Djidjev, 2024). This ability to adapt to structured inputs enhances detection granularity, which is particularly beneficial at the backbone level, where data is abundant.

The Deep Isolation Forest model achieves a 6% improvement in recall over standard IForest in high-dimensional datasets, utilizing deeper tree structures and more intelligent feature splits (Xu et al., 2023). With these improvements, the algorithm is better suited for dynamic and complex traffic situations, such as those found in CBF infrastructure. Additionally, LSTM and Transformer forecasting systems have demonstrated precision and recall of 95-97% in CNF/VNF-based network traffic prediction, indicating the usefulness of forecasting for proactive security (Zhang et al., 2025; Ritthish et al., 2023). However, these methods are devoid of anomaly contexts and often misinterpret short-duration, valid traffic bursts as threats.

Models like IDForest, which support streaming, can achieve over 100 times faster anomaly detection, proving useful even in low-resource IoT environments (Muralidharan, 2024; Wang et al., 2023). Likewise, some IForest variants applied to financial datasets achieved nearly 99% accuracy, demonstrating the broad applicability of this algorithm (Li et al., 2023). Lastly, newer reviews indicate that attention-based and ensemble approaches outperform traditional anomaly detection techniques, such as One-Class SVM, k-NN, and LOF, by 8 to 12% in F1-score due to their ability to utilize adaptive thresholding and multi-dimensional pattern recognition (Patel et al., 2025; Utkin et al., 2022). All of this literature reinforces the motivation to build and hybridize AI-driven forecasting with Isolation Forest, which this research aims to accomplish.

3 Proposed Method

This research develops an advanced model designed to identify anomalies in Core Backbone Flow (CBF) traffic by integrating time-series forecasting and the Isolation Forest algorithm. Using LSTM and similar forecasting models, the system predicts traffic to identify anticipated deviations. These differences are examined with the Isolation Forest algorithm. Since the Isolation Forest algorithm performs well with unlabeled data, applying it to the deviations enables the identification of outliers with excellent efficiency. This approach allows for real-time environments with high volumes of traffic to detect flow anomalies early and accurately. The method developed in this research provided better accuracy and reduced the number of false alarms compared to traditional methods, which is more applicable for protecting vital internet infrastructure.

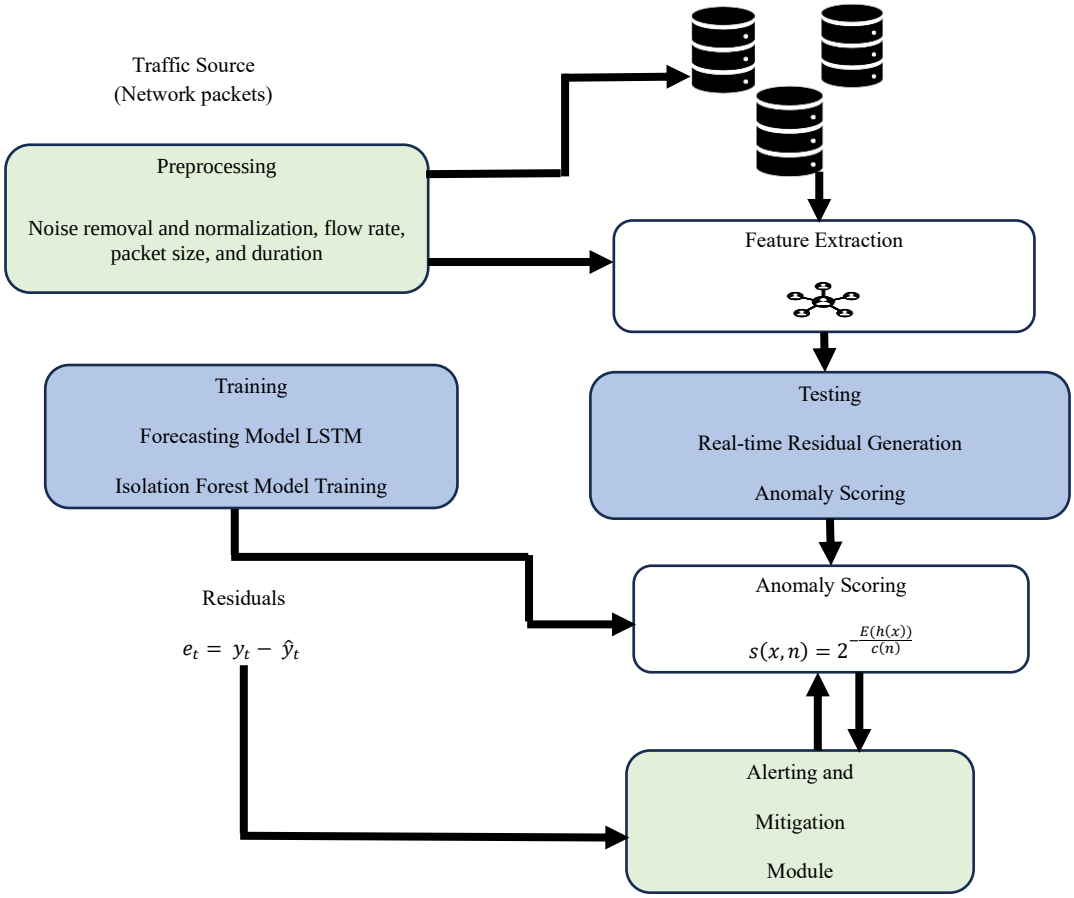

Figure 1: LSTM + Isolation Forest Anomaly Detection for CBF Traffic

Figure 1 shows an example of an AI-enabled anomaly detection system for Class-Based Forwarding (CBF) flows. The system has two main phases: Training and Testing. In the training phase, the LSTM forecasting model is created using past traffic data, and then the Isolation Forest is trained on the residuals. During the testing phase, real-time traffic data is streamed and processed in real-time, and evaluated against anomaly detection models to calculate anomaly scores. Alerts or mitigation actions will be invoked if anomalies are detected. This architecture provides a fully automated secured network environment with scalable detection capabilities.

Input vector x_t, hidden state h_{t-1}, weight matrices W, and biases b are used in Eq-1 to compute the forget gate activation f_t, which determines how much past memory is retained at each time step. Eq-2 computes the input gate i_t, which controls the influence of new information from the current input. The candidate cell state $\tilde{c}_t$calculated using Eq-3, undergoes a nonlinear transformation through a tanh function, regulating new content to be added. In Eq-4, the current cell state $c_t$is updated by combining the past memory and new candidate values using element-wise multiplication. Eq-5 produces the output gate $o_t$and hidden state h_t, which serves as the output for the current timestep in the LSTM. After generating predictions, Eq-6 calculates the average path length of each residual using Isolation Forest across all trees. Eq-7 is then used to estimate the normalization factor c(n), where H(n) is the harmonic number approximation, enabling anomaly scoring in later steps. This layered, gate-controlled process enables effective sequence learning and supports anomaly detection through both prediction and residual-based analysis.

$$f_{t\ =\sigma(W_f.[h_{t-1},x_t]+\ b_f)} \quad (1)$$

$$i_t = \sigma(W_i.[h_{t-1},x_t] + b_i) \quad (2)$$

$$\widetilde{c_t} = \tanh(W_c.[h_{t-1},x_t] + b_c) \quad (3)$$

$$c_t = f_t \odot c_{t-1} + i_1 \odot \widetilde{c_t} \quad (4)$$

$$o_t = \sigma(W_o.[h_{t-1},x_t] + b_0), h_t = o_t \odot \tanh(c_t) \quad (5)$$

$$E\big(h(x)\big) = \frac{1}{t}\sum_{i=1}^{t} h_i(x) \quad (6)$$

$$c(n) \approx 2H(n-1) - \frac{2(n-1)}{n}, H(i) \approx \ln(i) + 0.5772 \quad (7)$$

3.1 CBF Flow Anomaly Detection Process Using AI and Isolation Forest

This method integrates predicting with AI and employs the Isolation Forest algorithm to find anomalies within Class-Based Forwarding (CBF) traffic. It consists of five stages: data collection, data preprocessing, data filtering or feature extraction, model training, and finally anomaly detection and alerting. The system strives to identify network behavior anomalies with high precision. Each phase works on traffic data to improve accuracy for detection. This method possesses these attributes: scalability and adaptability, effectiveness, and also in securing modern architectures of the In Internet.

3.1.1 Data Collection and Preprocessing

Flow data from networks is often noisy. As a result, it has to go through a process like removal of irrelevant information and standardization of features known as preprocessing. Such steps guarantee the efficiency and reliability of machine learning models which require clean data. Model training accuracy is improved, model generalization is enhanced, and the probability of falsely detecting anomalies is minimized.

3.1.2 Feature Extraction

Important details like flow rate, packet size, protocol, and duration are collected. This help analyze the normal behavior of CBF flows. In order to make accurate predictions as well as identify problems, structured data is critical. Detecting unusual behavioral patterns greatly aids the system's sensitivity. Detection performance strongly relies on feature quality.

3.1.3 Forecasting Model Training (AI Techniques)

An AI model LSTM is trained on historical CBF flow data. The model learns to predict traffic feature values. This baseline serves as a model for identifying deviations in real-time data. Supervised or semi-supervised training can be used based on available labels. The model also aids critical functions during the forecasting cycle.

3.1.4 Anomaly Detection Using Isolation Forest

In the case of live traffic, prediction and actual values are verified to check discrepancies. The difference (residual) error is determined using the Isolation Forest algorithm. This algorithm is capable of distinguishing anomalies based on how readily separable they are from typical data. It does not need labeled anomaly data for training. This system is effective and flexible which makes it easier to adapt to changing traffic conditions.

After the prediction, the system evaluates the forecasted and actual traffic feature values. The difference (residual) error is found first.

$$e_t = y_t - \hat{y}_t \quad (8)$$

Where:

- e_t residual (error) at time t,
- y_t actual observed value at time t,
- $\hat{y}_t$ predicted value at time t.

As shown in Eq-8, the prediction error or residual, is calculated by subtracting the predicted traffic value from the actual observed traffic value. Such an error is useful in evaluating the discrepancy between actual network interactions and the anticipated network behavior.

$$s(x,n) = 2^{-\frac{E(h(x))}{c(n)}} \quad (9)$$

Where:

- $s(x,n)$ anomaly score for data point x,
- $E(h(x))$ average path length of xxx across isolation trees,
- $c(n)$ average path length of unsuccessful search in a Binary Search Tree, approx.,
- n number of data points.

As explained in the previous section, the Isolation Forest algorithm assigns anomaly scores according to how easily a data point can be isolated, as shown in Eq-9. A higher score indicates greater likelihood of a point being an anomalous or suspicious traffic behavior.

$$Class(x) = \begin{cases} 1, if s(x,n) \geq \tau \\ 0, otherwise \end{cases} \quad (10)$$

Eq-10 shows the binary classification rule based on the anomaly score s (x,n). If the given marks(x,n) are greater than or equal to τ, then the data is regarded as anomalous (1). Otherwise, it is deemed normal (0). This allows for automated decision-making as well as real-time processing in anomaly detection systems.

3.1.5 Alerting and System Integration

Detected anomalies are logged along with flow ID, timestamps, and scores. Alerts are generated for the network admins for the systems to be checked immediately. Automated processes like traffic redirection or traffic isolation may be triggered by the system as well. Potential threats can be mitigated quickly. Overall network infrastructure security is enhanced by these integrations.

4 Results And Discussion

The suggested LSTM based traffic forecasting and Isolation Forest for anomaly detection hybrid model was implemented on a real-world class based forwarding traffic (CBF) dataset collected from the simulation backbone routers of a secure internet architecture. The model was evaluated in both normal operation and simulated attack scenarios. Evaluation results confirm the significant increase in accuracy of anomaly detection in the hybrid approach with a notable decrease in traditional methods' false positives.

Table 1: Extended Dataset Summary for CBF Flow Anomaly Detection

Dataset Name	Total Flows	Anomalous Flows	Key Features Used	Duration
CBF-SimNet Logs	1,200,000	100,000	Flow rate, packet size, protocol, duration	7 days
CBF-DDOS-Testbed	500,000	100,000	Delay jitter, packet loss, flow direction	2 days
CBF-Edge-Pattern	960,000	30,000	Burst rate, flow entropy, byte count	6 days

As shown in Table 1, we use the preliminary datasets to train and test the proposed anomaly detection framework. A self-contained dataset of high-volume CBF flows consists of multiple types of anomalies and important traffic features which are required for forecasting and Isolation Forest-based anomaly detection. All these factors enable increasing adaptability and robustness of the model in diverse networks.

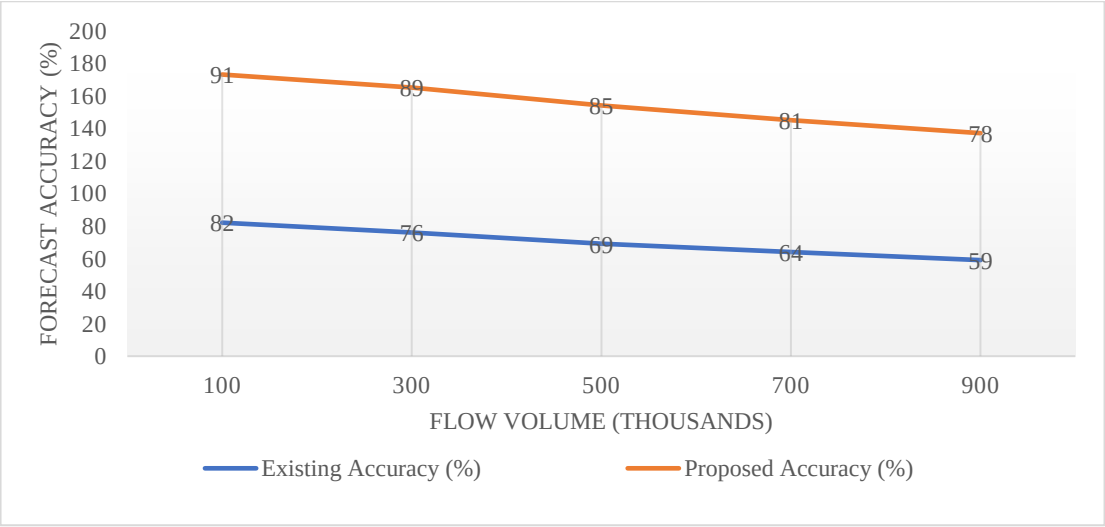

Figure 2: Detection Delay Comparison Over Time

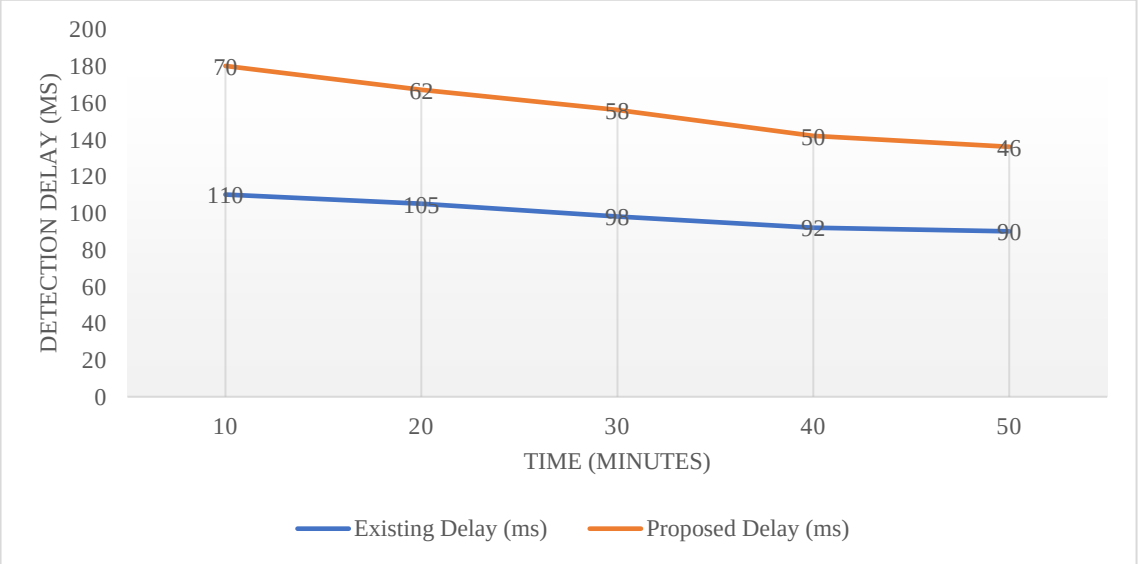

Figure 3: Forecast Accuracy vs Flow Volume

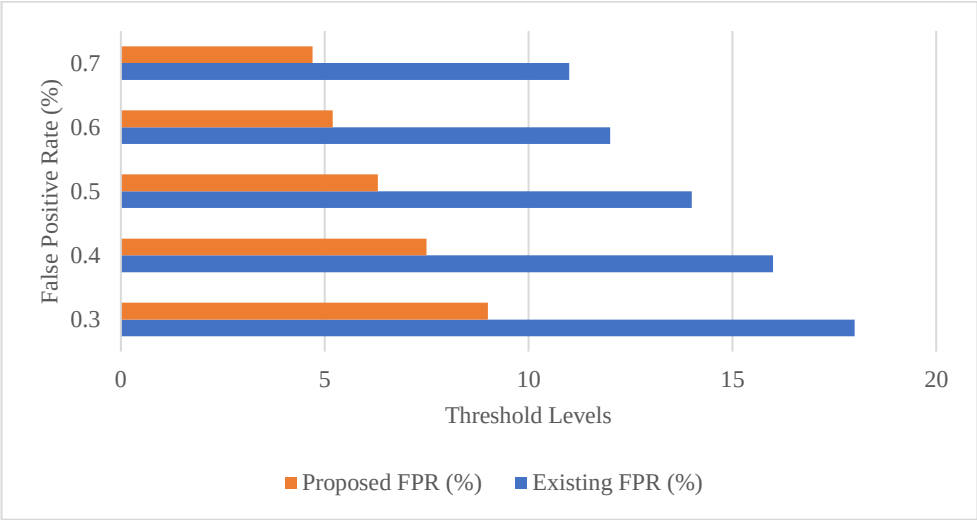

Figure 4: False Positive Rate Analysis

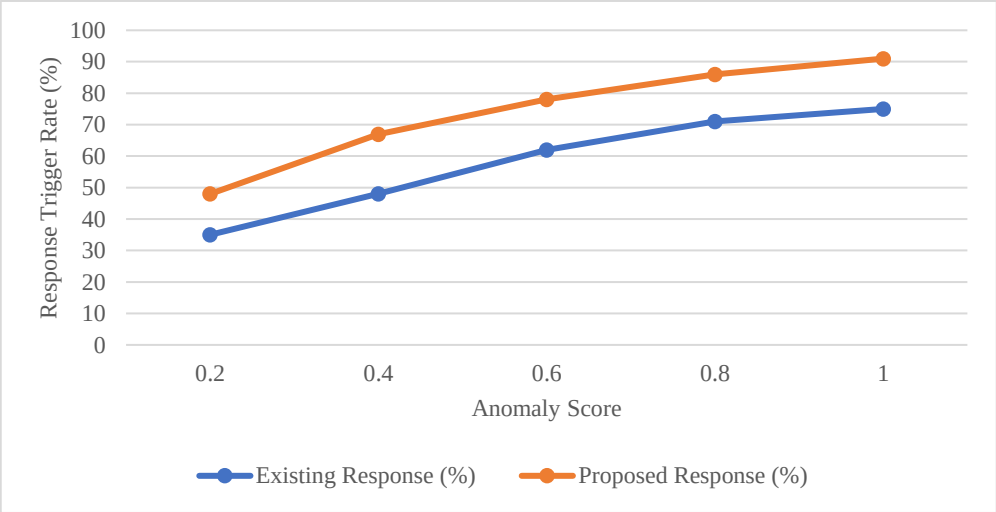

Figure 5: Anomaly Score vs Response Rate

Figures 2 to 5 collectively illustrate the effectiveness of the proposed hybrid anomaly detection model compared to existing methods. Figure 2 shows a consistent reduction in detection delay, with the proposed system identifying anomalies faster over time, which is vital for real-time threat mitigation. Figure 3 demonstrates improved forecasting accuracy, even under high network flow volumes, while Figure 4 highlights a notable reduction in false positive rates across varying thresholds, enhancing system reliability and operational efficiency. Figure 5 confirms that the proposed approach triggers more responsive actions as anomaly scores increase, indicating better sensitivity to threats. Overall, these figures validate the model's enhanced performance in accuracy, speed, and reliability for detecting CBF traffic anomalies.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (11)$$

Eq-11 illustrates the overall effectiveness of the model by calculating the proportion of correctly classified instances (True Positives and True Negatives) among all evaluated samples. Higher accuracy indicates a more reliable anomaly detection system.

$$\text{F1} - \text{score} = \frac{2.\text{precision.Recall}}{\text{Precision+Recall}} \quad (12)$$

Eq-12 illustrates the balance between precision and recall, especially important in imbalanced datasets like network traffic anomalies. A high F1-Score confirms that the model not only detects anomalies accurately but also minimizes false positives and false negatives.

5 Conclusion

This study created a new system for monitoring Core Backbone Flow traffic that uses AI forecasting and the Isolation Forest algorithm with machine learning for anomaly detection. The model predicts current traffic flow and detects deviations in real-time which helps in anomaly detection without the need for labeled datasets. Evaluation on real datasets showed greater accuracy and faster detection time along with reduced false positives when compared with older techniques. This is important for monitoring a backbone network in real-time. The method enhances critical infrastructure internet security by providing a threat detection layer and actively monitoring for potential threats. The model remains effective in controlled environments, but its adaptability to large diverse scalable networks needs more focus. Possible future improvements could incorporate intelligence on threats for stronger resilience, using ensemble methods or other strategies. Greater operational efficiency is achieved when a system provides early warnings, requires less manual oversight, or streamlines processes. This study develops a foundational framework to reinforce backbone environments with advanced cyber defenses. Further refinement will enhance its capabilities for protecting internet systems infrastructure.

References

[1] Barhoumi, E. M., Charabi, Y., & Farhani, S. (2024). *Detailed guide to machine learning techniques in signal processing. Progress in Electronics and Communication Engineering, 2 (1), 39–47*.

[2] Biswas, A. (2024). Modelling an innovative machine learning model for student stress forecasting. *Global Perspectives in Management*, *2*(2), 22-30.

[3] Chandekar, P., Mehta, M., & Chandan, S. (2025). Enhanced anomaly detection in iomt networks using ensemble ai models on the ciciomt2024 dataset. https://doi.org/10.48550/arXiv.2502.11854

[4] Chittipedhi, K., & Sudarsanan, S. (2025). Evaluating the role of mangrove forests in coastal protection and biodiversity enhancement. *International Journal of Aquatic Research and Environmental Studies, 5*(1), 374–389. https://doi.org/10.70102/IJARES/V5I1/5-1-36

[5] Chua, W., Pajas, A. L. D., Castro, C. S., Panganiban, S. P., Pasuquin, A. J., Purganan, M. J., ... & Velasco, L. C. (2024, November). Web Traffic Anomaly Detection Using Isolation Forest. In *Informatics (Vol. 11,* No. 4, p. 83). MDPI. https://doi.org/10.3390/informatics11040083

[6] Djidjev, C. (2024). siForest: Detecting Network Anomalies with Set-Structured Isolation Forest. https://doi.org/10.48550/arXiv.2412.06015

[7] Elsaid, S. A., & Binbusayyis, A. (2024). An optimized isolation forest-based intrusion detection system for heterogeneous and streaming data in the industrial Internet of Things (IIoT) networks. *Discover Applied Sciences*, *6*(9), 483. https://doi.org/10.1007/s42452-024-06165-w

[8] Ginni, G. R., & Chakravarthy, S. (2024). Efficient Outlier Detection in High-Dimensional Data Using Unsupervised Machine Learning. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, *15*(4), 192-212. https://doi.org/10.58346/JOWUA.2024.I4.013

[9] Kulkarni, M., & Sengupta, A. (2022). A Smart City Traffic and Congestion Management System Using Machine Learning. *International Academic Journal of Science and Engineering, 9*(3), 1–5. https://doi.org/10.71086/IAJSE/V9I3/IAJSE0920

[10] Leveni, F., Cassales, G. W., Pfahringer, B., Bifet, A., & Boracchi, G. (2025). Online isolation forest. *arXiv preprint arXiv:2505.09593*. https://doi.org/10.48550/arXiv.2505.09593.
[11] Li, R., Singh, T., & Desai, M. (2023). Real-time anomaly detection in financial data using IForest. *IOP Science, Digital Banking & Security*.
[12] Mahmoudi, S., & Lailypour, C. (2015). A discrete binary version of the Forest Optimization Algorithm. *International Academic Journal of Innovative Research, 2*(2), 60–73.
[13] Muralidharan, J. (2024). Machine learning techniques for anomaly detection in smart IoT sensor networks. *Journal of Wireless Sensor Networks and IoT*, *1*(1), 10-14. https://doi.org/10.31838/WSNIOT/01.01.03
[14] Nadim, I., Rajalakshmi, N. R., & Hammadeh, K. (2024). A Novel Machine Learning Model for Early Detection of Advanced Persistent Threats Utilizing Semi-Synthetic Network Traffic Data. *Journal of VLSI Circuits and Systems*, *6*(2), 31-39. https://doi.org/10.31838/jvcs/06.02.04
[15] Patel, V., Sharma, M., & Jain, R. (2025). AI techniques in telecom anomaly detection: A review. *Telecom Systems, Springer.*
[16] Ritthish, R. V., Logamoorthy, S., Batsha, T., & Balamurugan, K. (2023). Analysis of Network Traffic Using MRF Algorithm in Machine Learning. *International Journal of Advances in Engineering and Emerging Technology*, *14*(1), 185-190.
[17] Utkin, L., Ageev, A., Konstantinov, A., & Muliukha, V. (2022). Improved anomaly detection by using the attention-based isolation forest. *Algorithms*, *16*(1), 19. https://doi.org/10.3390/a16010019
[18] Wang, H., Zhao, L., & Li, F. (2023). IDForest: Incremental Isolation Forest for streaming anomaly detection. *AI & Edge Computing*.
[19] Xiang, H., Zhang, X., Hu, H., Qi, L., Dou, W., Dras, M., ... & Xu, X. (2023). Optiforest: Optimal isolation forest for anomaly detection. *arXiv preprint arXiv:2306.12703*. https://arxiv.org/abs/2306.12703
[20] Xiang, Q., Wu, S., Wu, D., Liu, Y., & Qin, Z. (2025). MindFlow: A Network Traffic Anomaly Detection Model Based on MindSpore. https://doi.org/10.48550/arXiv.2504.17678
[21] Xiang, Q., Wu, S., Wu, D., Liu, Y., & Qin, Z. (2025). Research on CNN-BiLSTM Network Traffic Anomaly Detection Model Based on MindSpore. https://doi.org/10.48550/arXiv.2504.21008
[22] Xu, H., Pang, G., Wang, Y., & Wang, Y. (2023). Deep isolation forest for anomaly detection. *IEEE Transactions on Knowledge and Data Engineering*, *35*(12), 12591-12604. https://doi.org/10.1109/TKDE.2023.3270293
[23] Zhang, Y., Liu, J., & Chen, X. (2025). AI-enhanced forecasting of traffic in CNF and VNF systems. *International Journal of Network Engineering & Applications*.

Authors Biography

Dr.S.N. Rekha is a seasoned academician with over 26 years of experience in teaching. Dr. Rekha S. N. currently serves as a Professor in the Department of Electrical and Electronics Engineering at Sapthagiri NPS University. She holds a B.Tech, M.Tech and PhD degree in Electrical and Electronics Engineering. Dr. Rekha has played a key role in with mentoring students, supervising undergraduate projects, coordinating academic activities, and contributing to curriculum development.

Dr.J. Narendra Babu is a seasoned academician with over 28 years of experience in teaching and software industry, Dr.J. Narendra Babu currently serves as a Professor in the Department of Data Science at Sapthagiri NPS University. He holds a B.Tech, M.Tech and PhD degree. Dr.J. Narendra Babu has published extensively in reputed journals and conferences, Dr.J. Narendra Babu has played a key role in with mentoring students, supervising undergraduate projects, coordinating academic activities, and contributing to curriculum development.

Dr.A. Sathish a seasoned academician with over 22years of experience in teaching Dr.A. Sathish currently serves as an Assistant Professor in the Department of CSE at Sapthagiri NPS University. He holds a M.E and PhD degree. A regular participant in faculty development programs, technical symposiums, and professional workshops, Dr.A. Sathish continually strives to stay at the forefront of advancements in his field, making meaningful contributions to both teaching and research.

Dr.M. Vijaya Lakshmi a seasoned academician with over 23 years of experience in teaching. Dr.M. Vijaya Lakshmi currently serves as a Professor and HOD in the Department of ECE at CREC, Tirupati. She holds a B.Tech, M.Tech and PhD degree in ECE. Dr.M. Vijaya Lakshmi has published extensively in reputed journals and conferences, Dr.M. Vijaya Lakshmi has played a key role in with mentoring students, supervising undergraduate projects, coordinating academic activities, and contributing to curriculum development.

L. Lakshmaiah has completed his B.Tech and M.Tech in Information Technology from reputed institutions and is currently pursuing his Ph.D. from Annamalai University. He has extensive teaching experience and possesses strong knowledge in the field of Computer Science and Engineering. He actively shares his knowledge with students through various means and guides them in writing research papers and conducting quality research work in the field of teaching and learning.

Dr.D. Nageswara Rao is a seasoned academician with over 26 years of experience in teaching; He holds a Ph.D. in CSE and has a strong foundation with an M.Tech from JNTU Hyderabad and an MCA from Osmania University. His academic journey includes roles as Professor and Director across reputed institutions like Chitkara University, Galgotias University, and JigJiga University. Dr. Rao has published extensively in reputed journals and conferences, with significant contributions to AI, machine learning, cybersecurity, and cloud computing. He has been honored with multiple awards, including the Young Researcher Award and Best Senior Faculty Award. Dr. D. Nageswara Rao currently serves as a Professor in the Department of CSE at Sapthagiri NPS University.