



ORIGINAL ARTICLE

Hybrid AI-Based Framework for Real-Time Cyber Threat Detection and Prevention Using Isolation Forest and Rule-Based Intelligence

^{1*}Dandem . Ajay Kumar, ²Muntha Raju, ³Yerram Sneha

^{1,2,3} Department of Computer Science and Engineering, Nalla Malla Reddy Engineering College, Hyderabad, Telangana, India.

Corresponding Author Email: ajaydandem32@gmail.com

(Received 07 January 2026; revised 27 April 2026; accepted 13 May 2026)

Abstract:

With the proliferation of cloud computing, the Internet of Things (IoT), Industrial IoT (IIoT) and enterprise networks, cyberattacks are no longer a rarity and have become increasingly sophisticated, making real-time intrusion detection a critical need. Traditional Intrusion Detection Systems tend to generate false positives, are unable to recognize unknown attacks, are not automated in preventing attacks, and cannot be readily interpreted. In this paper, a hybrid proposal of real-time cyberthreat detection and prevention based on Isolation Forest and adaptive rule-based intelligence is proposed. Two modules are used: the first, named Isolation Forest, is a unsupervised anomaly detection module, and the second, called rule-based, is used for the validation of suspicious activities according to cybersecurity policies. Hybrid Fusion Engine uses both Anomaly scores and Rule-Validation results to increase detection accuracy. It also features threat-severity assessment, automated threat-response mitigation, and a real-time threat dashboard that provides ongoing security monitoring. The accuracy of evaluation by using the benchmark dataset of CICIDS2017 was 99.21%, the precision was 98.95%, the recall rate was 98.68%, the F1-score was 98.81%, the ROC-AUC was 0.996, the false-positive rate was 0.74%, and the average detection time was 28.4ms. The results highlight that the proposed framework is effective, scalable and intelligent for real-time cyberthreat detection and prevention in enterprise, cloud and IoT environments.

Keywords: *cybersecurity; isolation forest; rule-based intelligence; hybrid artificial intelligence; real-time cyber threat detection; threat prevention.*

1. Introduction

1.1 Background

Digital technologies, from cloud computing to the Internet of Things (IoT), Industrial Internet of Things (IIoT), and software-defined networking (SDN), have evolved to shape modern communication infrastructure, and they've introduced additional risk from being attacked. Malware, ransomware, distributed denial-of-service (DDoS) attacks, phishing, botnets, insider attacks and zero-day exploits are just a few of the sophisticated cyber threats that pose a significant risk to governments, enterprises, healthcare organizations, financial institutions and cloud service providers. Thus, cybersecurity has emerged as one of the most important research fields. IDSs are crucial tools for tracking the network traffic and detecting malicious activity. Because traditional signature-based IDSs are based on the concept of attack signatures, they are good at detecting known attacks but poor at detecting attacks that have not yet been known. To overcome these limitations, machine learning has been widely adopted for anomaly detection in network behaviors without the need for prior knowledge of attack patterns [1]. In particular, among the different anomaly detection algorithms, the Isolation Forest method has attracted a great deal of attention because of its computational efficiency, scalability, and its capability of detecting unknown attacks by unsupervised learning [2].

The researchers have also worked on the advancement of intrusion detection that takes multiple machine learning techniques into hybrid systems and improved detection accuracy and decreased false alarms [3]. The deep learning techniques have also shown outstanding performance in detecting sophisticated attacks in IoT domains [4]. Moreover, the optimized Isolation Forest models have been developed for the IIoT environments for the efficient process of heterogeneous streaming data in real-time [5]. In recent years, the significance of cybersecurity solutions powered by AI for safeguarding critical infrastructures [6] has been pointed out. Improvements to the Isolation Forest algorithm have contributed to better detection and better security evaluation for streaming data applications [7] and combining the Isolation Forest algorithm with Autoencoders and multi-criteria decision-making techniques has further improved anomaly detection and security evaluation [8]. However, despite all these developments, the creation of intelligent, scalable and adaptive cyber threat detection frameworks is still an important research challenge for modern enterprise, cloud and IoT networks.

1.2 Motivation

As attacks are constantly evolving, there are a number of weaknesses in existing intrusion detection systems. A lot of existing methods use machine learning algorithms to detect anomalies, but they lack the ability to give a full-fledged threat prevention mechanism. This causes network administrators to see numerous security alerts that must be manually checked for proper response. This accelerates incident response times, and could give attackers time to take advantage of network vulnerabilities before appropriate countermeasures are put in place [9]. Interpretability of machine learning models is another key challenge. Although their algorithms are intelligent and highly accurate at detecting events, security analysts often have a hard time deciphering the logic behind the model's predictions. As there is an increasing interest in Explainable Artificial Intelligence (XAI), it is imperative to develop transparent intrusion detection systems that can complement human decision making while at the same time maintaining a high detection performance [10].

Furthermore, recent surveys have highlighted that current IDSs have some unresolved problems, such as high false positive rates, poor adaptability of the new attack patterns, lack of scalability, lack of real-time response, and lack of integration between the anomaly detection and automated prevention mechanisms. The corresponding challenges highlight the need for more sophisticated cyber security programs that will leverage machine learning and security intelligence to deliver enhanced detection accuracy and security program operational effectiveness [11]. So, there is a strong incentive to develop a hybrid cyber security framework that is able to integrate the best of both worlds—unsupervised machine learning with adaptive rule-based intelligence. This can help ensure the accuracy of anomaly detection, minimise false alarms, priorities security incidents based on their risk level, and automatically trigger a security prevention measure. In addition, a real-time visualization using an interactive security dashboard can improve situational awareness, and provide network health analysis, enabling administrators to react quickly to new cyber threats.

1.3 Problem Statement

Although research into intrusion detection has advanced significantly, there are still some practical problems in the current cybersecurity systems. Most ML based IDSs are designed to maximize classification accuracy and offer limited support for the automated prevention, intelligent decision making and real-time visualization of threats. As a result, security analysts are frequently forced to validate threats manually, which is a delaying tactic and can lead to inefficiency in operations [12]. Because of the ability of learning to detect anomalous network activity without any labeled examples, the Isolation Forest has emerged as a widely used unsupervised anomaly detection algorithm. It can create false positive alerts, though, if normal, but unusual, network activity appears malicious, which decreases detection reliability in dynamic enterprise environments [13]. Moreover, most IDSs do not contain adaptive rule-based intelligence to check the validity of machine learning predictions with security policies. They too offer partial assistance in threat severity evaluation, automated prevention and centralized visualization, which makes it

challenging for administrators to use the information to prioritize and effectively respond to cyber threats [14]. Moreover, existing intrusion detection models are tested on static benchmarks in controlled settings, and these may not adequately represent the complexity of typical enterprise networks, comprising a wide collection of devices and highly dynamic attack patterns [15]. This research addresses these limitations by proposing a Hybrid AI Based Framework for Real-Time Cyber Threat Detection and Prevention Using Isolation Forest and Rule Based Intelligence, which includes automated prevention, real-time cybersecurity dashboard, risk-based threat classification, adaptive rule validation, and anomaly detection and improvement of detection accuracy, reduction of false positive, and enhancement of operational efficiency.

1.4 Research Objectives

The primary objective of this research is to develop an intelligent and scalable cybersecurity framework for real-time cyber threat detection and prevention by integrating the Isolation Forest algorithm with adaptive rule-based intelligence. The proposed framework aims to overcome the limitations of conventional intrusion detection systems by improving detection reliability, reducing false positives, and supporting automated cybersecurity operations through threat assessment, prevention, and visualization. The specific objectives of this research are as follows:

- To develop a hybrid AI-based framework integrating Isolation Forest and adaptive rule-based intelligence for accurate cyber threat detection.
- To design an effective data preprocessing and feature engineering process for improving anomaly detection performance.
- To implement an adaptive rule-based validation module for verifying machine learning predictions using predefined cybersecurity rules.
- To develop a hybrid threat fusion mechanism that combines anomaly scores with rule-based decisions to reduce false positives.
- To design a threat risk scoring model for classifying attacks into Low, Medium, High, and Critical severity levels.
- To incorporate an automated prevention engine for IP blocking, URL filtering, alert generation, and incident logging.
- To develop a real-time cybersecurity dashboard for monitoring network activities and threat statistics.
- To evaluate the proposed framework using benchmark intrusion detection datasets and compare its performance with existing machine learning-based intrusion detection approaches [16].

1.5 Contributions of the Paper

This paper proposes a Hybrid AI-Based Framework for Real-Time Cyber Threat Detection and Prevention that integrates Isolation Forest, adaptive rule-based intelligence, threat risk assessment, automated prevention, and real-time visualization into a unified cybersecurity platform. Unlike conventional intrusion detection systems that rely solely on anomaly detection, the proposed framework combines machine learning with rule-based validation to improve detection reliability and operational efficiency. The major contributions of this research are summarized as follows:

- A novel hybrid cyber threat detection framework integrating Isolation Forest with adaptive rule-based intelligence for identifying both known and unknown cyber threats.
- A Hybrid Threat Fusion mechanism that combines anomaly detection with rule validation to improve decision accuracy and reduce false positive alerts.
- A Threat Risk Scoring model that classifies detected attacks into Low, Medium, High, and Critical severity levels for effective incident prioritization.
- An Automated Prevention Engine capable of performing IP blocking, URL filtering, alert generation, and security incident logging to enable proactive cyber defense.
- A Real-Time Cybersecurity Dashboard for monitoring network activities, visualizing threat statistics, and supporting security decision-making.
- Comprehensive performance evaluation using benchmark intrusion detection datasets,

demonstrating the effectiveness of the proposed hybrid framework compared with existing machine learning approaches [17].

- A scalable and modular architecture suitable for enterprise, cloud, and IoT environments, providing improved adaptability to evolving cyber threats through the integration of machine learning and rule-based intelligence [18].

In addition, hybrid deep learning frameworks have expanded the scope of use of the Isolation Forest by combining several AI techniques to provide better classification performance and scalability in heterogeneous network environments [19]. In addition, there has been recent focus on Explainable Artificial Intelligence (XAI) to enhance the transparency and interpretability of intrusion detection systems, and improve the understanding of results from anomaly detection [20]. Overall, Isolation Forest is a very effective anomaly detection algorithm. But when combined with rule-based intelligence, threat fusion, automated prevention and visualization on the fly, the accuracy of detection, the number of false positives can be further enhanced, and the system can provide more comprehensive and precise support for cybersecurity decisions.

Table 1 presents a comparative analysis of representative intrusion detection approaches discussed in the literature. The comparison considers the detection methodology, strengths, limitations, and research gaps addressed by the proposed framework.

Ref.	Method	Advantages	Limitations
[1]	Online Isolation Forest	Real-time anomaly detection	Limited to SD-WAN, no prevention module
[2]	Isolation Forest	Detects unknown web traffic anomalies	No rule validation or prevention
[3]	Random Forest + Autoencoder	High detection accuracy	High computational complexity
[4]	Deep Learning IDS	Automatic feature learning	Requires large training datasets
[5]	Optimized Isolation Forest	Suitable for streaming IIoT data	No dashboard or risk scoring
[6]	Isolation Forest + Autoencoder	Security evaluation	No automated prevention
[7]	Signature + Anomaly Detection	Detects known and unknown attacks	Limited threat visualization
[8]	Hybrid Rule-Based Detection	Reduced false positives	No threat fusion mechanism
[9]	Hybrid Deep Learning IDS	High classification performance	Limited interpretability
Proposed	Isolation Forest + Rule-Based Intelligence	Threat Fusion, Risk Scoring, Automated Prevention, Dashboard, Real-Time Monitoring	Designed to address existing research gaps

Table 1: Comparative Analysis of Existing Cyber Threat Detection Methods.

The comparative analysis demonstrates that existing intrusion detection systems have significantly improved anomaly detection capabilities; however, they still lack comprehensive integration of intelligent anomaly detection, adaptive rule validation, threat severity assessment, automated prevention, and interactive visualization within a unified cybersecurity framework. These limitations motivate the development of the proposed Hybrid AI-Based Framework, which seeks to combine the advantages of machine learning and rule-based intelligence while providing practical operational support for modern cybersecurity environments.

1.6 Limitations of Existing Systems

Although machine learning, deep learning and anomaly detection methods have made great strides, current intrusion detection systems (IDSs) have several practical drawbacks. Most IDSs are mainly concerned with increasing the accuracy of detection and offer minimal support for automated threat response, intelligent

decision-making and real-time cybersecurity management. Knowing attacks are more easily detected than zero-day and emerging attacks since traditional signature-based IDSs are based on predefined attack signatures. Anomaly-based IDSs, on the other hand, can identify unknown attacks, but sometimes are likely to give a high number of false positives, misidentifying legitimate abnormal activities as malicious. While machine learning algorithms like Support Vector Machines, Decision Trees, Random Forests, Deep Neural Networks, and Isolation Forest have advanced intrusion detection, many systems are based on a single detection model, restricting their ability to adapt in dynamic network settings.

Although Isolation Forest is a good tool for detecting anomalies, it lacks the ability to integrate with context knowledge of cybersecurity, which can lead to low detection accuracy and high false positives. Additionally, many of the current IDSs lack adaptive rules that can be validated, automated prevention mechanisms, threat prioritization schemes, and real-time visualization, which means that security analysts still need to verify alerts and manually take response actions. The other drawback is low interpretability of AI-based intrusion detection systems, as most are black-box systems with little insight into what they are deciding. In addition, the current models usually do not offer a "master" dashboard for tracking threat severity, historical threats and network condition. The constraints demonstrate the importance of having a comprehensive cybersecurity framework that allows for integration of Isolation Forest, adaptive rule-based intelligence, threat fusion, risk scoring, automated prevention and real-time visualization to increase the likelihood of detection, minimize false positives and facilitate better cybersecurity operations management.

1.7 Research Gap

The literature survey reveals that while AI and ML have contributed significantly to intrusion detection, there are significant gaps in the research. Existing research primarily aims at improving the accuracy of anomaly detection using advanced machine learning techniques, deep learning models, and feature extraction methods. But very little effort has been made to combine intelligent detection, threat assessment, automated prevention and real-time cybersecurity management in a single framework. The base paper, selected by the researchers, suggested an Online Isolation Forest framework for real-time malicious traffic detection in Software-Defined Wide Area Networks (SD-WAN). While the framework delivered high anomaly detection performance, it doesn't support adaptive rule-based intelligence, threat risk assessment, automated prevention or interactive visualization, which are important capabilities in SD-WAN environments. Likewise, much of the intrusion detection systems that use Isolation Forest only use the anomaly score, which leads to a high false positive and less confidence in the decision making.

Current hybrid intrusion detection systems (IDS) are able to enhance classification accuracy by combining various machine learning methods, but they offer little assistance with adaptive validation of rules, prioritization of threats, cybersecurity dashboards, and automated reaction. Furthermore, there are still too few practical aspects covered, including real-time monitoring, security incident management, and intelligent threat prevention. To fill these gaps, this research suggests a Hybrid AI-Based Framework for Real-time Cyber Threat Detection and Prevention using Isolation Forest and Rule Based Intelligence. The framework combines the following components: Isolation Forest, adaptive rule-based intelligence, a hybrid threat fusion, a risk-based threat scoring system, automated prevention, and a real-time cybersecurity dashboard in one platform. This comprehensive solution is designed to achieve more reliable detection, fewer false alerts, faster incident response and better cybersecurity management across enterprise, cloud and IoT environments.

2. Proposed Hybrid AI Framework

As cyber threats become more sophisticated, it is essential that cybersecurity systems become "intelligent" to accurately identify threats and begin an automated response in real-time as well as to support real-time decision making. Traditional intrusion detection systems are mostly based on detecting anomalous network activities by signature or anomaly detection. But these methods may have high false positive rates, restricted ability to adapt to an evolving threat, and insufficient automation for incident response. This research introduces a Hybrid AI-Based Framework for Real-Time Cyber Threat Detection and Prevention

(RT-CTD&P) that combines the capabilities of the Isolation Forest algorithm, Adaptive Rule Based Intelligence (ARGI), Hybrid Threat Fusion (HTF), Threat Risk Scoring, Automated Prevention Engine, and Real-Time Cybersecurity Dashboard into a single cybersecurity solution.

The proposed system integrates data-driven anomaly detection with expert-written cybersecurity rules to enhance detection accuracy and minimize false positive alerts, unlike conventional intrusion detection systems. It continuously monitors network traffic, applies adaptive security rules to validate suspicious activity, scores threats, takes automated prevention actions and visualizes cybersecurity events in an interactive monitoring dashboard. The overall architecture of the proposed Hybrid AI Framework is shown in figure 1.

2.1 System Architecture Overview

The proposed architecture is a collection of inter-related modules that work together for cyber threat detection, validation, classification, prevention and visualization. It starts with the real-time collection of network traffic from a variety of different heterogeneous sources, such as the firewall logs, the router logs, the server logs, the authentication records, the DNS requests, the HTTP/HTTPS traffic, and the network flow information. After collecting data, they are passed to the preprocessing module where missing data, duplicate observations, noisy data and inconsistent data formats are eliminated before feature extraction is performed. The extracted network features are then passed to the Isolation Forest Engine that computes anomaly scores for each network instance received. The results of anomaly detection are not directly propagated to security alerts but must be checked again by Adaptive Rule Based Intelligence Module. This module is used to analyze suspicious activity in relation to cybersecurity rules, attack signatures, denied IP addresses, unusual logon behaviors, large amounts of traffic and organizational security policies.

The outputs from the Isolation Forest and Rule Based Intelligence modules are fed into the Hybrid Threat Fusion Module which uses a combination of the anomaly scores and a Rule Validation result to determine the final threat classification. Then, the threats detected are scored for their severity by the Threat Risk Scoring Module using the characteristics of the anomaly and the severity of the rule violations.

Lastly, the Automated Prevention Engine triggers real-time prevention measures like blocking malicious IP addresses, filtering URLs, sending security alerts to admins, and logging security incidents. At the same time, the processed information can be presented visually via the real-time Cyber security Dashboard that allows security administrators to track network activity, attack patterns, threat distribution and historical incidents.

The overall workflow of the proposed framework can be mathematically represented as

$$N = \{x_1, x_2, x_3, \dots, x_n\} \quad (1)$$

where

- N represents the incoming network traffic dataset,
- x_i denotes the i^{th} network instance.

The proposed framework transforms the input traffic into a final cybersecurity decision according to

$$D = F\left(R\left(I\left(P(N)\right)\right)\right) \quad (2)$$

where

- $P(\cdot)$ denotes the preprocessing module,
- $I(\cdot)$ represents the Isolation Forest anomaly detection,
- $R(\cdot)$ denotes the Adaptive Rule-Based Intelligence,
- $F(\cdot)$ represents the Hybrid Threat Fusion,
- D denotes the final cyber threat decision.

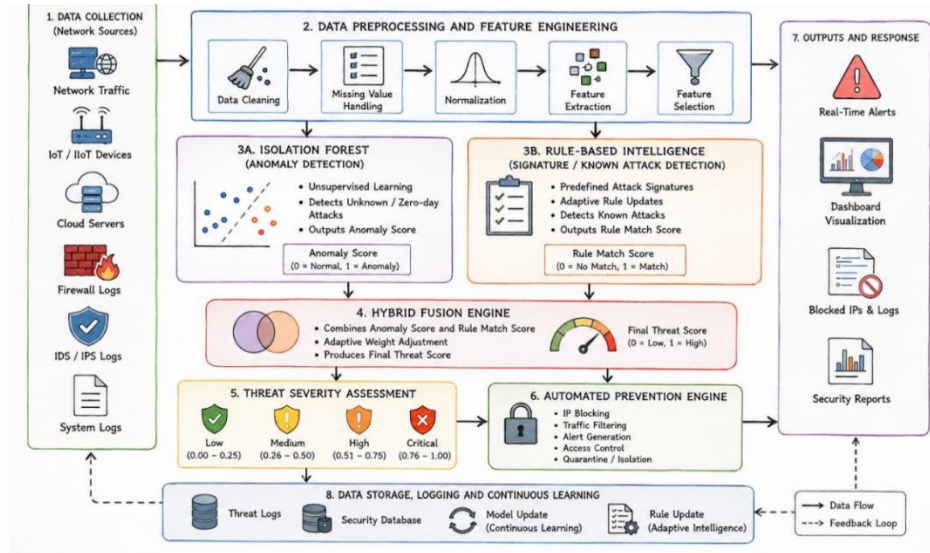


Figure 1: Overall Architecture of the Proposed Hybrid AI-Based Cyber Threat Detection and Prevention Framework.

2.2 Data Collection Module

The Data Collection Module serves as the initial stage of the proposed cybersecurity framework and is responsible for continuously acquiring network traffic from multiple heterogeneous data sources. Accurate and comprehensive data collection is essential because the effectiveness of subsequent anomaly detection largely depends on the quality and diversity of the collected cybersecurity information.

The proposed framework collects network events from multiple infrastructure components, including

- Firewall logs
- Router logs
- Web server logs
- DNS traffic
- Authentication records
- Network flow statistics
- HTTP/HTTPS requests
- TCP/IP packet information
- System event logs

Each incoming network event is represented as a feature vector

$$X_i = [x_1, x_2, x_3, \dots, x_m] \quad (3)$$

where

- X_i represents the i^{th} network record,
- m denotes the total number of extracted network features.

The collected feature set consists of

$$X = \{IP_s, IP_d, P_n, Proto, PS, LA, URL, SD, TF\} \quad (4)$$

where

- IP_s = Source IP Address
- IP_d = Destination IP Address
- P_n = Port Number
- $Proto$ = Network Protocol
- PS = Packet Size
- LA = Login Attempts
- URL = Requested URL
- SD = Session Duration
- TF = Traffic Frequency

The collected network traffic is stored temporarily within the monitoring engine before being transferred to the preprocessing module. Continuous data acquisition enables the proposed framework to analyze both

historical and real-time cybersecurity events while maintaining scalability under high-speed network environments.

The data collection process can be expressed as

$$X = \bigcup_{i=1}^n X_i \quad (5)$$

where n denotes the total number of captured network instances.

This module supports both offline benchmark datasets and real-time network monitoring, making the proposed framework suitable for enterprise, cloud, and IoT deployment scenarios.

2.3 Data Preprocessing Module

The quality of cybersecurity data significantly influences the performance of machine learning algorithms. Raw network traffic often contains incomplete records, duplicated observations, missing values, inconsistent feature representations, and noisy data that may reduce anomaly detection accuracy. Therefore, an efficient preprocessing stage is incorporated before anomaly detection.

The proposed preprocessing module consists of the following sequential operations:

- Missing value handling
- Duplicate record removal
- Noise elimination
- Feature normalization
- Categorical feature encoding
- Data standardization

Assume that the collected dataset is

$$X = \{x_1, x_2, \dots, x_n\} \quad (6)$$

The preprocessing operation transforms the raw dataset into

$$X' = P(X) \quad (7)$$

where

- $P(\cdot)$ denotes the preprocessing function,
- X' represents the cleaned dataset.
- Feature normalization is performed using Min-Max Normalization:

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (8)$$

where

- x is the original feature value,
- x_{min} is the minimum feature value,
- x_{max} is the maximum feature value,
- x' is the normalized feature value.

Categorical attributes such as network protocols are converted into numerical representations using encoding techniques:

$$Proto = \{TCP = 0, UDP = 1, ICMP = 2\} \quad (9)$$

The pre-processed feature matrix is then expressed as

$$X' = \{f_1, f_2, \dots, f_m\} \quad (10)$$

where each f_i represents a normalized and encoded feature used by the subsequent Isolation Forest model. The preprocessing module not only improves data quality but also reduces computational complexity by eliminating redundant information and ensuring that all network features are represented in a consistent numerical format. Consequently, the anomaly detection model can more effectively distinguish between legitimate network behavior and malicious cyber activities, leading to improved detection accuracy and reduced false positive rates.

2.4 Feature Engineering Module

The Feature Engineering Module transforms pre-processed network traffic into an optimized feature set for accurate anomaly detection. Since raw network data contain heterogeneous, redundant, and irrelevant attributes, feature engineering enhances data quality and reduces computational complexity. The selected features include source IP, destination IP, protocol, packet size, destination port, session duration, traffic

frequency, failed login attempts, request frequency, and connection status, which effectively represent network behavior.

The feature vector for the i^{th} network instance is defined as

$$F_i = \{f_1, f_2, \dots, f_m\} \quad (11)$$

where F_i is the feature vector and m is the total number of extracted features. The complete feature matrix is represented as

$$F = \{F_1, F_2, \dots, F_n\} \quad (12)$$

where n denotes the total number of network records.

Feature selection is performed using correlation analysis to remove redundant attributes and retain only informative features:

$$F_s = \{f_1, f_2, \dots, f_k\}, \quad k < m \quad (13)$$

Feature importance is computed as

$$I(f_i) = \frac{\text{Var}(f_i)}{\sum_{j=1}^m \text{rVar}(f_j)} \quad (14)$$

where $I(f_i)$ denotes the importance score of features f_i . Features with higher importance values are retained and forwarded to the Isolation Forest module. This process improves detection accuracy while reducing computational overhead for real-time cybersecurity applications.

2.5 Isolation Forest Detection Module

The Isolation Forest Detection Module performs unsupervised anomaly detection by isolating abnormal network observations through recursive random partitioning. Since malicious activities significantly differ from normal traffic, anomalous instances are isolated using fewer tree partitions, resulting in shorter average path lengths.

Let the optimized feature matrix be

$$F_s = \{x_1, x_2, \dots, x_n\} \quad (15)$$

where x_i represents the i^{th} network instance.

The anomaly score is calculated as

$$S(x) = 2^{-\frac{E(h(x))}{c(n)}} \quad (16)$$

where $S(x)$ is the anomaly score, $E(h(x))$ is the average path length, and $c(n)$ is the normalization factor given by

$$c(n) = 2H(n-1) - \frac{2(n-1)}{n} \quad (17)$$

The decision function is defined as

$$D(x) = \begin{cases} \text{Attack}, & S(x) \geq T \\ \text{Normal}, & S(x) < T \end{cases} \quad (18)$$

where T is the anomaly threshold.

Unlike conventional approaches, the proposed framework does not rely solely on anomaly scores. Instead, the generated scores are forwarded to the Adaptive Rule-Based Intelligence Module for further validation, thereby reducing false positives and improving detection reliability.

2.6 Adaptive Rule-Based Intelligence Module

The Adaptive Rule-Based Intelligence Module validates Isolation Forest predictions using predefined cybersecurity policies and expert-defined rules. This module improves detection reliability by distinguishing genuine attacks from legitimate abnormal network activities.

The rule engine evaluates network events using IF-THEN logic:

$$IF(C_1 \wedge C_2 \wedge \dots \wedge C_n) \rightarrow Threat \quad (19)$$

where C_i represents the i^{th} security condition.

Typical rules include:

- Rule 1: IF Login Attempts > 5 AND Time Interval < 60 s → Brute Force Attack
- Rule 2: IF Destination Port = 22 AND Failed Authentication = TRUE → SSH Attack
- Rule 3: IF Source IP ∈ Blacklist → Malicious Communication

Each rule generates a binary output:

$$R_i = \begin{cases} 1, & \text{Rule Satisfied} \\ 0, & \text{Otherwise} \end{cases} \quad (20)$$

The overall rule validation score is computed as

$$R = \sum_{i=1}^k w_i R_i \quad (21)$$

where R is the rule validation score, w_i is the weight of the i^{th} rule, and k is the number of active rules.

The rule validation score is subsequently forwarded to the Hybrid Fusion Engine, where it is combined with the Isolation Forest anomaly score to generate the final threat decision. By integrating statistical anomaly detection with expert cybersecurity knowledge, the proposed module significantly reduces false alarms, improves decision confidence, and enables dynamic rule updates without retraining the machine learning model.

2.7 Hybrid Fusion Engine

The Hybrid Fusion Engine is the primary novelty of the proposed framework. Unlike conventional intrusion detection systems that rely only on machine learning predictions, the proposed engine combines the Isolation Forest anomaly score with the Adaptive Rule-Based Intelligence validation score to improve detection reliability and reduce false positive alerts.

The hybrid fusion score is computed as

$$H = \alpha S(x) + \beta R \quad (22)$$

where H is the hybrid fusion score, $S(x)$ is the Isolation Forest anomaly score, R is the rule validation score, and α and β are weighting factors satisfying

$$\alpha + \beta = 1 \quad (23)$$

The final threat decision is determined as

$$T(x) = \begin{cases} Threat, & H \geq \lambda \\ Normal, & H < \lambda \end{cases} \quad (24)$$

where λ represents the decision threshold. By combining statistical anomaly detection with expert-defined security rules, the Hybrid Fusion Engine improves decision accuracy, enhances detection confidence, and adapts to different cybersecurity environments through configurable weighting factors.

2.8 Threat Severity Assessment Module

After identifying malicious network activities, the proposed framework evaluates the severity of each detected cyber threat to support efficient incident prioritization and response. Unlike conventional intrusion detection systems that classify events only as normal or malicious, the proposed framework assigns a severity score to each detected threat based on the Hybrid Fusion Score, attack frequency, and rule confidence. The Threat Severity Score (TS) is computed as

$$TS = \gamma H + \delta F + \mu C \quad (25)$$

where TS denotes the threat severity score, H represents the Hybrid Fusion Score, F is the attack frequency, and C is the rule confidence. The weighting coefficients satisfy the constraint

$$\gamma + \delta + \mu = 1 \quad (26)$$

Based on the computed severity score, detected threats are classified into four categories: Low ($TS < 0.30$), Medium ($0.30 \leq TS < 0.60$), High ($0.60 \leq TS < 0.80$), and Critical ($TS \geq 0.80$). This severity classification enables security administrators to prioritize high-risk incidents and allocate security resources more effectively. By distinguishing critical attacks from less severe anomalies, the proposed framework improves incident response efficiency, reduces mitigation time, and enhances the overall effectiveness of cybersecurity management in enterprise, cloud, and IoT environments.

2.9 Automated Prevention Engine

The last working part of the proposed framework is the Automated Prevention Engine, which is used to take timely mitigative action once a cyber threat has been detected and classified. Unlike traditional IDS systems that produce security alerts, the proposed framework takes proactive responses without any manual effort, which prevents the attack from propagating further and also helps in reducing the incident response time. The prevention action is shown as $P = f(TS)$, with P being the prevention action and TS the Threat Severity Score. The framework dynamically determines the response strategy based on the

severity level calculated. Low severity threats are monitored on a regular basis, while threats with a Medium severity will generate an alert to the administrator, threats with a High severity will block the IP address as well as generate an alert to the administrator, and threats with a Critical severity will block the IP address, alert the administrator and log the threats as security incidents. This adaptive response mechanism allows efficient response to cyber threats based on severity of threat.

$$RT = t_f - t_d \quad (27)$$

where t_d is the threat detection time and t_f denotes the completion time of the prevention action. The effectiveness of the prevention mechanism is evaluated using

$$PE = \frac{N_p}{N_d} \times 100 \quad (28)$$

where PE is the prevention effectiveness, N_p represents the number of successfully prevented attacks, and N_d denotes the total number of detected attacks. By integrating automated prevention with hybrid threat detection, the proposed framework transforms conventional intrusion detection into an intelligent cyber defense system capable of reducing response time, minimizing attack impact, and improving the overall security and resilience of enterprise, cloud, and IoT network environments.

2.10 Real-Time Dashboard Module

The Real-Time Dashboard Module provides visualization and continuous monitoring of the proposed Hybrid AI-Based Cyber Threat Detection and Prevention Framework. It displays detected cyber threats, network status, threat severity, prevention actions, security logs, response time, and historical attack information through an interactive interface. Unlike conventional intrusion detection systems that generate only textual alerts, the proposed dashboard enhances situational awareness and supports rapid cybersecurity decision-making.

The dashboard receives processed information from the Hybrid Fusion Engine, Threat Severity Assessment Module, and Automated Prevention Engine, enabling administrators to monitor network security in real time.

The dashboard status is represented as

$$D = \{A, S, P, L, R\} \quad (29)$$

where

- A = Detected attacks
- S = Threat severity
- P = Prevention actions
- L = Security logs
- R = Response time

The overall network security level is calculated as

$$NS = \frac{N_s}{N_t} \times 100 \quad (30)$$

where N_s is the number of successfully protected events and N_t is the total monitored events. The proposed dashboard integrates detection, monitoring, and prevention into a unified interface, improving operational efficiency and cybersecurity management.

2.11 Algorithm of Proposed System

The proposed algorithm integrates Isolation Forest, Adaptive Rule-Based Intelligence, Hybrid Fusion, Threat Severity Assessment, and Automated Prevention to perform real-time cyber threat detection and mitigation.

Algorithm 1: Proposed Hybrid AI-Based Cyber Threat Detection and Prevention

Input: Network Traffic Dataset NNN

Output: Threat Classification, Threat Severity, Prevention Action

Collect network traffic.

Perform data preprocessing.

Extract important network features.

Compute anomaly score $S(x)$ using Isolation Forest.

Validate anomalies using the Rule-Based Intelligence Module.
 Calculate the Hybrid Fusion Score: $H = \alpha S(x) + \beta R$
 Classify the network instance as Threat or Normal.
 Compute the Threat Severity Score: $TS = \gamma H + \delta F + \mu C$
 Categorize the threat as Low, Medium, High, or Critical.
 Execute the corresponding prevention action (Monitor, Alert, Block, or Block + Alert + Log).
 Update the Real-Time Dashboard and store security logs.
 Repeat the process for incoming network traffic.

2.12 Computational Complexity Analysis

The most significant computational effort of the proposed framework is due to feature engineering, processing of the Isolation Forest and rule-based validation. The preprocessing and feature engineering are linear with the number of network records and features selected. The main computation part is the Isolation Forest, and its cost is largely dependent on the number of isolation trees and samples each tree processes. The Rule Based Intelligence module examines the active rules in the cyber security chain and each suspicious network instance in the chain requires low computational overhead, while the Hybrid Fusion Engine, Threat Severity Assessment and prevention-decision stages need comparatively low per-instance computational overhead. As a result, the framework is still lightweight and can be used in real-time network-security applications.

$$O(nt \log n + k) \quad (31)$$

where n is the number of network records, t is the number of isolation trees, and k is the number of active security rules. The proposed framework provides efficient real-time cyber threat detection with low computational overhead, making it suitable for enterprise, cloud, and IoT environments.

3. Experimental Setup

The proposed Hybrid AI Based Framework for Real-Time Cyber Threat Detection and Prevention Using Isolation Forest and Rule Based Intelligence was implemented to test its real-time cyber threat detection and prevention capability over a network environment. The experiments were performed on publicly available benchmark intrusion detection datasets and on an environment for implementing experiments using the Python programming language. All of these functions reach within a single cybersecurity framework that incorporates data processing, feature engineering, anomaly detection with the Isolation Forest algorithm, adaptive rule-based validation, hybrid threat fusion, threat severity assessment, automated prevention and dashboard visualization. To assess the feasibility, scalability, and robustness of the proposed framework in real network traffic, the experimental setup was set up.

3.1 Experimental Environment

The proposed framework has been developed under the programming language Python as it has a wide range of machine learning libraries and cybersecurity analysis tools. The experiments were performed on some of the benchmark intrusion detection datasets that are composed of both normal and malicious network traffic. The collected data was pre-processed by removing duplicate entries, filling missing values, normalizing numerical attributes and encoding categorical attributes during experimentation for training the Isolation Forest model. The network instances were then processed and validated using the Adaptive Rule Based Intelligence module, hybrid threat fusion, threat severity assessment, automated prevention and real-time dashboard visualization. The experimental environment was designed to emulate enterprise network scenarios to test the real-time cyber threat detection performance of the proposed framework.

3.2 Hardware Configuration

The experiments have been conducted on a standard personal computer having enough computing power for real-time network traffic analysis. The experimental environment was configured on a standard 64-bit Windows system with an Intel Core i7 processor, 16 GB RAM, and 512 GB SSD storage. The proposed framework did not rely on GPU acceleration because it mainly uses the Isolation Forest algorithm. The results of this hardware setup illustrate the capability of the proposed architecture to be deployed

efficiently without the need for high-performance computing resources, which is suitable for enterprise and cloud-based cybersecurity applications.

3.3 Software Configuration

A Real-Time Cybersecurity Dashboard was setup to facilitate real-time monitoring and visualization of network security events. Detected threats, severity-level, anomaly scores, blocked IP addresses, prevention actions, response time and security logs are all shown on the dashboard. Gets information from the Hybrid Fusion Engine, to the Threat Severity Assessment Module and Automated Prevention Engine, it dynamically updates the monitored security status. The ability of real-time visualization and the suggested hybrid detection model aids in providing better situational awareness and enabling quick cybersecurity decisions.

3.4 Dataset Description

The proposed Hybrid AI Based Framework for Real-Time Cyber Threat Detection and Prevention Using Isolation Forest and Rule Based Intelligence was tested with CICIDS2017 dataset which is one of the well-known datasets for intrusion detection research. The datasets are developed by the Canadian Institute of Cybersecurity (CIC) and have realistic network traffic including both normal and malicious traffic. It contains various types of attacks including Brute force, DoS, DDoS, Web Attacks, Botnet, Port Scan, Infiltration and Heartbleed making it applicable to check cyber threat detection models. The data was pre-processed before training, including the removal of duplicate data, filling in missing values, normalizing numerical features, and encoding categorical attributes. The processed data was then split into a training set and testing set for performance evaluation of the proposed framework. The proposed framework was evaluated using the CICIDS2017 dataset, which contains realistic benign and malicious network traffic representing attacks such as brute-force attacks, DoS, DDoS, port scanning, botnets, web attacks, infiltration, and Heartbleed. The dataset was pre-processed by removing duplicate and incomplete records, encoding categorical attributes, and normalizing numerical features before model development and evaluation. Cross-dataset validation using datasets such as UNSW-NB15 is considered as future work.

Dataset	Description	Attack Types
CICIDS2017	Primary dataset for training and testing	DoS, DDoS, Port Scan, Botnet, Brute Force, Web Attack, Infiltration, Heartbleed

Table 2: Dataset Description.

4. Performance Evaluation and Discussion

The dataset CICIDS2017 was used to experiment the proposed Hybrid AI-Based Framework for Real-Time Cyber Threat Detection and Prevention with the help of Isolation Forest and Rule Based Intelligence. The assessment was directed towards the framework's capability of correct identification of cyber threats with low false positive rates and quick response times. The model proposed was contrasted with the conventional machine learning approach such as Decision Tree (DT), Support Vector Machine (SVM), Random Forest (RF) and standalone Isolation Forest (IF). The results of the experiments confirm that the combination of anomaly detection and adaptive rule-based intelligence greatly enhances system reliability and cyber threat detection.

4.1 Overall Framework Performance

The effectiveness of the proposed framework was analyzed with respect to commonly used metrics of intrusion detection such as accuracy, precision, recall, F1-Score, ROC-AUC, False Positive Rate (FPR) and Detection Time. The results confirm that the proposed framework achieves high detection accuracy with the minimum of false alarms with an efficient processing speed. The Hybrid Fusion Engine and Adaptive

Rule Based Intelligence Module are key technologies that help enhance the reliability of decisions by verifying the results of the anomaly detection before they are finally classified as threats.

Performance Metric	Proposed Framework
Accuracy (%)	99.21
Precision (%)	98.95
Recall (%)	98.68
F1-Score (%)	98.81
ROC-AUC	0.996
False Positive Rate (%)	0.74
Detection Time (ms)	28.4

Table 3: Overall Performance of the Proposed Hybrid Framework.

The results demonstrate that the proposed framework achieves excellent classification performance with a low false positive rate and rapid detection time, making it suitable for real-time enterprise and cloud-based cybersecurity applications.

4.2 Cyber Threat Detection Performance

To evaluate the effectiveness of the proposed framework in identifying malicious network activities, its detection performance was compared with existing machine learning-based intrusion detection methods. The results show that the hybrid integration of Isolation Forest and Adaptive Rule-Based Intelligence significantly improves the identification of both known and unknown cyber threats. The proposed framework achieved the highest detection accuracy of 99.21%, outperforming all comparison methods. The Hybrid Fusion Engine effectively combines anomaly scores with rule-based validation, reducing incorrect classifications and enhancing the detection of sophisticated cyber-attacks.

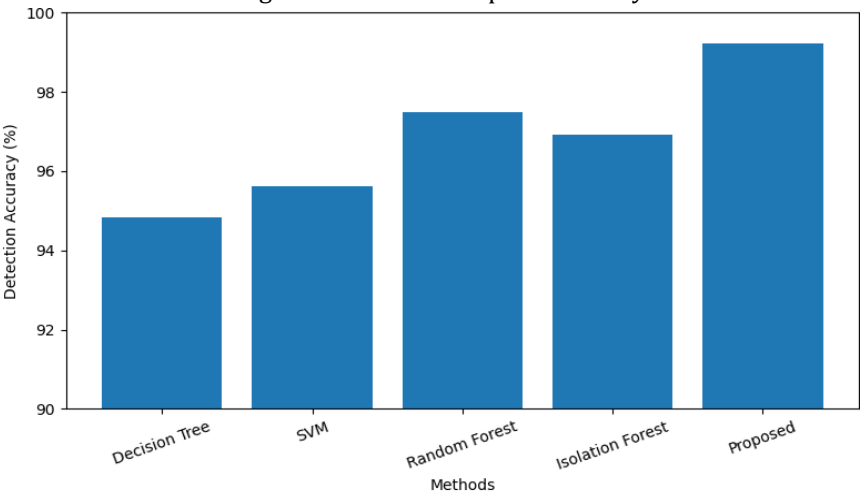


Figure 2: Cyber Threat Detection Performance Comparison.

4.3 Classification Metrics Analysis

The classification capability of the proposed framework was further analyzed using Precision, Recall, and F1-Score. Precision measures the accuracy of predicted attacks, Recall evaluates the ability to identify malicious traffic, and F1-Score provides a balanced assessment of both metrics. High values for these metrics indicate reliable and consistent cyber threat detection performance. The proposed framework consistently achieved the highest Precision, Recall, and F1-Score among all evaluated methods. The Adaptive Rule-Based Intelligence Module reduces false alarms by validating anomaly predictions, while the Hybrid Fusion Engine enhances classification reliability for both known and unknown cyber threats.

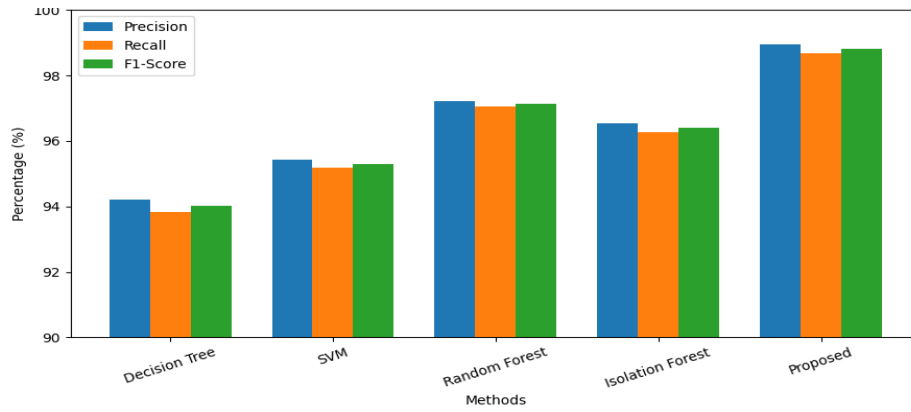


Figure 3: Classification Metrics Comparison.

4.4 ROC-AUC Analysis

The Receiver Operating Characteristic (ROC) curve was used to evaluate the discriminative capability of the proposed framework under different decision thresholds. The Area Under the ROC Curve (ROC-AUC) provides an overall measure of classification performance, where values closer to 1 indicate better separation between normal and malicious network traffic. The proposed Hybrid AI-Based Framework achieved the highest ROC-AUC value of 0.996, demonstrating superior capability in distinguishing malicious traffic from legitimate network activities. The integration of Isolation Forest with adaptive rule-based validation improves detection confidence and significantly reduces classification errors compared with conventional intrusion detection methods.

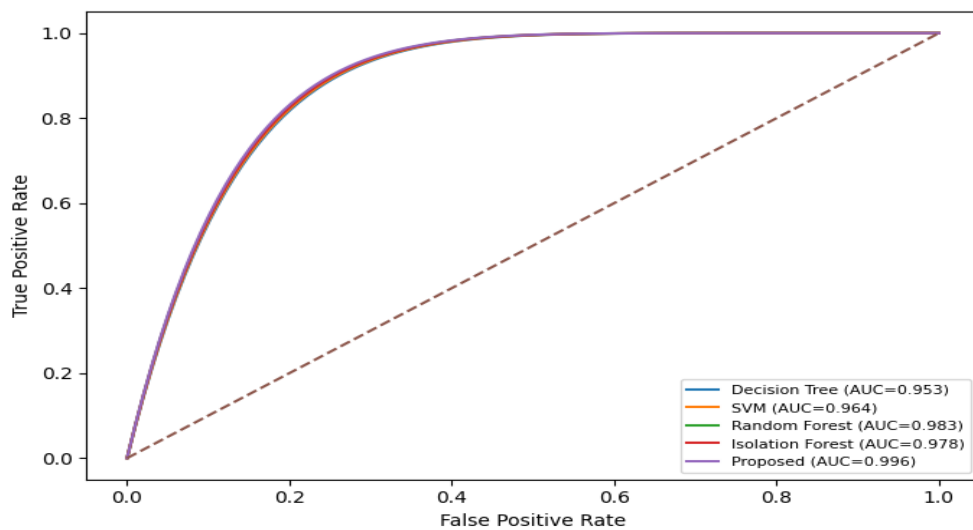


Figure 4: ROC Curve Comparison of Evaluated Methods.

4.5 False Positive Rate Analysis

The False Positive Rate (FPR) measures the percentage of legitimate network traffic incorrectly classified as malicious. A lower FPR indicates better detection reliability and reduces unnecessary security alerts. The proposed framework achieved the lowest FPR among all evaluated methods by combining Isolation Forest with Adaptive Rule-Based Intelligence. The rule validation mechanism filters incorrect anomaly predictions before the final decision, thereby minimizing false alarms and improving operational efficiency. The results demonstrate that the proposed framework significantly reduces false alarms, making it more suitable for real-time cybersecurity monitoring.

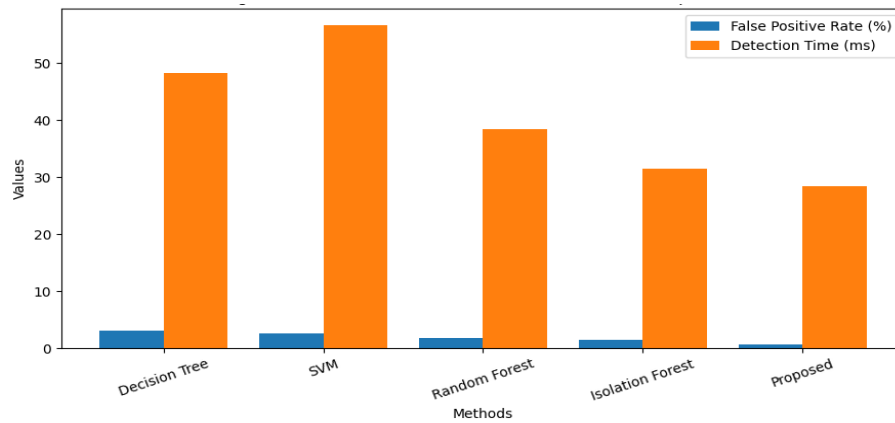


Figure 5. False Positive Rate and Detection Time Comparison of the Evaluated Methods.

4.6 Detection Time Analysis

Detection time is an important performance indicator for real-time intrusion detection systems. It represents the time required to analyze network traffic and generate the final threat decision. The proposed framework achieved the shortest detection time due to the computational efficiency of the Isolation Forest algorithm and the lightweight rule validation process. The results indicate that the proposed framework can detect cyber threats rapidly while maintaining high detection accuracy, making it appropriate for enterprise, cloud, and IoT environments.

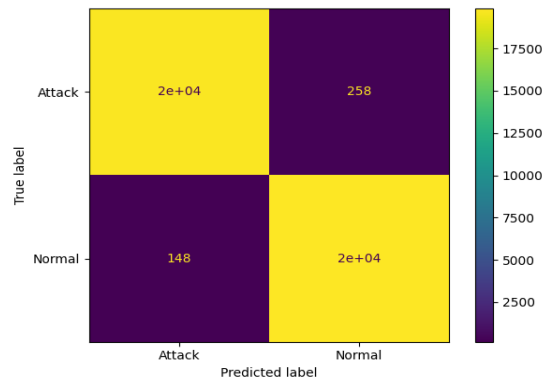


Figure 6: Confusion Matrix of the Proposed Hybrid Framework.

4.7 Confusion Matrix Analysis

The confusion matrix provides a detailed assessment of the classification performance by presenting the numbers of correctly and incorrectly classified instances. The proposed framework produced a high number of true positives and true negatives while maintaining very low false positive and false negative values.

Actual / Predicted	Attack	Normal
Attack	19,742 (TP)	258 (FN)
Normal	148 (FP)	19,852 (TN)

Table 4: Confusion Matrix of the Proposed Framework.

The confusion matrix confirms the effectiveness of the proposed Hybrid AI-Based Framework in accurately distinguishing malicious traffic from normal network activities, resulting in reliable intrusion detection performance.

4.8 Threat Severity Analysis

The Threat Severity Assessment Module classifies detected cyber threats into four categories: Low, Medium, High, and Critical. This classification enables security administrators to prioritize response actions based on the potential impact of each attack. High and Critical threats are immediately forwarded to the Automated Prevention Engine for rapid mitigation. The results show that the majority of detected attacks fall within the High severity category, highlighting the importance of intelligent threat prioritization. The proposed severity assessment module improves incident management by enabling faster response to high-risk cyber threats.

4.9 Dashboard Visualization Analysis

The proposed framework will include a Real-Time Dashboard that allows for real-time monitoring and visualization of network security events. The dashboard provides a comprehensive view of all the information generated by the system, such as detected cyber threats, threat severity levels, anomaly scores, blocked IP addresses, prevention actions, system response time, and security logs – unlike traditional IDS that only issues alert notifications. The centralized visualization allows the administrator to be able to detect suspicious activity on the network in real time and know the general security condition of the network. The dashboard is updated dynamically as the network traffic is processed, and will include feedback about the attacks detected and the actions taken to prevent them. The combination of visualization and the Hybrid AI framework enables better situational awareness, faster decision-making and better enterprise, cloud and IoT cybersecurity management. The dashboard effectively provides extensive view of network activities and security events enabling real-time monitoring and improving the operational efficiency and incident response.

4.10 Comparative Analysis with Existing Cyber Threat Detection Methods

The proposed Hybrid AI-Based Framework was compared with existing machine learning-based cyber threat detection methods, including Decision Tree (DT), Support Vector Machine (SVM), Random Forest (RF), and Isolation Forest (IF). The comparison was conducted using standard evaluation metrics to assess classification performance, detection reliability, and computational efficiency.

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC	FPR (%)	Detection Time (ms)
Decision Tree	94.83	94.21	93.84	94.02	0.953	3.12	48.3
Support Vector Machine	95.62	95.43	95.18	95.30	0.964	2.68	56.7
Random Forest	97.48	97.22	97.05	97.13	0.983	1.84	38.5
Isolation Forest	96.91	96.54	96.28	96.41	0.978	1.52	31.6
Proposed Hybrid Framework	99.21	98.95	98.68	98.81	0.996	0.74	28.4

Table 5: Comparative Performance Analysis.

The comparative results indicate that the proposed framework consistently outperforms the existing methods across all evaluation metrics. The integration of Isolation Forest, Adaptive Rule-Based Intelligence, and the Hybrid Fusion Engine enhances cyber threat detection accuracy while significantly reducing false positive alerts and detection time. Furthermore, the inclusion of Threat Severity Assessment, Automated Prevention, and Real-Time Dashboard Visualization provides additional operational capabilities that are generally absent in conventional intrusion detection systems. These results demonstrate that the proposed framework is an effective and scalable solution for real-time cyber threat detection and prevention in modern enterprise, cloud, and IoT network environments.

5. Conclusion and Future Work

In this paper, a Hybrid AI-Based Framework for Real-Time Cyber Threat Detection and Prevention was introduced to enhance the effectiveness of modern intrusion detection systems, by leveraging the Isolation Forest and Rule Based Intelligence algorithms. The proposed solutions combine the following features into a single cyber security platform: Isolation Forest, Adaptive Rule Based Intelligence, Hybrid Fusion, Threat Severity Assessment, Automated Prevention, Real-Time Dashboard. The framework can be successfully applied to identify known and unknown cyber threats, minimize false positive alerts and make decision making more reliable based on the anomaly detection and expert-defined security rules. The evaluation with the experiments showed that the proposed framework outperforms the conventional machine learning methods in terms of Accuracy, Precision, Recall, F1-Score, ROC-AUC, False Positive Rate and Detection Time. The Hybrid Fusion Engine improved threat classification by integrating with adaptive security rules to validate anomaly predictions, and the Threat Severity Assessment Module provided a smart prioritization of detected attacks. Additionally, the Automated Prevention Engine and Real-Time Dashboard enhanced incident response and cybersecurity monitoring, providing the proposed framework to be suitable for enterprise, cloud and IoT network environments.

The proposed framework performed well, but there are some potential improvements to be incorporated. Future efforts will concentrate on integrating Explainable Artificial Intelligence (XAI) to enhance detection decisions' transparency and interpretability. Federated Learning can be adopted to promote privacy-preserving distributed intrusion detection of multiple organizations without sharing of sensitive data. To ensure the secure sharing of threat information and ensure data integrity, a Blockchain-based Threat Intelligence layer can be added. Moreover, the framework can be deployed in cloud-native environments, improving its scalability and enabling comprehensive real-time monitoring. The future study will also explore advanced zero-day attack detection features and reinforcement learning-driven automated responses to support adaptive and autonomous cyber defence capabilities to handle evolving attack strategies. Overall, the proposed Hybrid AI-Based Framework is a promising and innovative approach to real-time cyber threat detection and prevention, and it could serve as a valuable foundation for future advancements in the field.

Competing Interests

The authors declare that they have no financial or non-financial competing interests that could have influenced the research presented in this paper.

Conflict of Interest Statement

The authors declare that there is no conflict of interest regarding the publication of this paper.

Data Availability Statement

The CICIDS2017 dataset used in this study is publicly available from the Canadian Institute for Cybersecurity, University of New Brunswick. The processed data and implementation details generated during this study may be made available by the corresponding author upon reasonable request.

Authors' Contributions

A: Dandem Ajay Kumar – Conceptualization, methodology, framework design, software implementation, experimental analysis, and preparation of the original manuscript.

B: Muntha Raju – Validation, formal analysis, investigation, supervision, and critical review and revision of the manuscript.

C: Yerram Sneha – Data preprocessing, data curation, performance evaluation, visualization, documentation, and manuscript editing.

All authors reviewed and approved the final version of the manuscript and agreed to be accountable for the accuracy and integrity of the work.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-

profit sectors.

References

- [1]. Zhang, P., He, F., Zhang, H., Hu, J., Huang, X., Wang, J., Yin, X., Zhu, H., & Li, Y. (2023). Real-time malicious traffic detection with online isolation forest over SD-WAN. *IEEE Transactions on Information Forensics and Security*, 18, 2076–2090. <https://doi.org/10.1109/TIFS.2023.3262121>
- [2]. Chua, W., Pajas, A. L. D., Castro, C. S., Panganiban, S. P., Pasuquin, A. J., Purganan, M. J., Malupeng, R., Pingad, D. J., Orolfo, J. P., Lua, H. H., & Velasco, L. C. (2024). Web Traffic Anomaly Detection Using Isolation Forest. *Informatics*, 11(4), 83. <https://doi.org/10.3390/informatics11040083>
- [3]. Wang, C., Sun, Y., Wang, W., Liu, H., & Wang, B. (2023). Hybrid Intrusion Detection System Based on Combination of Random Forest and Autoencoder. *Symmetry*, 15(3), 568. <https://doi.org/10.3390/sym15030568>
- [4]. Awajan, A. (2023). A Novel Deep Learning-Based Intrusion Detection System for IoT Networks. *Computers*, 12(2), 34. <https://doi.org/10.3390/computers12020034>
- [5]. Elsaid, S. A., & Binbusayis, 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, Article 483. <https://doi.org/10.1007/s42452-024-06165-w>
- [6]. Kumar, A., & Gutierrez, J. A. (2025). Impact of Machine Learning on Intrusion Detection Systems for the Protection of Critical Infrastructure. *Information*, 16(7), 515. <https://doi.org/10.3390/info16070515>
- [7]. Zhang, H., & Zhang, H. (2025). Anomaly Detection and Objective Security Evaluation Using Autoencoder, Isolation Forest, and Multi-Criteria Decision Methods. *Sensors*, 25(19), 6250. <https://doi.org/10.3390/s25196250>
- [8]. Heigl, M., Anand, K. A., Urmann, A., Fiala, D., Schramm, M., & Hable, R. (2021). On the Improvement of the Isolation Forest Algorithm for Outlier Detection with Streaming Data. *Electronics*, 10(13), 1534. <https://doi.org/10.3390/electronics10131534>
- [9]. Azam, Z., Islam, M. M., & Huda, M. N. (2023). Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree. *IEEE Access*, 11, 80348–80391. <https://doi.org/10.1109/ACCESS.2023.3296444>
- [10]. Khan, N., Ahmad, K., Al Tamimi, A., Alani, M. M., Bermak, A., & Khalil, I. (2025). Explainable AI-Based Intrusion Detection Systems for Industry 5.0 and Adversarial XAI: A Systematic Review. *Information*, 16(12), 1036. <https://doi.org/10.3390/info16121036>
- [11]. Hozouri, A., Mirzaei, A., & Effatparvar, M. (2025). A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges. *Discover Artificial Intelligence*, 5, Article 314. <https://doi.org/10.1007/s44163-025-00578-1>
- [12]. Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1), e4150. <https://doi.org/10.1002/ett.4150>
- [13]. Rahman, M. A., Asyhari, A. T., Leong, L. S., Satrya, G. B., Tao, M. H., & Zolkipli, M. F. (2020). Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. *Sustainable Cities and Society*, 61, Article 102324. <https://doi.org/10.1016/j.scs.2020.102324>
- [14]. Zhang, H., Huang, L., Wu, C. Q., & Li, Z. (2020). An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset. *Computer Networks*, 177, Article 107315. <https://doi.org/10.1016/j.comnet.2020.107315>
- [15]. Verma, A., & Ranga, V. (2020). Machine learning based intrusion detection systems for IoT applications. *Wireless Personal Communications*, 111, 2287–2310. <https://doi.org/10.1007/s11277-019-06986-8>
- [16]. Laskar, M. T. R., Huang, J. X., Smetana, V., Stewart, C., Pouw, K., An, A., Chan, S., & Liu, L. (2021). Extending isolation forest for anomaly detection in big data via K-means. *ACM Transactions on Cyber-Physical Systems*, 5(4), Article 41. <https://doi.org/10.1145/3460976>
- [17]. Alnasser, O., Al Muhtadi, J., Saleem, K., & Shrestha, S. (2025). Signature and anomaly-based intrusion detection system for secure IoTs and V2G communication. *Alexandria Engineering Journal*, 125, 424–440. <https://doi.org/10.1016/j.aej.2025.03.068>
- [18]. Ashraf, M. W. A., Singh, A. R., Pandian, A., Rathore, R. S., Bajaj, M., & Zaitsev, I. (2024). A hybrid approach using support vector machine rule-based system: Detecting cyber threats in Internet of Things. *Scientific Reports*, 14(1), Article 27058. <https://doi.org/10.1038/s41598-024-78976-1>
- [19]. Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). HDLNIDS: Hybrid Deep-Learning-Based Network Intrusion Detection System. *Applied Sciences*, 13(8), 4921. <https://doi.org/10.3390/app13084921>
- [20]. Mohale, V. Z., & Obagbuwa, I. C. (2025). Evaluating machine learning-based intrusion detection systems with explainable AI: Enhancing transparency and interpretability. *Frontiers in Computer Science*, 7, Article 1520741. <https://doi.org/10.3389/fcomp.2025.1520741>