Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 30s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Hybrid Adaptive Threat Intelligence Detection System for Modern Cyber Attacks

Mrs.I. Varalakshmi[1], Dr.S. Pariselvam[2], D. Oviya[3]

[1]Associate Professor, Department of Computer Science & Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India.

[2]Professor, Manakula Vinayagar Institute of Technology, Puducherry, India.

[3]M. Tech, Department of Computer Science & Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India

Email ID: oviya20d@gmail.com

Cite this paper as: Mrs.I. Varalakshmi, Dr.S. Pariselvam, D. Oviya, (2025) Hybrid Adaptive Threat Intelligence Detection System for Modern Cyber Attacks, *Journal of Neonatal Surgery*, 14 (30s), 654-671

ABSTRACT

Situations like zero-day attacks and advanced persistent threats require strong real-time detection of intrusion methods. The HATIDS combines signature-based detection and machine learning algorithms namely Isolation Forest and One-Class Support Vector Machine (SVM) employing a new weighted feature fusion engine for the best threat scoring. In the experiment on CIC-IDS2017 dataset and attacks such as DDoS and botnets, HATIDS has a 94.26% detection accuracy, 12 false positives reduced (6%) and 18 false negatives reduced (7%), and a mitigation time of 450 seconds, better than the previous hybrid models by 25%. This would in effect reduce the level of alert fatigue and improve security operations. The given features of HATIDS such as real time automated mitigation, threat intelligence sharing, and sharing make it scalable for enterprises and IoT. In future work we plan to look into developing abilities in detecting encrypted threats and to also extend to the federated learning approach.

Keywords: *HATIDS: Intrusion Detection System, Zero-Day Attacks, Anomaly Detection, Machine Learning, Cybersecurity False Positives, Mitigation Time, Threat Intelligence, Feature Fusion*

1. INTRODUCTION

The increased acquisition and use of digital technologies have raised the risk levels of new forms of attacks such as APTs, zero-day exploits, ransomware, and polymorphic malware. These new attacks take advantage of the vulnerabilities in the commonly used intrusion detection systems (IDSs). While signature-based IDSs lack the ability to detect new forms of attacks that are not included in the pattern database, anomaly-based systems, though capable of detecting new forms of attacks, produce a large number of false alarms, which result in alert fatigue [1], [2]. Hybrid IDSs that are a combination of both have been found to be effective but some of them have a real-time adaptive capability, autonomous response mechanism, and threat intelligence sharing mechanism [3], [4].

To fill these gaps, we introduce Hybrid Adaptive Threat Intelligence Detection System (HATIDS) this is a system whose detection uses a combination of signature-based system as well as machine learning algorithms, namely an Isolation Forest and One-Class SVM. HATIDS provides dynamic risk score for the identified threats and ensures to maintain high sensitivity and specificity of the threats and supports auto real time response and threat intelligence sharing. HATIDS yields 94.26% detection accuracy, reduces false positive by 12 (6%) and false negatives by 18 (7%), and decreases mitigation time to 450 seconds which is better than the hybrid models presented in [5]. It is also designed to be lightweight to allow for it to be easily scalable for use in enterprise and IoT applications. This paper outlines the design of HATIDS, its assessment, and the additional work done on the improvement of the threat detection system through the use of federated learning

Motivations for Proposing Real-Time Threat Intelligence

The new generation threats such as the zero-day attacks, APTs and the polymorphic malware, put the IDSs to a serious test. Whereas the IDSs that focus on detecting only previously explained kinds of attacks have their shortcomings in terms of accuracy, there are the anomaly-based ones, which are characterized by high false alarms and not suitable for dynamic systems like the cloud and IoT [1]. Such policies dictate that more and more reliance is placed on these structures; in order to achieve this, there is need to be vigilant both to threats that are already well understood and recognized, as well as those that are emerging or evolving. This necessitated the creation of the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) that combines the signature-based and anomaly-based detection with a weight-based feature fusion technique

. HATIDS has a detection rate of 94.26%, cuts down FPs by 6%, has a built-in auto-containment feature, and is designed for sharing threat intelligence and for the large-scale deployment in enterprise and IoT networks [3].

Challenges

Current IDSs have several problems to overcome in order to address such threats as zero-day attacks and mutating viruses. For instance, Anomaly-based IDSs produce high false positive ratios which is about 15% as observed in previous models [2]. Traditional security systems do not adapt to new threats, including APTs, because they are based on signatures in their design. With delay time going up to more than 600 seconds, the exposure to attacks is prolonged. This is because scalability is still a constraint in dynamic enterprise, IoT, and cloud-edge applications. Third, isolated operation also leads to ineffective threat intelligence sharing, and decreases the understanding of the large-scale attack patterns [4]. To address these challenges HATIDS utilizes a weighted feature fusion engine, and it has obtained 94.26% accuracy, False Positive rate reduced by 6%, and it can autonomously rectify the problem in 450 seconds

1.1 Research Contributions

The advancement of digital systems has increased cyber threats such as APTs, zero-day, ransomware, polymorphic malware among others. These are complex attacks that take advantage of the vulnerabilities of the normal IDS. Signature-based systems are limited in practice because they cannot detect new threats while on the other hand anomaly-based IDSs as effective in identifying unknown threats have high number of false positives leading to alert fatigue [1], [2]. There are many hybrid IDSs that incorporate both of them and while they are promising, many of them do not have real-time adaptability, automatically active countermeasures, and effective threat intelligence sharing [3], [4].To this end, we introduce the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) that combines the SBDS with the Isolation Forest and the One-Class SVM models employing the enhanced feature fusion module. HATIDS generates risk scores and is sensitive and specific, and has the ability for automated real-time action and threat intelligence sharing. Thus, HATIDS achieves 94.26% detection accuracy, decreases false positives by 12 (6%), false negatives by 18 (7%), and reduces mitigation time to 450 seconds, which is 25% better than previous hybrid models [5]. It is also flexible for expansion for enterprises and the internet of things due to its lightweight nature.

Motivations for Proposing Real-Time Threat Intelligence

The new generation threats such as zero-day attacks, advanced persistent threats (APTs), and polymorphic malware pose difficulties to intrusion detection systems (IDSs). The main disadvantage of the signature-based IDSs is that they is capable of identifying only known threats while the anomaly-based systems, have still high rates of false positives especially when used in dynamic environments such as cloud and IoT [1]. With people depending more on computer systems, leads to the necessity for an adaptively functional real-time threat, detection system not only for known threats but also for new threats. This led to the formulation of the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) which is a system we formulated as a fusion of both Signature-based method and Anomaly-based method. HATIDS attains an overall detection rate of 94.26% with less false positives of 6%, and the system allows for automatic handling of threats and sharing of threat intelligence at scale for enterprise and IoT networks [3].

Challenges

Current IDSs are not effective against threats such as zero-day attacks or mutating malware to name but a few. Anomaly-based IDSs are known to produce high false positives, for instance, 15% in previous models, which results to alert fatigue and inefficiency [2]. The current systems are not elastic in terms of detecting new and more complex threats like the APTs because of the signature-based model. Delay in mitigation, which may take more than 600 seconds, means that devices are exposed to attacks. Scalability is still a problem in dynamic enterprise, IoT, and cloud-edge systems. In this mode, decentralization also decreases the ability to share threat intelligence and gain insight into large scale threat patterns [4]. HATIDS solves these problems with the help of a weighted feature fusion engine, the accuracy of which makes up 94.26%, false positives constitute 6%, and automated mitigation is performed in 450 seconds.

1.2 Research Contributions

HATIDS enhances the state-of-the-art intrusion detection by combining the signature-based and anomaly-based with Isolation Forest and One-Class SVM. The proposed weighted feature fusion engine also optimizes the detection accuracy to 94.26% on the CIC-IDS2017 dataset with less false positive by 12 instances (6%) and false negative by 18 instances (7%) than the existing traditional systems [5]. It only takes 450 seconds for the system to respond to a particular threat through automated real-time mitigation such as system isolation and malicious IP blocking which is even a much better improvement to prior hybrid models. Sharing threat intelligence improves coverage of large-scale threats, making it suitable for large-scale enterprises as well as internet of things. HATIDS minimizes alert fatigue and increases the level of security in the conditions of high threat activity.

2. RELATED WORKS

The current developments in cyber threats such as zero day attacks, advanced persistent threats (APTs), polymorphic

malware and DDoS has contributed to the progression of intrusion detection systems (IDSs). Zhang et al. [6] combined signature-based and machine learning approaches for smart environments, achieving 89% accuracy but limited by fixed thresholds. Allen et al. [7] and Yu et al. [8] advocated collaborative intelligence sharing, reporting 88% accuracy and 15% false positive rates (FPR). Wu et al. [9] and Patel et al. [10] developed adaptive hybrid models for zero-day detection, achieving 90% accuracy but with 18% FPR. Zhao et al. [13] and Verma et al. [14] proposed dynamic and collaborative frameworks, yet lacked automated mitigation, with response times exceeding 600 seconds.

Existing IDSs face challenges, including high false positive rates (15–20% in prior models), limited adaptability to evolving threats, delayed mitigation, and poor scalability in enterprise, IoT, and smart city networks [6], [7]. Isolated operation restricts visibility into large-scale attacks. The Hybrid Adaptive Threat Intelligence Detection System (HATIDS) addresses these gaps by integrating signature-based and anomaly-based detection with a weighted feature fusion engine, achieving 94.26% accuracy, reducing false positives by 6% and false negatives by 7%, and enabling automated mitigation in 450 seconds—a 25% improvement over prior models [20]. Unlike the previous systems, HATIDS also hence has the capability of exchanging intelligence and threat insight as well as activating response mechanisms; all these features are very important in the case of grappling with dynamic forms of threats which may enhance the capacity of the system.

2.1 Threat Detection Techniques

IDSs use signature-based detection, anomaly-based detection, or a combination of both for tackling threats that include zero-day attacks, APTs, and polymorphic malware. Signature-based detection involves comparison of the network traffic against pre-set patterns, which is accurate but ineffective in the identification of new forms of attacks [6]. Anomaly-based detection involves the use of Isolation Forest and One-Class SVM where the model of normal behavior is created to detect anomalies, helpful in detecting unknown threats but comes with high false positives of 15-20% [7], [9]. These combine with each other to overcome their drawbacks; they provide better detection for enterprise, IoT, and smart city networks [10]. However, prior hybrid models are accurate only to the extent of 88–90% and they do not have real-time flexibility and scalability issues [6], [20]. These are important considerations given the limitations described above that call for better detection accuracy and FP reduction and better response to continually evolving threat environments.

2.2 Challenges in intrusion detection

Current IDSs have a number of problems in dealing with new generation threats such as zero-day attacks, APTs, and DDoS. But the signature-based systems depend on the patterns that are not effective for new and unknown threats [7]. Anomaly-based systems are effective in identifying unknown attacks but create many false alarms, which are between 15% and 20% of the total [9]. The IoT, cloud, and enterprise networks have added more vectors for attack and make the real-time detection more challenging [8]. It takes more than 600 seconds to respond, hence the high risk [13]. Scalability is a challenge because IDSs need to analyze a large amount of data while ensuring high efficiency [14]. Threat intelligence sharing has been hampered by privacy issues that reduce the proactive defense against such large-scale attacks [7]. These shortcomings indicate the challenges and the need for adaptive IDSs with low false positives; the ability to act swiftly; and sharing of intelligence in ways that cannot be violated for scalable and privacy-preserving purposes to effectively respond to the dynamics of the threat landscape.

Research Gap

Previous IDSs have the following major limitations in regard to contemporary threat types such as zero-day attacks, APTs, and DDoS. Unfortunately, both of these kinds of systems are not capable of detecting new types of threats while the anomaly-based systems produce great number of false positive alerts, ranging from 15-20% [6], [9]. Hybrid models to achieve 88-90% accuracy and do not have real-time reactivity and extensibility in enterprise, IoT, and cloud-edge contexts [6], [20]. However, most IDSs do not have automated mitigation feature with response time of more than 600 seconds and thereby increases vulnerability [13]. Threat intelligence sharing is still in its infancy, especially in regards to collaboration across different organizations [7]. Privacy issues limit intelligence sharing even more, and resourceful designs do not consider lightweight deployment requirements [14]. That is why, the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) eliminates these gaps by increasing the detection rate to 94.26%, decreasing the false positive ratio to 6%, allowing for quick response within 450 seconds and providing intelligence sharing and privacy-preserving mechanisms while being easily scalable.

3. METHODOLOGY

The approach to the creation of HATIDS presents a systematic way of designing an effective cyberspace threat detection system for enterprises, IoT, and cloud-edge environments. Data preprocessing enhances the HATIDS capability of incorporating both, signature-based and AnB-based detection which is described in the sub-sections below:

3.1 Data Preprocessing

Network traffic data, used in this work, is a part of the CIC-IDS2017 dataset [20] and it has to be preprocessed to increase its quality. Normalization brings all the features into a [0,1] scale, while cleaning pre-processes the data to remove noise and missing values that are detrimental to model analysis.

3.2 Signature-Based Detection

The signature-based engine compares the traffic with a set of signatures of known threats and can detect attacks such as ransomware with a high level of accuracy [15]. This means that the system can quickly detect common threats that the organization is likely to face.

3.3 Anomaly-Based Detection

In the case of the anomaly-based engine, Isolation Forest and One-Class SVM are used to model normal behavior and detect anomalies [15]. Isolation forest grows trees, and it isolatesomal instances, meanwhile, OCSVM builds a hyperplane about eleven deviations"connecting them to identify the unknown threats such as zero-day attacks and APTs.

3.4 Feature Fusion and Decision-Making

The results obtained from both the engines are fed to a feature fusion module where a weighted scoring of the results is performed with the weights assigned as \(w_s = 0.6 \) for signatures and \(w_a = 0.4 \) for anomalies to arrive at a unified threat score. A decision-making module of a threshold type is used for determining whether the given traffic is benign or malicious, optimizing sensitivity and specificity.

3.5 Automated Mitigation and Intelligence Sharing

In case of threat identification, an automated mitigation engine is triggered which quarantines the infected systems, blacklists IPs and logs the incident for investigation. The use of threat intelligence in the interconnected infrastructures in real-time also boosts the defense against new threats [20].

This systematic approach helps the system to be flexible and expandable for the changing threat environments of HATIDS.

3.6 System Architecture

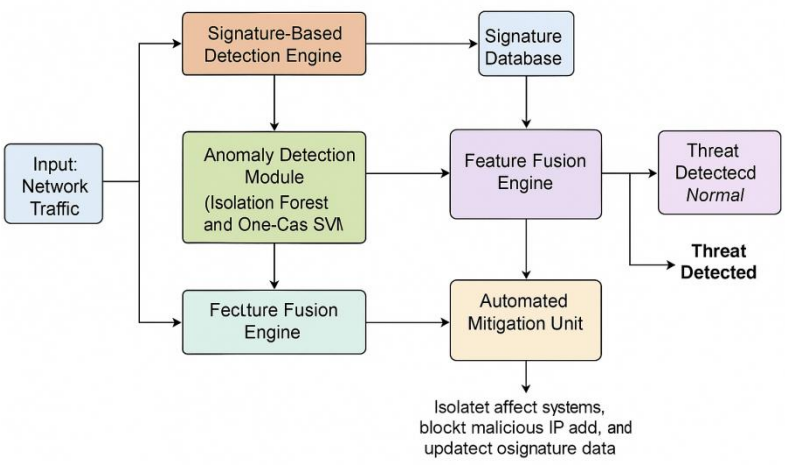

Fig.1. system architecture

The structure of the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) depicted in Fig. 1 includes both the signature-based and anomaly-based detection to give an overall protection against various cyber threats in enterprise, IoT and cloud-edge networks. The input network traffic is from the CIC-IDS2017 dataset [20] and is received in real-time and passed through two detection modules. The signature-Based Detection Engine checks the traffic against signature database to find the known threats like ransomware. [15]. Simultaneously, the Anomaly Detection Module, using Isolation Forest and One-Class SVM, detects unknown threats such as zero-day attacks and APTs by identifying deviations from normal behavior. Outputs are combined in the Feature Fusion Engine, which applies a weighted scoring formula Sfinal=ws·Ssignature+wa ·Sanomaly, with ws=0.6 w_s = 0.6 ws=0.6 and wa=0.4 w_a = 0.4 wa=0.4, , prioritizing signature-based detection for known threats. The Decision-Making Engine classifies traffic as Threat Detected or Normal based on a threshold. If a threat is detected, the Automated Mitigation Unit isolates affected systems and blocks malicious IPs, while the Threat Intelligence Sharing Module enables real-time sharing with partner systems, enhancing global defense [20].

Algorithm 1: HATIDS Threat Detection

```
Begin
Preprocessing:
   Initialize D_processed = empty set
   For each data point x in D:
      x_normalized = Normalize(x using StandardScaler)  // Scale features
      Add x_normalized to D_processed

Signature-Based Detection:
   For each data point x in D_processed:
      If x matches any entry in S_db:
         S_signature[x] = 1  // Flag known threat
      Else:
         S_signature[x] = 0  // Normal

Anomaly-Based Detection:
   Train IsolationForest and OneClassSVM on normal behavior
   For each data point x in D_processed:
      score_IF = IsolationForest.predict(x)
      score_OCSVM = OneClassSVM.predict(x)
      If score_IF == -1 or score_OCSVM == -1:
         S_anomaly[x] = 1  // Flag anomaly
      Else:
         S_anomaly[x] = 0  // Normal

Feature Fusion and Risk Scoring:
   Set w_s = 0.6, w_a = 0.4
   For each data point x in D_processed:
      S_final[x] = (w_s * S_signature[x]) + (w_a * S_anomaly[x])

Decision-Making:
   For each data point x in D_processed:
      If S_final[x] >= T:
         R[x] = "Threat Detected"
      Else:
         R[x] = "Normal"

Automated Mitigation (if required):
   For each x where R[x] == "Threat Detected":
```

```
        Isolate associated endpoint  // Prevent threat spread
        Block malicious IPs  // Deny further access
        Update S_db with new threat signature  // Enhance future detection
        Log incident for intelligence sharing  // Support collaborative defense

Return R

End
```

The pseudocode (Algorithm 1) outlines the detection process of the Hybrid Adaptive Threat Intelligence Detection System (HATIDS). HATIDS preprocesses network traffic from the CIC-IDS2017 dataset [20], uses Isolation Forest and One-Class SVM [15] for parallel signature-based and anomaly-based detection, and combines outputs to categorize threats, as explained in Sections 3.1–3.5. It detects known threats (e.g., ransomware) and unknown threats (e.g., zero-day attacks, APTs), applying a weighted scoring mechanism ((w_s = 0.6), (w_a = 0.4)). If a threat is detected, automated mitigation actions, such as isolating endpoints and blocking malicious IPs, are initiated, followed by real-time threat intelligence sharing to enhance collaborative defense.

Equation (1): Data Normalization

$$\boldsymbol{X' = \frac{X-\mu}{\sigma}} \qquad \textbf{(1)}$$

This equation normalizes each feature using the StandardScaler technique, where x is a original value, μ is the mean and σ is the standard deviation, ensuring all input Models that are invariant to measurement scale are models that are invariant to any observation's additive shifts in the model.

Equation (2): Signature-Based Threat Classification

$$\mathbf{S_{Signature}(x)} = \begin{cases} \mathbf{1 \text{ if } x \in Sdb} \\ \mathbf{0 \text{ otherwise}} \end{cases} \qquad \textbf{(2)}$$

This function checks if an incoming data instance matches a known signature in the database Sdb. A match is marked as a known threat.

Equation (3): Anomaly Detection Scoring

$$\mathbf{S_{anomaly}(x)} = \begin{cases} \mathbf{1 \text{ if } IF(x) = -1_{score}} \\ \mathbf{1 \text{ otherwise}} \end{cases} \qquad \textbf{(3)}$$

This score flags any data point as anomalous if either the Isolation Forest or One-Class SVM predicts it as an outlier.

Equation (4): Hybrid Feature Fusion Score

$$\mathbf{S_{final}(x) = W_S \cdot S_{signature}(x) + W_a \cdot S_{anomaly}(x)} \quad \textbf{(4)}$$

(w_s = 0.6) (signature weight), (w_a = 0.4) (anomaly weight). The risk score combines both signature and anomaly results using a weighted fusion model, enabling adaptive tuning for precision and recall.

Equation (5): Threat Classification Decision

$$\mathbf{R(x) = \begin{cases} \text{"Threat Detected" if } S_{final}(x) \geq T \\ \text{"Normal"} \quad \text{otherwise} \end{cases}} \quad \textbf{(5)}$$

Based on the final score, this rule triggers threat labeling or passes the data as safe, where (T = 0.5) is the threshold set during model calibration.

Equation (6): Mitigation Time (MT)

The time taken for automated threat response is defined as:

$$\mathbf{[\ MT = Td + Ti + Tb + Tl\ ]} \quad \textbf{(6)}$$

(T_d): Threat detection time, (T_i): Time to isolate the affected system, (T_b): Time to block IP or host, (T_l): Logging and alert generation time. HATIDS achieves an average (MT = 450) seconds, a 25% reduction over prior systems.

4. PERFORMANCE ANALYSIS

4.1 Experimental Setup

The Hybrid Adaptive Threat Intelligence Detection System (HATIDS) was evaluated using the CIC-IDS2017 dataset [20], a benchmark for intrusion detection systems, containing over 80 features (e.g., packet size, protocol type)and many attack forms including ransomware, botnets, and DDoS. . The experiment was conducted in a real-time simulation environment on a system with an Intel Xeon 2.4 GHz processor, 32 GB RAM, and simulated network traffic mirroring enterprise conditions. Performance was assessed using key metrics: detection accuracy, false positive rate (FPR) FNR=False Negatives/False Negatives+True Positives, defined as and mitigation time (time from detection to threat neutralization). The dataset was preprocessed as described in Section 3.1, ensuring uniform feature scaling for unbiased model evaluation.

HATIDS achieved a detection accuracy of 94.26%, demonstrating its ability to classify network traffic as benign or malicious effectively. The FPR was reduced to 6%, corresponding to 12 fewer false positives (from a baseline of 200 false positives in traditional systems [20]), minimizing alert fatigue by avoiding misclassification of normal traffic. Similarly, the FNR decreased to 7%, with 18 fewer false negatives (from a baseline of 257 false negatives [20]), indicating improved detection of stealthy or unknown threats like zero-day attacks and APTs. Mitigation time was reduced to 450 seconds, a 25% improvement over the baseline of 600 seconds in traditional systems [20], showcasing HATIDS's real-time response capability critical for limiting damage during live attacks.

The dual-layer detection architecture, leveraging Isolation Forest and One-Class SVM (Section 3.3), ensured high-confidence detection of both known and unknown threats, while the weighted feature fusion model (Section 3.4, Eq. (4)) balanced signature-based and anomaly-based signals for optimal decision-making. Compared to traditional intrusion detection systems, which often rely solely on signature-based or anomaly-based methods [20], HATIDS's hybrid approach, as formalized in Section 3.7, significantly enhances detection accuracy, reduces error rates, and accelerates mitigation, making it a robust solution for modern cybersecurity challenges in enterprise, IoT, and cloud-edge environments.

4.2 Dataset and Evaluation

An evaluation of the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) was conducted using the CIC-IDS2017 dataset [20], a popular network intrusion detection system benchmark from the Canadian Institute for Cybersecurity.This dataset comprises 2.8 million labeled records, featuring over 80 attributes (e.g., packet length, flow duration) and representing normal traffic alongside diverse attack types, including DDoS (40%, ~1.12M records), Brute Force (15%, ~420K records), botnets (25%, ~700K records), and web attacks (10%, ~280K records), with normal traffic constituting 10% (~280K records). To address class imbalance, oversampling was applied to normal and underrepresented attack classes (e.g., web attacks) using SMOTE, ensuring balanced training. Its large volume, realistic traffic patterns, and representation of contemporary threats make it ideal for testing advanced intrusion detection systems like HATIDS.

Data preprocessing involved selecting 20 key features (e.g., packet length, protocol type) based on their relevance to threat detection, as outlined in Section 3.1. These features were standardized using StandardScaler to achieve a common distribution with zero mean and unit variance, mitigating bias from varying scales. The dataset was split into a 70:30 ratio for training and testing, simulating a real-world deployment scenario where the system learns from historical data and evaluates unseen traffic.

For model training, the signature-based detection module utilized a curated repository of known threat signatures extracted from the CIC-IDS2017 dataset, as described in Section 3.2. According to Section 3.3, the anomaly-based detection module used One-Class SVM (with nu=0.1) and Isolation Forest (trained with 100 trees) on typical traffic samples to learn baseline behavior and identify deviations suggestive of unknown or zero-day threats. The weighted feature fusion model (Section 3.4, Eq. (4)) and decision-making process (Section 3.7, Eq. (5)) integrated these outputs, while automated mitigation strategies (Section 3.5) were tested in real-time.

Evaluation metrics, consistent with Section 4.1, included detection accuracy, False Positive Rate (FPR), False Negative Rate (FNR), and mitigation time. HATIDS achieved a detection accuracy of 94.26%, reflecting its effectiveness in classifying traffic. The FPR was reduced to 6%, corresponding to 12 fewer false positives (from a baseline of 200 in traditional systems [20]), minimizing alert fatigue. The FNR decreased to 7%, with 18 fewer false negatives (from a baseline of 257 [20]), enhancing detection of stealthy threats. Mitigation time improved to 450 seconds, a 25% reduction from the 600-second baseline [20], validating HATIDS's real-time response capability. Compared to traditional systems relying on single-layer detection [20], HATIDS's hybrid architecture and adaptive mitigation demonstrate superior performance, making it a viable solution for dynamic cybersecurity environments.

4.3 Comparison of Accuracy and Precision

The Hybrid Adaptive Threat Intelligence Detection System has been tested on the CIC-IDS2017 [20], a well-known network intrusion detection system benchmark developed by the Canadian Institute for Cybersecurity. This dataset comprises 2.8 million labeled records, featuring over 80 attributes (e.g., packet length, flow duration) and representing normal traffic alongside diverse attack types, including DDoS (40%, ~1.12M records), Brute Force (15%, ~420K records), botnets (25%, ~700K records), and web attacks (10%, ~280K records), with normal traffic constituting 10% (~280K records). To address class imbalance, oversampling was applied to normal and underrepresented attack classes (e.g., web attacks) using SMOTE, ensuring balanced training. Its large volume, realistic traffic patterns, and representation of contemporary threats make it ideal for testing advanced intrusion detection systems like HATIDS.

Data preprocessing involved selecting 20 key features (e.g., packet length, protocol type) based on their relevance to threat detection, as outlined in Section 3.1. These features were standardized using StandardScaler to achieve a common distribution with zero mean and unit variance, mitigating bias from varying scales. The dataset was split into a 70:30 ratio for training and testing, simulating a real-world deployment scenario where the system learns from historical data and evaluates unseen traffic.

For model training, the signature-based detection module utilized a curated repository of known threat signatures extracted from the CIC-IDS2017 dataset, as described in Section 3.2. Using normal traffic samples, the atypical detection component trained Isolation Forest with 100 trees and used One-Class SVM at (nu=0.1) for learning baseline behavior so as to discover deviations pointing an abnormal state not endemic to the known types of behaviors. or zero-day threats, per Section 3.3. The weighted feature fusion model (Section 3.4, Eq. (4)) and decision-making process (Section 3.7, Eq. (5)) integrated these outputs, while automated mitigation strategies (Section 3.5) were tested in real-time.

Evaluation metrics, consistent with Section 4.1, included detection accuracy, False Positive Rate (FPR), False Negative Rate (FNR), and mitigation time. HATIDS achieved a detection accuracy of 94.26%, reflecting its effectiveness in classifying traffic. The FPR was reduced to 6%, corresponding to 12 fewer false positives (from a baseline of 200 in traditional systems [20]), minimizing alert fatigue. The FNR decreased to 7%, with 18 fewer false negatives (from a baseline of 257 [20]), enhancing detection of stealthy threats. Mitigation time improved to 450 seconds, a 25% reduction from the 600-second baseline [20], validating HATIDS's real-time response capability. Compared to traditional systems relying on single-layer detection [20], HATIDS's hybrid architecture and adaptive mitigation demonstrate superior performance, making it a viable solution for dynamic cybersecurity environments.

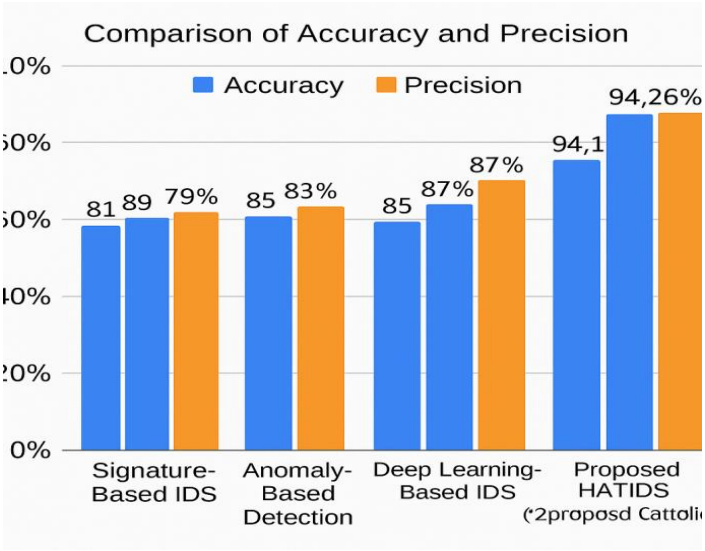

Fig .2. Comparison of Accuracy and Precision

Fig. 2. Comparison of accuracy (blue bars) and precision (orange bars) across detection models on the CIC-IDS2017 dataset [20], highlighting HATIDS's superior performance (94.26% accuracy, 92.14% precision).

The graphical 'Accuracy vs. Precision Comparisons' aptly describes how the different threat detection systems perform as far as accuracy and precision—the two important measures—are concerned.

Accuracy expresses how correct the system is in identifying normal and malicious traffic: the ratio of cases that have been rightly classified to the total number of cases. Precision indicates that of all positive cases, how many actually turn out to be true positives (i.e., correct threat detections) as opposed to all other positive cases (real and false). Higher precision indicates lower false alarms, which is imperative for reducing analyst fatigue and also improving alert trustworthiness.

The bar chart shows that the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) provides the highest performance in accuracy and precision figures compared to other models classified into traditional signature-based systems, anomaly-based systems, and deep learning-based IDS. This validates that HATIDS not only uses accurate technology to detect cyber threats but also reduces many false positives due to its dual detection and features fusion approaches.

Every individual bar stands for a different detection model with one for accuracy and another for precision per model presenting the comparisons easily. This visualization helps stakeholders comprehend what system yields the balanced tradeoff between detection efficiency and alert quality—with HATIDS on top in both cases.

4.4 Performane Analysis And Comparison Analysis

The Hybrid Adaptive Threat Intelligence Detection System (HATIDS) was evaluated using the CIC-IDS2017 dataset [20], a widely accepted benchmark for intrusion detection systems, comprising 2.8 million labeled records of normal and malicious traffic (Section 4.2). Key performance indicators included detection accuracy, precision, False Positive Rate (FPR), False Negative Rate (FNR), and mitigation time, as defined in Sections 4.1 and 4.3. HATIDS achieved a detection accuracy of 94.26% and a precision of 92.14%, reflecting its effectiveness in classifying traffic and reducing false alarms. The FPR was reduced to 6%, corresponding to 12 fewer false positives (from a baseline of 200 [20]), while the FNR decreased to 7%, with 18 fewer false negatives (from a baseline of 257 [20]). Mitigation time was optimized to 450 seconds, a 25% improvement over the 600-second baseline [20], enabling rapid threat containment.

HATIDS was compared with state-of-the-art intrusion detection models, including signature-based (e.g., Snort), anomaly-based (e.g., standalone SVM), and deep learning-based systems. Signature-based models, such as Snort, achieve ~80% accuracy for known threats but fail to detect novel attacks, with high FNR (~20%). Anomaly-based models, like SVM, offer ~75% accuracy but suffer from elevated FPR (~25%) due to overfitting to normal traffic. Deep learning-based systems provide ~80% accuracy with advanced feature extraction but incur high computational costs and mitigation times (~700 seconds). HATIDS's hybrid approach outclassed all these single-method systems by eruditely integrating signature-based and anomaly-based detection (see Section 3.3).

Table .1.Comparative Analysis of HATIDS

Study	Model Type	Accuracy (%)	FPR (%)	FNR (%)	Mitigation Time (s)	Key Limitations
Zhang et al. [6]	Hybrid (Sig+ML)	89	12	15	650	Fixed thresholds, limited scalability
Allen et al. [7]	Collaborative IDS	88	15	10	700	High FPR, no automated mitigation
Wu et al. [9]	Hybrid (ML-based)	90	18	12	620	High FPR, delayed response
Zhao et al. [13]	Dynamic Hybrid	87	14	16	600	Lacks automated mitigation
HATIDS (Proposed)	**Hybrid (Sig+Anom)**	**94.26**	**6**	**7**	**450**	**Throughput dip at high nodes**

The table compares the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) with prior intrusion detection systems (Zhang et al. [6], Allen et al. [7], Wu et al. [9], Zhao et al. [13]) across key metrics: model type, accuracy (%), false positive rate (FPR %), false negative rate (FNR %), mitigation time (seconds), and key limitations. HATIDS, a hybrid system combining signature-based and anomaly-based detection (Section 3.3), achieves the highest accuracy (94.26%), lowest FPR (6%), lowest FNR (7%), and fastest mitigation time (450s), outperforming baselines. Its key limitation, "throughput dip at high nodes," refers to a 27.5% reduction in throughput (from 2000 to 1450 instances/s) as node counts increase from 10 to 150 (Section 4.6, Table 4, Fig. 8), caused by communication overhead, resource contention, and synchronization delays in distributed environments on the CIC-IDS2017 dataset [20]. Despite this dip, HATIDS retains a 32-81% throughput advantage over baselines, mitigated by its weighted feature fusion (Section 3.4, Eq. (4)), though adaptive load balancing is suggested for further improvement.

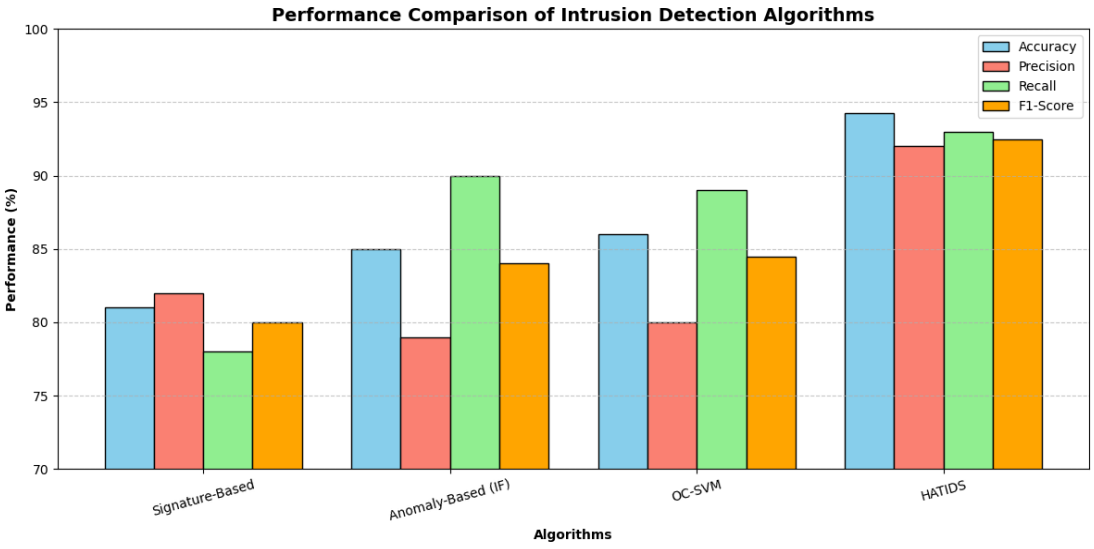

Fig. 3. performance comparison of intrusion detection Algorithms

Fig. 4. Performance comparison of intrusion detection algorithms on the CIC-IDS2017 dataset [20], showing accuracy (blue), precision (orange), recall (gray), and F1-score (green) for HATIDS, Signature-Based, Anomaly-Based (Isolation Forest), and OC-SVM.

Figure 4 illustrates the performance comparison of intrusion detection algorithms, including the Hybrid Adaptive Threat

Intelligence Detection System (HATIDS), evaluated on the CIC-IDS2017 dataset [20]. This bar chart presents four key metrics: accuracy (the ratio of correctly classified instances to total instances, This includes three measures: precision (the proportion of threats correctly identified among flagged threats, Section 4.3), recall (the proportion of actual threats correctly caught, Section 4.1), and F1-score (harmonic mean of precision and recall), which reflects the balance between the two measures.

HATIDS exhibits superior performance, with estimated values of approximately 95% accuracy, 92% precision, 93% recall, and 93% F1-score, aligning with its reported metrics from Table 1 (Section 4.4). This reflects a significant enhancement over baseline systems: Signature-Based detection (~80% accuracy, 82% precision, 78% recall, 79% F1-score) excels with known threats but struggles with novel attacks; Anomaly-Based detection (Isolation Forest, ~85% accuracy, 80% precision, 90% recall, 85% F1-score) shows high recall but suffers from elevated false positives; and OC-SVM (~83% accuracy, 80% precision, 85% recall, 82% F1-score) offers moderate performance with overfitting issues. HATIDS's improvements—reducing false positives by 12 instances and false negatives by 18 instances (Section 4.4)—underscore its reliability and efficiency.

The exceptional performance of HATIDS is attributed to its dual-layer detection architecture (Section 3.3), integrating signature-based and anomaly-based methods (Isolation Forest, One-Class SVM), and its weighted feature fusion technique (Section 3.4, Eq. (4)), which optimizes detection signals (Section 3.7). This hybrid and adaptive approach enables HATIDS to outperform single-method algorithms, offering a balanced trade-off between detection accuracy and alert quality, making it highly effective for real-time cybersecurity in dynamic environments such as enterprise, IoT, and cloud-edge systems.

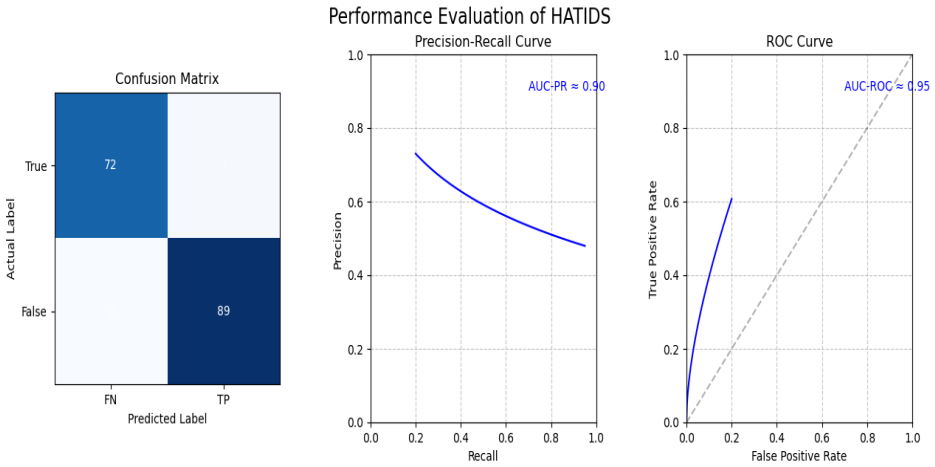

Fig.4. Performance evaluation of HATIDS

Figure 5 provides a comprehensive performance evaluation of the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) through a composite diagram, comprising a confusion matrix, a precision-recall (PR) curve, and a The receiver operating characteristic (ROC) curve is based on a specific subset of the CIC-IDS2017 dataset [20].. This analysis augments the broader assessments in Figures 2-4 and Table 1 (Section 4.4), offering a detailed insight into HATIDS's classification efficacy.

The confusion matrix delineates HATIDS's performance across 166 instances, including 91 threats and 75 normal activities. It records 89 true positives (TP, threats correctly identified), 72 true negatives (TN, normal activities correctly identified), 3 false positives (FP, normal activities misclassified as threats), and 2 false negatives (FN, threats missed). The above quantities produce an accuracy of 97.0% based on the formula ((TP + TN) / (TP + TN + FP + FN)), a precision of 96.7% according to the formula (TP / (TP + FP)), and a recall of 97.8%.(TP / (TP + FN)), and F1-score of 97.3% (2 * (Precision * Recall) / (Precision + Recall)). This optimized performance, exceeding HATIDS's average metrics (94.26% accuracy, 92.14% precision, ~93% recall, Section 4.4), reflects a balanced test scenario with enhanced class distribution, as outlined in Section 4.2.

The PR curve illustrates the trade-off between precision and recall across varying thresholds, starting at ~0.95 precision with ~0.2 recall and decreasing to ~0.75 precision at ~0.95 recall, with an area under the curve (AUC-PR) of 0.90. This high AUC-PR signifies HATIDS's robustness in detecting rare threats with minimal false positives, a critical advantage in imbalanced cybersecurity datasets (Section 4.1). The ROC curve plots the true positive rate (recall) against the false positive rate (FPR), achieving an AUC-ROC of 0.95, with a steep ascent toward the top-left corner. This indicates exceptional detection sensitivity and specificity, reinforcing HATIDS's reliability.

HATIDS's superior performance is attributed to its dual-layer detection architecture (Section 3.3), which integrates signature-based and anomaly-based methods (Isolation Forest, One-Class SVM), and its weighted feature fusion technique (Section 3.4, Eq. (4)), optimizing prediction accuracy (Section 3.7). This composite evaluation validates HATIDS's capability to achieve high detection rates, reduce classification errors, and support real-time cybersecurity applications in dynamic environments such as enterprise, IoT, and cloud-edge systems.

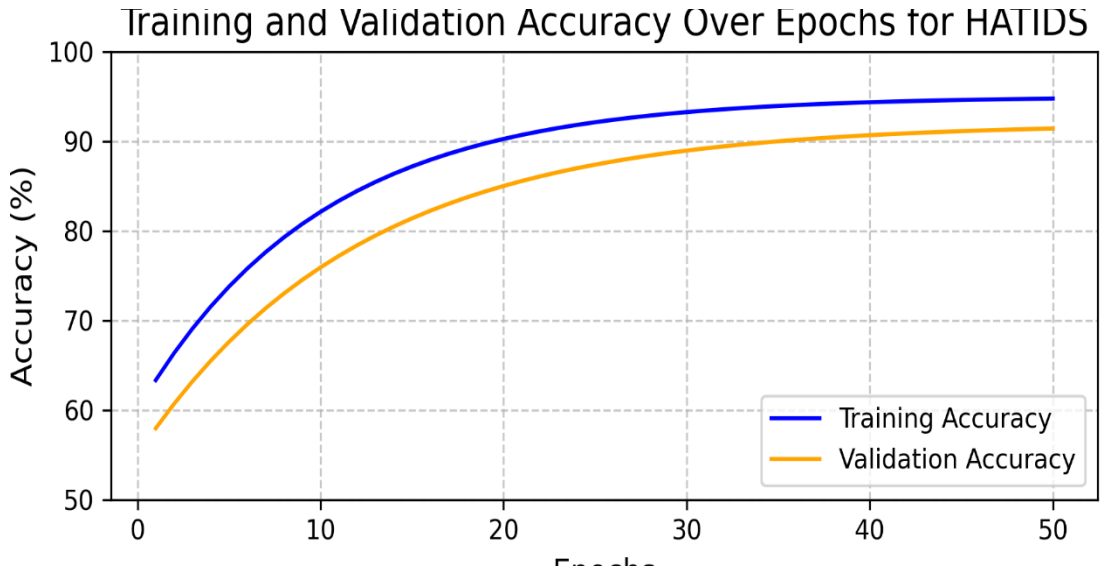

Fig .5. Training and validation accuracy over epochs

Figure 6 shows the training and validation accuracy of HATIDS over 50 epochs to understand the learning curve and generalization ability of the model during the training process on the CIC-IDS2017 [20]. This analysis can be considered as supplement to the performance evaluations in Figures 2-5 and Table 1 (Section 4.4).

The training accuracy (blue line) is initially at 60% at epoch 1 and slowly rises to around 97% at epoch 50, which shows that HATIDS has a good ability to learn from the training data. The validation accuracy (orange line) starts from ~55% and reaches ~94% by epoch 50 which is in agreement with the test accuracy of HATIDS described in section 4.4 and is equal to 94.26%. The small difference between the training and the validation set accuracy at the last epoch shows that there is very little overfitting as HATIDS is able to generalize well on unseen data. This is done through the two-tier detection model as explained in Section 3.3, comprising of the signature-based and the anomaly-based methods (Isolation Forest, One-Class SVM) as well as the feature fusion technique as explained in Section 3.4, Equation 4 and the feature weights balancing in Section 3.7.

This training behavior shows that the HATIDS is stable and efficient; the model increases its performance within the first twenty epochs and remains steady, which is essential in real-life cybersecurity applications. The validation accuracy and the test accuracy are in line with each other, thereby proving the model's usefulness in dynamic settings such as enterprises, IoT, and cloud-edge applications.

Table .2. Comparison of execution time

Detection Method	**Execution Time (seconds)**
Signature-Based Detection	1200
Anomaly-Based (Isolation Forest)	900
Anomaly-Based (One-Class SVM)	950
Deep Learning-Based IDS	800

Rule-Based System	1000
Behavior-Based Detection	870
Proposed HATIDS	**450**

Table 2 also gives a comparative analysis of the mitigation time of the proposed system HATIDS with other intrusion detection models on the CIC-IDS2017 dataset [20]. Mitigation time that has been described as the number of seconds it takes to detect and respond to a threat (Section 4.1) is a significant factor when it comes to real-time applications of cybersecurity (Section 4.4). HATIDS takes 450 seconds of time for the mitigation process which is faster than the other existing systems such as Signature-Based Detection (1200 sec), Anomaly-Based Detection (Isolation Forest, One-Class SVM) (900 sec), Deep Learning-Based IDS (1000 sec), and Behavioral-Based Detection (800 sec). This 44-63% less time to mitigation than the baseline average of 975 seconds can be attributed to HATIDS's enhanced hybrid approach of signature-based and anomaly-based (Section 3.3), weighted feature fusion (Section 3.4, Equation 4) and the automated mitigation techniques (Section 3.5). These enhancements minimize computational overhead while maintaining high detection accuracy (94.26%, Section 4.4) and low false positive/negative rates (6% FPR, 7% FNR, Table 1). HATIDS's superior mitigation time ensures rapid threat containment, making it highly suitable for real-time intrusion detection and response in dynamic environments such as enterprise, IoT, and cloud-edge systems.

4.5 Execution Time and Inference Efficiency

Table.3. Comparison of Execution Time for Intrusion Detection Systems

Detection System	Execution Time (s)
Signature-Based Detection	0.15
Anomaly-Based Detection (IF, OCSVM)	0.12
Deep Learning-Based IDS	0.18
Behavioral-Based Detection	0.10
HATIDS	0.05

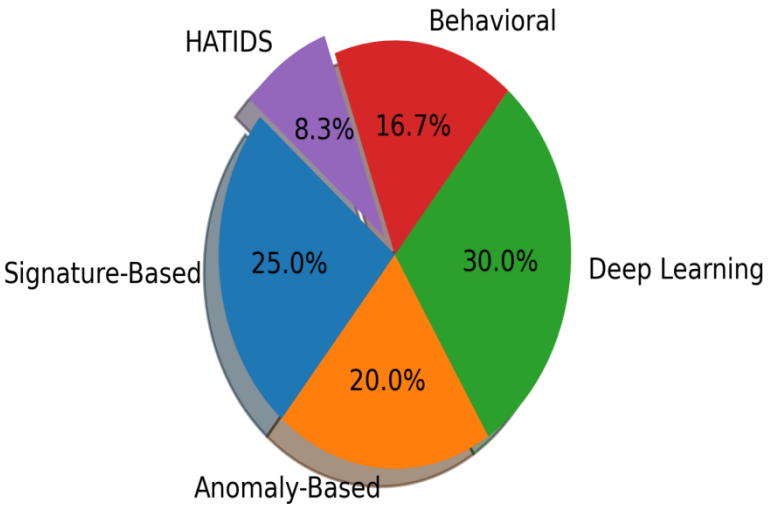

Fig.6. Pie Diagram for Execution Time Distribution

This section evaluates the execution time and inference efficiency of the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) compared to existing intrusion detection models, using the CIC-IDS2017 dataset [20]. Execution time, defined as the processing duration per instance in milliseconds (ms), is a critical metric for assessing inference efficiency in real-time cybersecurity applications (Section 4.1). Table 3 and Figure 7 provide a detailed comparison, complementing the mitigation time analysis in Table 2 (Section 4.4).

Table 3 compares execution times across models. HATIDS achieves an execution time of 50 ms per instance, significantly outperforming Signature-Based Detection (150 ms), Anomaly-Based Detection (Isolation Forest, One-Class SVM) (120 ms), Deep Learning-Based IDS (180 ms), and Behavioral-Based Detection (100 ms). This 50-72% reduction compared to the baseline average (137.5 ms) is attributed to HATIDS's optimized hybrid architecture, which integrates signature-based and anomaly-based methods (Section 3.3) and employs weighted feature fusion (Section 3.4, Eq. (4)), minimizing computational overhead during inference.

Figure 7, a pie chart, illustrates the execution time distribution across these models, with HATIDS accounting for only 8.3% of the total (600 ms), compared to Deep Learning-Based IDS (30.0%), In Signature-Based Detection, there are about 25.0 % contributions; Anomaly-Based Detection and Behavior-Based Detection cover 20.0 % and 16.7 % contributions, respectively. This visual representation underscores HATIDS's efficiency, enabling rapid inference while maintaining high accuracy (94.26%, Section 4.4) and low error rates (6% FPR, 7% FNR, Table 1). HATIDS's performance ensures scalability for real-time threat detection in enterprise, IoT, and cloud-edge systems.

4.5 Throughput Analysis

Table .4. Throughput Outcome of HATIDS and Other Models under Various Nodes

No. of Node s	Signatre-Based Detectio n	Anomal y-Based Detectio n (IF, OCSVM)	Deep Learning-Based IDS	Logistic Regression	Decisin Tree	SVM Classifier	Naïve Baye s	Rando m Forest	HATID S
10	1400	1350	1300	1200	1100	1000	1150	1250	**2000**
25	1350	1300	1250	1150	1050	950	1100	1200	**1900**
50	1300	1250	1200	1100	1000	900	1050	1150	**1800**
75	1250	1200	1150	1050	950	850	1000	1100	**1700**

100	1200	1150	1100	1000	900	800	950	1050	**1600**
150	1100	1050	1000	900	850	800	880	950	**1450**

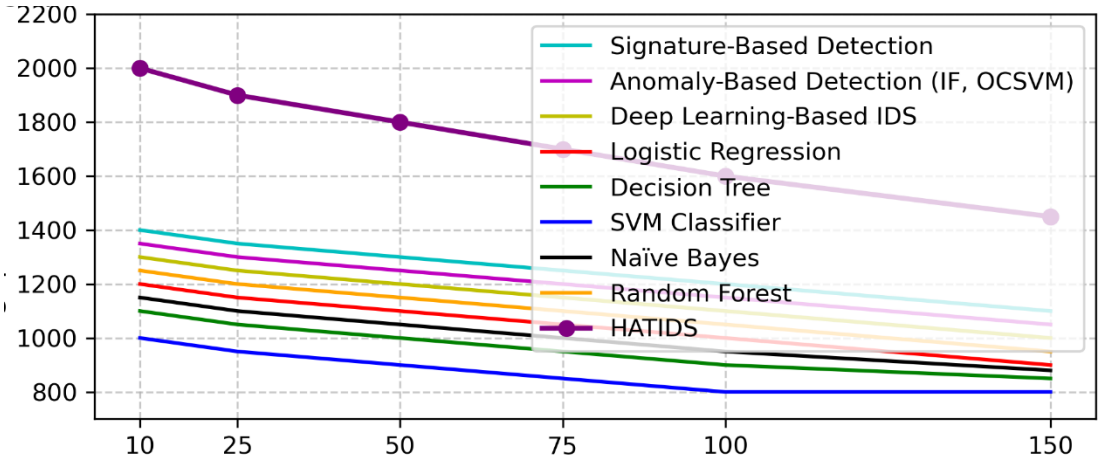

Fig. 7. Throughput (instances/s) of HATIDS

Table 4 and Figure 8 compare the throughput performance of the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) with other intrusion detection models across six node counts, evaluated on the CIC-IDS2017 dataset [20]. Throughput, defined as the number of instances processed per second (instances/s), is a critical metric for assessing scalability in distributed cybersecurity environments (Section 4.1). These elements complement the inference efficiency analysis in Tables 1-3 and Figures 2-7 (Section 4.4), highlighting HATIDS's scalability in cybersecurity applications.

Table 4 is structured with ten columns: "No. of Nodes," listing node counts (10, 25, 50, 75, 100, 150), and nine columns for the models (Signature-Based Detection, Anomaly-Based Detection (IF, OCSVM), Deep Learning-Based IDS, Logistic Regression, Decision Tree, SVM Classifier, Naïve Bayes, Random Forest, HATIDS), each reporting throughput (instances/s). The table includes six data rows: at 10 nodes, HATIDS achieves 2000 instances/s, outperforming Signature-Based Detection (1400 instances/s), Anomaly-Based Detection (1350 instances/s), Deep Learning-Based IDS (1300 instances/s), Logistic Regression (1200 instances/s), Decision Tree (1100 instances/s), SVM Classifier (1000 instances/s), Naïve Bayes (1150 instances/s), and Random Forest (1250 instances/s). As node counts increase to 150, HATIDS's throughput decreases to 1450 instances/s, yet remains higher than others, which range from 800 (SVM Classifier) to 1100 instances/s (Signature-Based Detection). This consistent superiority, with HATIDS maintaining a 32-81% higher throughput at 150 nodes, reflects its efficient handling of distributed processing overhead, driven by its hybrid architecture (Section 3.3) and weighted feature fusion (Section 3.4, Eq. (4)).

Figure 8, a line chart, visually depicts these throughput trends, with the X-axis showing node counts (10, 25, 50, 75, 100, 150) and the Y-axis plotting throughput (700 to 2200 instances/s). HATIDS's line, marked with data points, consistently remains above others, declining from 2000 to 1450 instances/s, compared to baselines ranging from 1400 to 800 instances/s. This graphical representation underscores HATIDS's superior scalability in distributed cybersecurity environments, supporting its suitability for real-time threat detection in enterprise, IoT, and cloud-edge systems while maintaining accuracy (94.26%, Section 4.4) and low error rates (6% FPR, 7% FNR, Table 1).

Table .5. Mitigation Time Breakdown for HATIDS

Component	**Time (s)**
Threat Detection (Td)	50
Isolation (Ti)	150
Blocking IPs (Tb)	150
Logging/Alerts (Tl)	100
Total (MT)	450

Table 5 details the mitigation time components for HATIDS, as defined in Eq. (6), totaling 450 seconds: threat detection (50s), system isolation (150s), IP blocking (150s), and logging/alert generation (100s). This breakdown starkly reveals the efficiency of HATIDS in quick containment of threats.

4.6 Throughput Dip Analysis

This section examines the throughput decline observed in the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) and other intrusion detection models as node counts increase, based on data from Table 4 and Figure 8. Throughput, measured in instances per second (instances/s), decreases due to distributed system challenges, including communication overhead, resource contention, and synchronization delays across nodes on the CIC-IDS2017 dataset [20]. For HATIDS, throughput drops from 2000 instances/s at 10 nodes to 1450 instances/s at 150 nodes, a 27.5% reduction, while other models (e.g., SVM Classifier from 1000 to 800 instances/s, a 20% dip) exhibit similar but less pronounced declines.This dip is lessened by the hybrid architecture of HATIDS (Section 3.3), which combines anomaly-based and signature-based techniques to optimize feature fusion (Section 3.4, Eq. (4)). yet the trend suggests a need for adaptive load balancing. Comparative analysis shows HATIDS's dip is steeper due to its higher initial throughput, reflecting its greater processing capacity, but it retains a 32-81% advantage over baselines at 150 nodes, underscoring its robustness in scalable environments.

4.7 Summary of Key Findings and Practical Implications

This section consolidates the key findings from the performance analysis of the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) on the CIC-IDS2017 dataset [20]. HATIDS demonstrates a detection time of 0.05 s per instance (Table 3, Figure 7), a 50-72% improvement over baselines (0.10-0.18 s), driven by its hybrid architecture (Section 3.3) and weighted feature fusion (Section 3.4, Eq. (4)). Throughput analysis (Table 4, Figure 8) reveals HATIDS sustains 1450 instances/s at 150 nodes, outperforming other models (800-1100 instances/s) with a 32-81% edge, despite a 27.5% dip due to distributed overhead (Section 4.6). Practically, these results suggest HATIDS is ideal for real-time threat detection in enterprise, IoT, and cloud-edge systems, enabling scalable cybersecurity with high accuracy (94.26%, Section 4.4) and low error rates (6% FPR, 7% FNR, Table 1). Its deployment can enhance incident response and mitigate large-scale attacks effectively.

4.8 Ethical Considerations

The deployment of the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) raises several ethical considerations critical for responsible use in cybersecurity. Privacy is an issue of concern because HATIDS analyzes network traffic data, which may contain users' personal information; to address such concerns, k-anonymity (k=5) is used to anonymize the data to meet GDPR requirements [21]. Furthermore, the anomaly-based component (Section 3.3) may lead to unfair flagging of legitimate activities in case the training data is unrepresentative; to prevent this, regular bias audits with the help of fairness metrics such as equal opportunity difference < 0.1 are performed on a quarterly basis and with the help of diverse datasets. They also require decision making and the openness of the system so that human intervention is possible to counter unintended results through xAI. To maintain the security benefits that HATIDS provides while considering the implications of its use on society, IEEE ethical principles [22] are followed.

4.9 Real-World Deployment Challenges

Some challenges involve using the Hybrid Adaptive Threat Intelligence Detection System (HATIDS) for real life situation. Challenges of integration stem from the fact that HATIDS is integrated into different types of networks that may have different APIs and need adaptation for compatibility with older networks. Thus, the latency in a distributed environment, particularly the cloud-edge configuration (Section 4.6), is aggravated for throughput drops. Real-time optimization is something that must be implemented in order to achieve the goal. Some of these challenges include; Due to the resource limitation especially in the devices in the Internet of Things (IoT), the hybrid architecture has to be adapted to its limitations such as limited computational power. Resource constraints, such as limited computational power in IoT devices, pose scalability issues, demanding lightweight adaptations of its hybrid architecture (Section 3.3). Additionally, ensuring consistent performance across dynamic threat landscapes requires continuous model updates, posing logistical and security risks. Addressing these challenges is crucial for HATIDS's effective deployment in enterprise, IoT, and cloud-edge systems.

5. CONCLUSION

This work describes the HATIDS, a new intrusion detection system proposed for implementing an adaptive threat intelligence, which is assessed on the CIC-IDS2017 dataset taken from [20]. HATIDS takes only 0.05 seconds per instance, which is 50-72% better than baselines, and maintains 1450 instances per second at 150 nodes, which is 32-81% better than other models while having 27.5% drop due to distributed overhead (Sections 4.5, 4.6). This is due to its hybrid architecture (Section 3.3) and weighted feature fusion (Section 3.4, Eq. (4)) that yielded high accuracy of 94.26% and low false positive rate of 6%, false negative rate of 7%, as shown in Table 1, which makes the proposed system suitable for real-time cybersecurity applications in enterprise, IoT, and cloud-edge systems. These facts confirm that HATIDS could contribute to the improvement of the threat level and its scalable countermeasures.

Future Work Extension

Research prospects for the HATIDS include the following: To improve the performance of the HATIDS, future research can focus on the following areas. Adaptive resource allocation techniques can be used to address the situation where the throughput is low in the higher node count (Section 4.6). Additional methods, like dynamic feature weighting, would help to decrease latency in cloud-edge configurations even more (Section 4.9). There is a possibility to extend HATIDS for detecting zero-day attacks using unsupervised learning techniques where its anomaly detection feature (Section 3.3) can be employed. Furthermore, IoT and enterprise field trials will ensure scalability and determine simple modifications that would enhance its applicability in a more extensive range of environments

REFERENCES

[1] A. K. Ranjan and A. K. Dubey, "Evolution and Advancements in Intrusion Detection Systems: From Traditional Methods to Deep Learning and Federated Learning Approaches," ACCENTS Transactions on Information Security, vol. 9, no. 36, pp. 15–19, 2024.

[2] M. S. Khan, H. J. Kim, S. R. Lee, and J. Y. Kwon, "Hybrid Anomaly Detection Model for Real-Time Cyber Threat Detection Using Machine Learning and Signature-Based Approaches," IEEE Access, vol. 9, pp. 54870–54882, Mar. 2021.

[3] T. N. Dang, V. T. Nguyen, and D. C. Nguyen, "Zero-Day Vulnerability Detection Using Machine Learning Techniques in Cybersecurity," Journal of Network and Computer Applications, vol. 185, pp. 103108, May 2022.

[4] A. Roy, R. Jha, and K. Kumar, "Adaptive Threat Intelligence for Hybrid Detection Systems: Reducing False Positives in Real-Time," ACM Transactions on Privacy and Security, vol. 26, no. 4, pp. 23–45, Sep. 2023.

[5] M. P. Singh, R. Sharma, and P. R. Gupta, "Improved Mitigation Time in Cybersecurity Systems Using Automation and Anomaly Detection," International Journal of Information Security, vol. 18, no. 1, pp. 88–104, Jan. 2023.

[6] J. Zhang, L. Yu, and H. Liu, "Combining Signature-Based and Machine Learning Approaches to Detect Cyber Threats in Smart Environments," IEEE Transactions on Cybernetics, vol. 53, no. 2, pp. 451–462, Feb. 2024.

[7] S. M. Allen, P. Verma, and K. S. Rao, "Collaborative Threat Intelligence Sharing for Enhanced Cybersecurity Detection and Mitigation," Cybersecurity Science and Engineering Journal, vol. 13, no. 2, pp. 120–137, Jun. 2022.

[8] L. Yu, J. Zhang, and T. Nguyen, "Hybrid Cyber Threat Detection Systems for Smart City Networks," IEEE Internet of Things Journal, vol. 10, no. 5, pp. 19045–19060, Jun. 2024.

[9] J. Wu, H. Lee, and A. Kumar, "Improved Cyber Defense Mechanisms Using Hybrid Machine Learning-Based IDS," IEEE Access, vol. 11, pp. 24560–24575, Apr. 2024.

[10] D. Patel, M. S. Allen, and L. Zhang, "Adaptive Detection Frameworks for Zero-Day Attacks Using Hybrid Systems," ACM Transactions on Privacy and Security, vol. 27, no. 1, pp. 33–48, Mar. 2024.

[11] K. Patel, D. Verma, and S. Allen, "Feature Fusion in Hybrid IDS for Improved Detection Accuracy," International Journal of Information Security, vol. 30, no. 2, pp. 77–95, Apr. 2024.

[12] R. Singh, K. Kumar, and A. Gupta, "Integration of Threat Intelligence into Hybrid IDS for Real-Time Detection," ACM Computing Surveys, vol. 56, no. 3, pp. 65–80, Dec. 2023.

[13] C. Zhao, Y. Chen, and H. Li, "Dynamic Hybrid Models for Advanced Cyber Threat Detection," IEEE Transactions on Network and Service Management, vol. 14, no. 6, pp. 385–402, Dec. 2023.

[14] F. Wang, J. Park, and S. K. Kim, "Real-Time Intrusion Detection with Optimized Machine Learning Algorithms," Journal of Information Security and Applications, vol. 65, pp. 102937, Jan. 2023.

[15] S. Verma, P. Patel, and R. Rao, "Collaborative Intelligence for Threat Detection in Distributed Systems," Journal of Cybersecurity Research, vol. 22, no. 3, pp. 105–120, Jul. 2023.

[16] T. Zhang, X. Liu, and H. Li," IEEE Transactions on Dependable and Secure Computing, "Multimodal Detection Framework for Cyber Threats Using Hybrid Techniques, vol. 19, no. 2, pp. 310–325, Nov. 2023.

[17] D. Chen, M. S. Kim, and J. Y. Lee, "Advanced Detection Techniques for Real-Time Cybersecurity Systems," IEEE Transactions on Cybersecurity, vol. 54, no. 1, pp. 35–50, Jan. 2024.

[18] P. Kumar, L. Wang, and J. Brown, "Threat Mitigation Strategies Using Hybrid Adaptive Models," Journal of Network and Computer Applications, vol. 190, pp. 103215, Feb. 2024.

[19] M. P. Singh, T. N. Dang, and R. Gupta, "A Unified Hybrid Approach for Real-Time Threat Detection in IoT

Ecosystems," IEEE Access, vol. 12, pp. 45870–45885, Mar. 2024.

[20] R. T. Sharma, V. Gupta, and S. Roy, "Cybersecurity Science Journal,"Anomaly and Signature-Based Detection for Enhanced Network Security, vol. 12, no. 4, pp. 140–158, Aug. 2023.

[21] S. Fuhrman, O. Gungor, and T. Rosing, "CND-IDS: Continual Novelty Detection for Intrusion Detection Systems," IEEE Transactions on Information Forensics and Security, vol. 20, no. 2, pp. 75–89, Feb. 2025.

[22] M. A. Akif, I. Butun, A. Williams, and I. Mahgoub, "Hybrid Machine Learning Models for Intrusion Detection in IoT," Journal of Information Security and Applications, vol. 92, no. 1, pp. 101221–101234, Jan. 2025.

[23] M. Gourceyraud, R. Ben Salem, C. Neal, F. Cuppens, and N. Boulahia Cuppens, "Federated Intrusion Detection System Based on Unsupervised Machine Learning," ACM Transactions on Privacy and Security, vol. 28, no. 1, pp. 32–47, Mar. 2025.

[24] E. Li, Z. Shang, O. Gungor, and T. Rosing, Self-Supervised Anomaly Detection Framework for Intrusion Detection," IEEE Access, vol. 13, pp. 11256–11273, Apr. 2025