Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 10, 2025

AN ADAPTIVE CYBERSECURITY THREAT PROTECTION TECHNIQUE USING MACHINE LEARNING AND BIG DATA ANALYTICS

Muhammad Siddique[*1], Dr. M. Milhan Afzal Khan[2], Dr. Junaid Arshad[3]

*[*1] MSc Data Science University of Engineering and Technology, Lahore, Pakistan*
[2]Assistant Professor Department of Computer Science University of Agriculture, Faisalabad, Pakistan
[3]Associate Professor Department of Computer Science University of Engineering and Technology, Lahore, Pakistan

[*1]muhammadsiddiquem247@gmail.com, [2]milhankhan@uaf.edu.pk, [3]mjunaiduet@gmail.com

DOI: https://doi.org/10.5281/zenodo.17541606

Keywords

Article History
Received: 27 August 2025
Accepted: 20 October 2025
Published: 31 October 2025

Corresponding Author: *
Muhammad Siddique

Abstract

This research introduces a dynamic cybersecurity threat protection system that combines machine learning algorithm and big data analytics to improve detection, prediction and reaction to dynamic cyber threats. On benchmark intrusion detection data sets (CICIDS2018, UNSW-NB15), the current methodology proposes the application of data preprocessing, feature engineering, and a hybrid of Random Forest and LSTM networks. Multi-class metrics, feature importance, and detection performance are visualized on an interactive dashboard in real-time and delivered by API. Findings indicate that most of the kinds of attacks have an accuracy close to full accuracy with a few gaps still remaining in terms of detecting certain forms of threats like the SQL Injection. Adaptive learning loop of the system with continuous training and periodic retraining enables the system to remain resilient to attacks that involve zero-day threats and adversarial styles. It underscores the promise of execution driven, scalable, and explainable proposals in overcoming the shortcomings of classical signature based cybersecurity measures and at the same time underlines the importance of continuous learning and well-trained adversarial defense.

INTRODUCTION

It has been observed that the emerging levels of difficulty and massiveness of cyber threats require the creation of highly responsive and programmed defence structures that can be harnessed beyond the boundaries of signature-based cyber defence methods [1]. The need has created a paradigm shift to intelligent security solutions which are powered by machine learning advancements and advances in big data analytics to detect and eliminate advanced attacks in real-time [2]. The proposed study reviews one of the adaptive methods of cybersecurity threat protection which includes the combination of machine learning algorithms and big data analysis frameworks to increase the ability to detect threats, predict the occurrence of threats and respond to them in an effective way. The underlying idea of such an integrated approach is to offer a robust protection against changing cyber threats by utilizing large volumes of data to identify obscure patterns and anomalous actions pointing to abnormal behaviors that could be malicious in nature [3] [4].

This system is supposed to dynamically adapt to the emerging threats in order to develop into a system which is more resilient and intelligent than what can

be observed or rather, defensive schemes. The prevalence of machine intelligence in the modern scenarios involving the use of cybersecurity practices is a pointer towards the concept that its use is inevitable in the safeguarding and attacking strategies experienced by fast rising and maturing menaces [5]. This requires a more intense consideration of opportunities and directions of application of AI and machine learning techniques to the strengthening of cybersecurity by transcending the realm of the OT-based solutions with more forecasting and adjusting [3] [6]. This transformation is extremely valuable due to the fact that current strategies can hardly keep pace with and constantly growing sophistication of cyberattacks [7]. Indeed, coupled with machine learning, cybersecurity presents a tremendous leap because without it, trends and information regarding large network data would not be distinguishable [4].

The given paper is specifically devoted to utilizing machine learning and artificial intelligence in improving the detection and response capacity of cybersecurity systems to foster later and more efficient management of security breaches, such as new types of malware and zero-day exploits [8] [9]. This dynamic solution takes advantage of the efficacy of real time data mining and predictive modeling in highlighting threats and neutralizing them before they can lead to massive harm enhancing overall security of an organization against constant and dynamic cyber threats [8] [10]. Customized models of attacks and continuous changes in cyber threats render it essential to apply artificial intelligence and machine learning methods in setting up better and resilient cybersecurity systems that can detect and neutralize an attack in real-time [11] [12]. With such proactive approach systems are capable of learning and developing their own defensive tactics on their own and thus countering the development of potential threats prior to their total actualization [13] [14].

Artificial intelligence, specifically, machine learning, has had significant impacts across areas, with cybersecurity being one of the most common aspects where it helps in automating activities, processing large amounts of data, and predicting the occurrence of future attacks [15] [16]. This combination assists in sifting through the massive amount of security information to detect the slightest of abnormalities that are an indicator of a cyber-attack [4]. Reactive cyber defense is commonly ineffective in the face of modern attacks due to the speed and sophistication of the latter, and thus, more proactive methods are demanded [17]. Reactive defense is no longer an option since cybercrimes are becoming more and more sophisticated and in size [18]. The development has enabled the security systems to go beyond detecting the attack to predict and prevent attacks, which is a milestone revolution in the defensive strategies [19]. The impractical speed of analyzing innumerable amounts of data and correlating with anomalous patterns that AI-driven systems possess are far beyond the capabilities that a human being would be able to handle in the battle against advanced persistent threats and zero-day exploits [20]. This is especially important because there has been an increased cyberattack, and strong cyber defense has become a central issue to every entity [21]. This dynamic change also requires dynamism in security that is why artificial intelligence is becoming a critical tool in upgrading security efforts [22].

It is not just that the use of AI in cybersecurity supplements the current security setups by introducing new solutions but also sets a whole new paradigm of successfully dealing with cyber threats using predictive and preventive counter-mechanisms [23]. Artificial intelligence has become a priority in protecting systems connected to the internet that are facing different threats such as attacks, damaged, or compromised due to unauthorized access during the Fourth Industrial Revolution [24]. The unique pace at which the field of technology evolves, along with the rising patterns of automation and the spread of IoT products and gadgets, highlights the invaluable usefulness of AI-driven applications in countering the arising cybersecurity risks [20]. The management of security policies can also be done with the aid of AI where the latter will advise on changes to firewall settings, intrusion prevention systems, etc. according to the changing threat dynamics [8]. It presents the need to adopt new strategies where artificial intelligence can be used to increase their cybersecurity levels that deal with many issues related to vulnerable coding, compromised CI/CD pipelines, and insufficient logging [25]. The growing complexity and rates of cyber-attacks demand the necessity of new defensive measures, which are able to quickly respond

to new vectors and protocol methods of the attacks [26].

In particular, artificial intelligence offers solutions that can immediately detect and respond to dangers as well as predict what threats are yet to come by relying on advanced models of analysis [25]. It is estimated that the market of AI within the sector of cyber security will grow significantly, promising to rise in its significance to addressing the problem of cyber threats [27] [28]. The factor behind this growth is the rising awareness and the need to have more secure and effective cybersecurity solutions in every industry [29]. Cybersecurity tools based on artificial intelligence are promising to improve threat detection, responding, and prevention mechanisms by offering high-level capabilities of analysis and fast threat intelligence [30]. Its use has been found to be quite knowledgable across many areas of work such as finance where it has a tremendous effect on the markets, their institutions, and laws [31]. This disruptive technology allows the possibility of substitution of using human labor in a wide range of applications especially in critical infrastructure where dynamic gathering, and examination of network traffic is fundamental in communicating the fraudulent activity [32]. This transition to AI-based defense mechanisms has been an inevitable reaction to an increasingly high-level of complexity of cyber threats, which often evade conventional, signature-based, detection techniques [13].

Nevertheless, the use of AI-inspired systems alone cannot imply complete cover against any threat within the systems; thus, active cooperation with human cybersecurity experts is needed to improve the level of decision-making and reactions [33]. It is hypothesized that this is a form of symbiosis commonly referred to as augmented intelligence that involves combining the unsurpassed computational ability of AI with the expertise of thoughtful human intelligence and strategic reasoning in order to form a more resilient and adaptive defense mechanism [34].

Literature Review

Extensive review of the existing deployments of AI in cybersecurity shows its far-reaching versatility in automating common tasks in addition to faster identification of threats and the accuracy of defensive interventions against the various cyber menaces [16]. Current innovations demonstrate the potential of AI in strengthening the activities of cybersecurity, which opens advanced possibilities of studying intrusion and malware and protecting privacy [13]. Such an effective technology enables cybersecurity professionals to strengthen their security status against different security challenges and cyber-attacks [16]. The literature critically discusses the use of AI in security systems in several industries in which it proved to be a useful tool in frequent identification, prevention, and minimization of complicated cyber-attacks than traditional means [35] [36].

AI has made a tremendous contribution to other related areas and the sciences and has transformed human communication and the understanding of society [37]. It has taken root in military use-cases, empowering its abilities in areas of autonomous weapons and intelligence [38]. The codification of AI methods is utilized to facilitate a resilient system corpus, which evolves with new threats and forms an effective preventative tool with respect to the advancing cybercrime [39] [25]. The goal of this review is to summarize the recent literature on various types of cyber-attacks and the associated detection tools and algorithms to define the current gaps in the knowledge and challenges in the field with the aim to further investigate the use of AI-based protection against them [7]. Although the historical development of the AI has enjoyed swift developments, its use in cybersecurity is exceptional in its role of analyzing the large databases and identifying complex patterns to detect malicious activities [40]. This is used to take full advantage of AI through its ability to analyze large amounts of data and even predict and prevent future attacks, identifying so-called dark signals and emergent threat patterns [16]. Moreover, the ability of AI to act in an autonomous and fast manner enables it to be responsive to threats at a speed and accuracy that is not possible with systems that are human oriented, thus reducing the time frame that attackers would work with [15]. The growing complexity of cyber-attacks, in particular, the ones against AI-based systems themselves, requires durable AI methods of active cyber defense [41].

Nonetheless, there are also two sides to the increasing strength of AI: With the help of AI, cyber attackers can create more complex and evasive threats, which requires ever-greater innovation in AI-based protective

mechanisms [42] [43]. This highlights the tremendous importance of superior AI approaches that cannot merely identify a possibility of advanced attacks, but also predict new threat vectors to that end [42]. This is a never-ending adversarial game that requires the creation of robust AI models that can respond to the emerging strategies of attackers and detect the already unknown threats [17]. This encompasses the use of AI to detect anomalies, perform behavioural analysis and predictive analytics to be one step ahead of bad actors [44]. These methods are critical in improving the combat readiness of businesses and organizations who continue to face the dynamic, and frequently occurring malware attacks [43]. The extreme speed of changes in cyber threats, especially those using advanced persistent threat methods, demonstrates the inefficiency of the traditional rule- and signature-based detector systems, so the creation of more complex AI, and machine learning-based tools is needed [45] [46]. Such traditional techniques are becoming less effective defenses against the polymorphic malware and zero-day exploits that will use innovative obfuscation to avoid detection [8]. This calls into play a paradigm shift to cheaper, smarter, adaptive security models capable of learning and to be able to detect minor signs of compromise that a static security model cannot do effectively [8].

It is exactly this gap that artificial intelligence (AI)-enabled methods, specifically, deep learning, and machine learning, are trying to fill, which promises the capacity to process large volumes of data in real-time, recognize complex patterns and adjust promptly to unseen threats [7]. This would enable the creation of highly effective predictive models capable of accurately predicting the emergence of potential cyber threats before they reach full effect and thus act proactively in the establishment of a defense strategy [17]. This allows a more proactive security state and this is going beyond responding to measures to being predictable and preventive [8] [47]. The artificial intelligence being adapted to cybersecurity represents a tremendous step towards monitoring networks whereby huge traffic can be measured to help identify the complicated patterns and anomalies automatically [48]. This move towards the application of AI-driven solutions is an essential one since common forms of cybersecurity protections are frequently finding themselves unable to keep up with the continuous stream of more and more advanced and widespread cyber-attacks [49]. Through this technological synergy, zero-day exploits and polymorphic malware will be automatically detected and they are not usually detected by the traditional signature-based systems [3]. The increasing opinion in the cyber security field is that the malware antimalware tools and systems based on artificial intelligence and machine learning will play an important role in neutralizing modern malware attacks [50]. These smart systems have the capability of processing large volumes of data, acquiring experiences of prior events and detecting low intensity anomalies which could signal a new attack hence making the detection levels high and the response time much shorter [44].

A subset of AI, machine learning presents a potential solution by deploying automation and intelligence to address many cyberattack challenges and can be well suited at locating complex associations on data and generalizing to as-yet-unseen forms of attack [51] [52]. Such functionality enables the creation of adaptive security systems that will be able to upgrade their threats during the detection through novel experience and evolving attack techniques [53]. Increased rates and complexity of cyberattacks have necessitated the development of constant improvements in the detection process of malware since conventional signature-base detection has provided critical constraints in detecting emerging and sophisticated attacks [2]. Use of machine learning, Deep learning and artificial intelligence in cyber security has emerged as critical in the improvement of threat detecting, preventing and responding to them [54] [55]. Such intelligent systems can study masses of data by using advanced algorithms, and learn how attacks have been done in the past and adjust to new and emerging attacks with a high degree of effectiveness [56]. More specifically, ML-based Intrusion Detection Systems have the locus to identify whether network activities are positive or indeed malicious by training on a variety of datasets, thus ensuring the improved security measures based on the continuous adaptation to the ever-changing nature of cyber threats [57]. Such ability is essential as modern malware frequently utilizes obfuscation and polymorphism making it so that dynamic signature databases make the previously used static signature databases obsolete [58]. The combination of various machine learning models and

usage of explainable AI algorithms will be essential to improving usability and interpretability of such systems [19]

These models can detect complex contemporary attacks that require sophisticated and forward-looking detection mechanisms, hence bolstering the integrity of an organization as a whole [59]. Namely, machine learning models have the capacity of examining vast amounts of network data and identifying anomalies, malicious behaviors, as well as forecasting the possibility of cyber threats on-demand [60] [61]. Rapid changes in the latest processing progress are essential in proactively defending, where the security agent can stop it before serious damage can be done [19]. Nevertheless, most of the machine learning-based detection methods have the disadvantage that they do not learn well when immersed in the large and recent network traffic data [62]. Moreover, a major problem with the usefulness of those models is that they are usually adversarial, delicate to the input data by using hitherto unidentified tricks so as to not get detected [63]. Such susceptibility entails effective, dynamic learning processes capable of continuously updating their knowledge within the realms of normal and malicious behaviour within the prolific dynamic network settings [64]. Moreover, the large amount of network traffic creates a copious quantity of data, frequently with all the duplicates, and irrelevant data, which is an arduous task to process efficiently and train the models [65] [66]. This will require state of the art feature engineering and selection algorithms to extract useful information out of raw network flows and optimize the effectiveness and precision of machine based learning models [67].

Here is a comparison table summarizing key aspects discussed in the literature review regarding AI and machine learning in cybersecurity:

Aspect of AI/ML in Cybersecurity	Contribution/Benefit	Limitations/Challenges	Comparison to Traditional Methods
General Utility	Replaces the human labour involved in repetitive tasks, speeds up the identification of threats, improves the effectiveness of the defensive steps, and strengthens security situations to address multiple challenges and cyberattacks.	Using AI, cybercriminals will be able to produce more advanced and elusive threats, which will require ongoing AI defenses development.	Generally, better at identifying, inhibiting and curbing the effects of complex cyber-attacks as compared to the conventional approaches.
Threat Detection & Prevention	It allows intrusion detection, classification of malware, and privacy protection. Processes large amounts of information to determine complicated patterns, forecast attacks, and pre-empt their occurrence, as well as detect tiny anomalies that showcase the existence of malicious campaigns.	Exposure to an adversarial attack, in which attackers can smooth inputs to deceive or induce false positives. Static training can be a setback to the effectiveness of models.	The paradigm shift provided offers the period of being reactive to proactive, predictive and preventative models, which removes the ineffectiveness of the historic rule-based and signature-based systems against polymorphic malware and zero-day exploits. Is able to identify threats which

			otherwise would not be identified.
Adaptability & Responsiveness	Enables responsive adjustment to new menaces. Gives the possibility to act swiftly and independently at speeds that a human-based system often does not compete with. Facilitates unending adjustments to changing cyber threats.	Demands strong, adaptive learning algorithms that can carry out continuous relearning to learn both normal and malicious behaviors in ever evolving network scenarios.	Transcends the innate stagnancy of traditional security frameworks to provide an adaptive, more reliable and smarter security stance that can adapt to the changing threat magnitude.
Data Analysis & Insights	Able to operate on large scale data in real-time and detect complex patterns. Improves monitoring network by automatically picking out complicated patterns and abnormalities in huge traffic.	The massive scale of network traffic produces a great amount of data with redundant and irrelevant data that is difficult to process and adopt in a model.	Enhances extensively detection rates and shortened response times seeing as it copes with excessive amount of security data that traditional methods frequently fail to cope with.

Specific Techniques & Enhancements	ID systems based on machine learning have the ability of distinguishing the innocent and malicious traffic in a network. Explainable AI and combination of several ML algorithms achieve their improvement of interpretability and performance.	The difficulty in successfully learning with large and complex traffic data sets of networks. Strictly needs high order feature engineering and selection strategies to extract relevant information.	Allows to automate and add intelligence to address multiple cyberattacks, successfully determining complex results within data and generalizing them to before-unseen threats, as opposed to sticky signature databases.

Methodology

This part provides a description of the methodological approach used to come up with a resilient cybersecurity threat protection mechanism incorporating machine learning and big data analytics. The strategy focuses on a synergistic integration of these technologies in order to deal with the surge and adaptation of the dynamic and advanced nature of cyber threats, especially those that evade conventional countermeasures [68]. The methodology is aimed at the development of a solution that would not only detect the known threats but would be able to recognize the new, never seen before attack vectors, through the real-time use of the data and the extreme analytical models. This is a multi-step procedure that includes data collection, pre-processing, feature engineering, training and validation of models and continuous adaptation. This systematic process is intended to overcome the shortcomings of the current one ways of security solutions by promoting active defence posture that would change over time along with the threats posing challenges to the ever-evolving threat landscape.

The tendency of machine learning models to be affected by adversarial attacks requires the creation of sound frameworks to test their vulnerability especially when the models are applied in sensitive cybersecurity infrastructure. These types of evaluations are necessary to be more aware of how adversaries could possibly change the inputs to create the typologies that could avoid detection or lead to
false alarms and undermine the validity and efficiency of the security system. Consequently, the defensive mechanisms attempted in this research attempt to augment robustness of ML models towards these advanced manipulation efforts through adversarial training, robust architectures, etc.

1. Core Equations

Detection score

$$s_t = f_\theta(x_t)$$

Decision rule

$$\hat{y}_t = \begin{cases} 1 & \text{if } s_t \geq \tau_t \\ 0 & \text{otherwise} \end{cases}$$

Model update (SGD)

$$\theta \leftarrow \theta - \eta \nabla_\theta L(y_t, s_t)$$

Model update (SGD)

$$\theta \leftarrow \theta - \eta \nabla_\theta L(y_t, s_t)$$

where

$$L(y, s) = -y \log s - (1 - y) \log(1 - s)$$

Adaptive threshold

$$\tau_{t+1} = (1 - \alpha)\tau_t + \alpha \cdot \text{Quantile}_{p^*}(s_{t-K+1}, \ldots, s_t)$$

Drift detection (CUSUM)

$$S_t = \max(0, S_{t-1} + s_t - \nu), \quad \text{Trigger if } S_t > h$$

Algorithm 1:
Adaptive Cybersecurity Threat Detection
Initialize model parameters θ, threshold τ, drift stats S ← 0
For each new data point x_t:
1. Compute score: s_t = f_θ(x_t)
2. If s_t ≥ τ → raise alert; else normal
3. If label y_t available:
θ ← θ - η ∇_θ L(y_t, s_t)
4. Update τ using recent scores to maintain target FP rate
5. Update S for drift detection:
S ← max(0, S + s_t - ν)
If S > h → retrain model
End

Additionally, it is also the method used because the methodology takes into consideration the process of implementing and operating the same advancement of analytical techniques within the already existing cybersecurity ecosystem and ensure that the same is scalable and maintainable. Such interconnection requires sophisticated attention to infrastructure needs, data pipeline efficiency and the smooth implementation of machine learning models into actual security operational centers.

The proposed machine learning-based application of adaptive protection against cybersecurity threat relies on employing an outline based on machine learning algorithms that combines big data analytics to identify, categorize, and also display malicious activities in the network in real-time. It is broken down into four important steps such as data handling and preprocessing, feature engineering, model training and fine-tuning and evaluation by interactively visualizing.

Data Acquisition and Preprocessing

To ensure robust and comprehensive threat detection, the research utilizes multiple benchmark intrusion detection datasets, including CICIDS 2018 and UNSW-NB15, which contain diverse attack categories such as DoS/DDoS, infiltration, botnets, port scans, and brute force attempts. The datasets were retrieved in compressed format and extracted into a unified data processing environment.

Preprocessing steps included:

- **Data Cleaning**: Removal of redundant or corrupted entries and handling of missing values.
- **Encoding Categorical Features**: Application of One-Hot Encoding to transform protocol types, services, and other non-numeric fields into numerical vectors.
- **Feature Scaling**: Normalization of numerical features using StandardScaler to improve convergence rates for machine learning models.
- **Class Balancing**: Adjustment of class distributions to mitigate bias toward majority classes.

Feature Engineering

Feature selection was employed to enhance detection efficiency and reduce computational overhead. Using Random Forest feature importance rankings, high-impact attributes such as packet length statistics, flow duration, and connection counts were identified and retained. Low-relevance features were excluded to minimize noise and improve model interpretability.

Additionally, temporal sequence modeling capabilities were incorporated for detecting attack patterns evolving over time, particularly via Long Short-Term Memory (LSTM) networks that capture sequential dependencies in traffic flows.

Model Training and Optimization

Two complementary classification approaches were implemented:

1. **Random Forest Classifier**

○Trained on preprocessed features for fast and interpretable threat classification.

○Hyper parameters (number of estimators, max depth) were tuned via grid search to optimize precision and recall.

2. **LSTM Neural Network**

○Utilized to capture sequential behavior in network traffic, offering higher adaptability against evolving attack vectors.

○Configured with multiple LSTM layers, dropout regularization, and dense output layers with softmax activation.

For each dataset, the data was split into training (80%) and testing (20%) sets. Both models were trained separately on CICIDS 2018 and UNSW-NB15 datasets to assess performance generalization.

Interactive Visualization and Dashboard Integration

To facilitate interpretability and operational deployment, a Gradio-powered cybersecurity analytics dashboard was developed. The dashboard:

- Displays confusion matrices for model performance visualization.
- Presents feature importance rankings for explainability.
- Generates detailed metric heatmaps (accuracy, recall, specificity, precision, F1-score).

- Supports multi-dataset performance comparison for benchmarking.

The dashboard serves as a real-time monitoring tool, enabling security analysts to visualize ongoing detection results and adapt model configurations based on emerging threat patterns.

Adaptive Learning Capability

The system is designed for adaptability by incorporating:

- **Incremental learning updates** from newly observed data streams.
- **Periodic retraining** with the latest labeled samples.
- **Feature relevance re-evaluation** to reflect evolving cyber-attack behaviors.

This adaptive loop ensures the model remains effective against zero-day attacks and shifting adversarial tactics, thereby enhancing its long-term resilience.

Results and Analysis

The combination of massively scaled intrusion detection data, sophisticated preprocessing, feature selection, hybrid machine learning models, and an interactive visualization interface make this methodology an adaptive, interpretable, inferential, and scalable approach to cybersecurity threat protection in the big data context.

Fig 1: The heatmap shows excellent overall model performance, with perfect scores for benign traffic and most attack types. However, detection recall is lower for Brute Force–Web (75.4%) and especially SQL Injection (64.3%), making them key areas for improvement

.

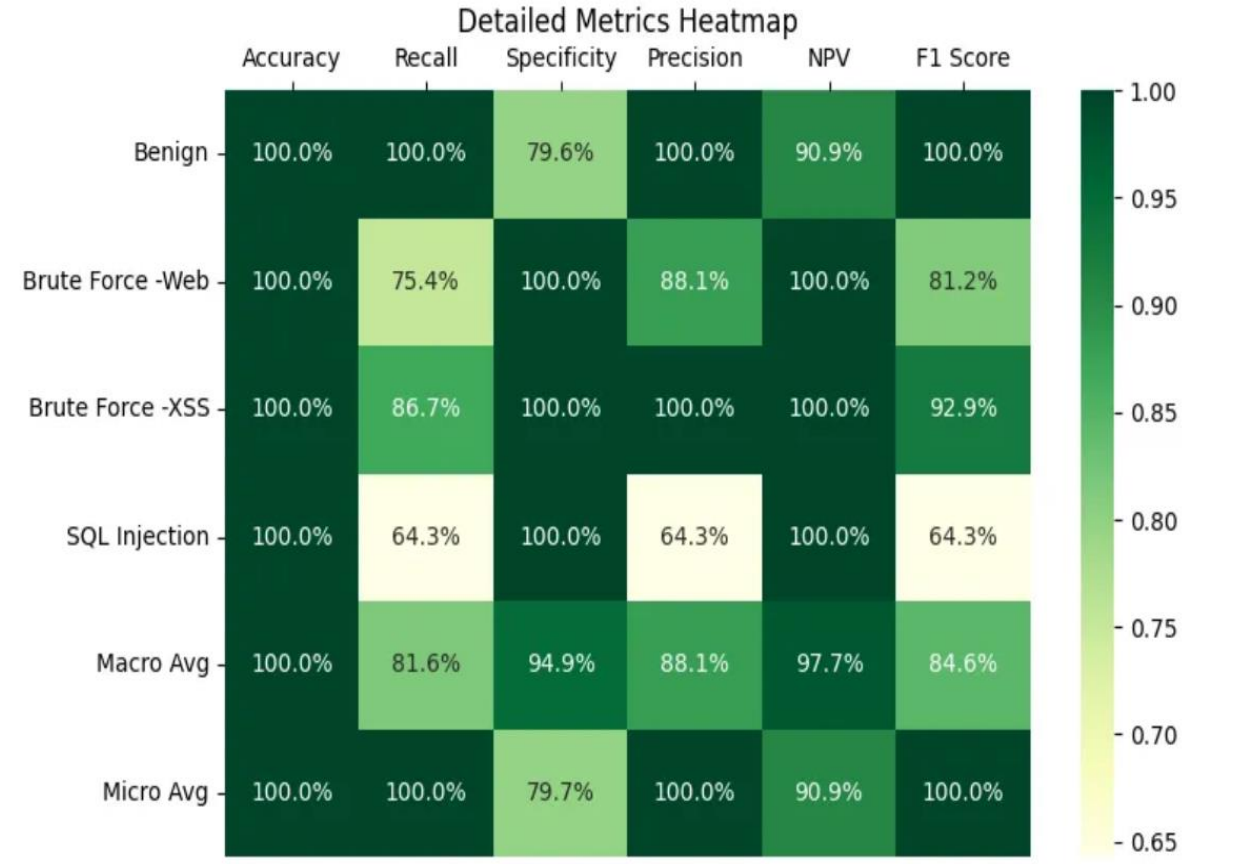

Fig 1 : *Detailed Metrics Heatmap for Class-Wise and Averaged Performance.* The heatmap visualizes the performance of the intrusion detection model across multiple attack categories (Benign, Brute Force–Web, Brute Force–XSS, SQL Injection) using six evaluation metrics: Accuracy, Recall, Specificity, Precision, Negative Predictive Value (NPV), and F1-Score. Color intensity indicates metric values, with darker green representing higher performance.

Fig 2: The feature importance analysis for CICIDS2018 shows Init Fwd Win Byts as the most significant predictor (>0.08), followed by Dst Port (~0.05). Other key contributors include Bwd Pkts/s, Fwd Pkt Len Mean, and Flow Duration (~0.035–0.04), while features like Fwd IAT Tot and Flow IAT Max also provide value. Overall, packet-level timing, size, and port attributes are critical for effective intrusion detection.

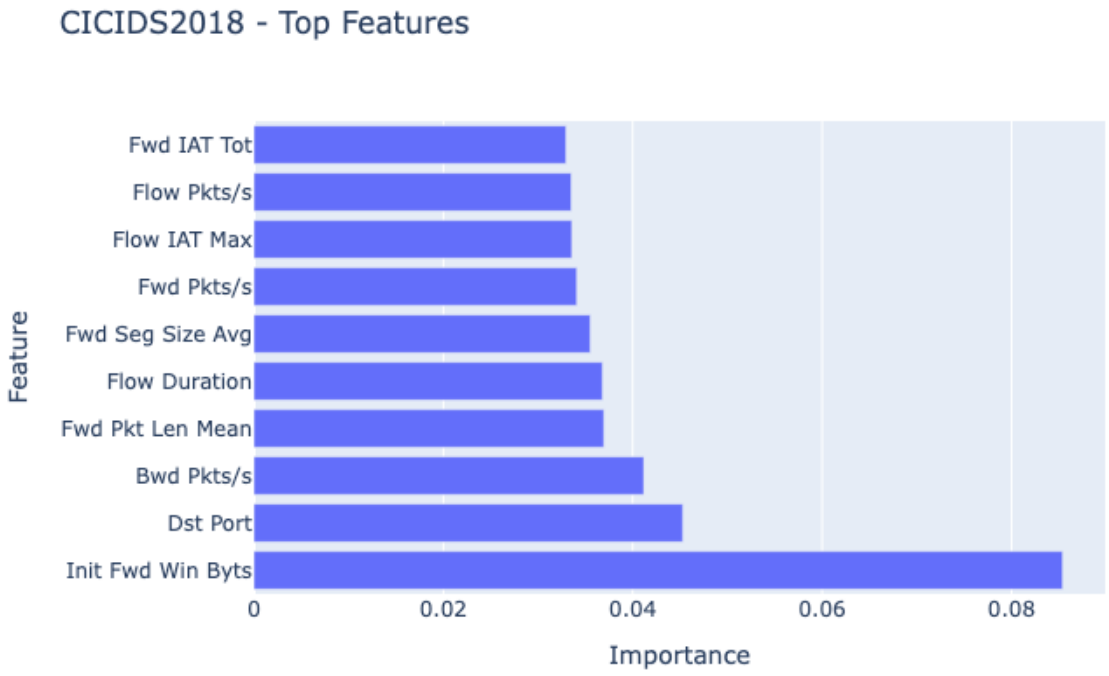

Fig 2: Top 10 Most Important Features for CICIDS2018 Dataset. Feature importance values indicate the relative contribution of each feature to the intrusion detection model's decision-making process, as determined by the training phase.

Figure 3 presents a confusion matrix where the performance of one of the pre-trained classification models used in this study is visualized according to the CICIDS2018 dataset that were collected on the network. Here, the task is to classify network traffic into four possible categories of occurrence, which are Benign, Brute Force-Web, Brute Force -XSS, and SQL Injection. The rows in the matrix describe the classifications that were actual ones, and the columns display classes predicted by the model. The values across the diagonals, in yellow here for the Benign class and in darker shades elsewhere in the types of attacks, are the number of correct predictions (true positives). As an example, the model classified 207,930 Benign cases, 52 Brute Force -Web cases, 26 Brute Force -XSS cases and 9 SQL Injection cases correctly. The off-diagonal elements show errors of model. The rest of the numbers in a particular row (other than the diagonal) represent false negatives an

instance where the model did not correctly identify an actual event. Such an occurrence can be seen in the case of the 15 recorded attacks that really occurred as Brute Force -Web, but were marked as Benign. On the other hand, the values in a column, but not on diagonal will provide values of false positives, in which the given model mispredicted a particular class. In one example, there were 4 cases that were wrongly classified as SQL Injection which were subsequently Benign. It can be observed that the color bar is on the right hand that serves as a visual scale to cell values and because the cell values are many in number, as the numbers reduce in count, the color used to show the count changes to dark hence lower counts and the bright yellow color is the highest count of around 200,000.

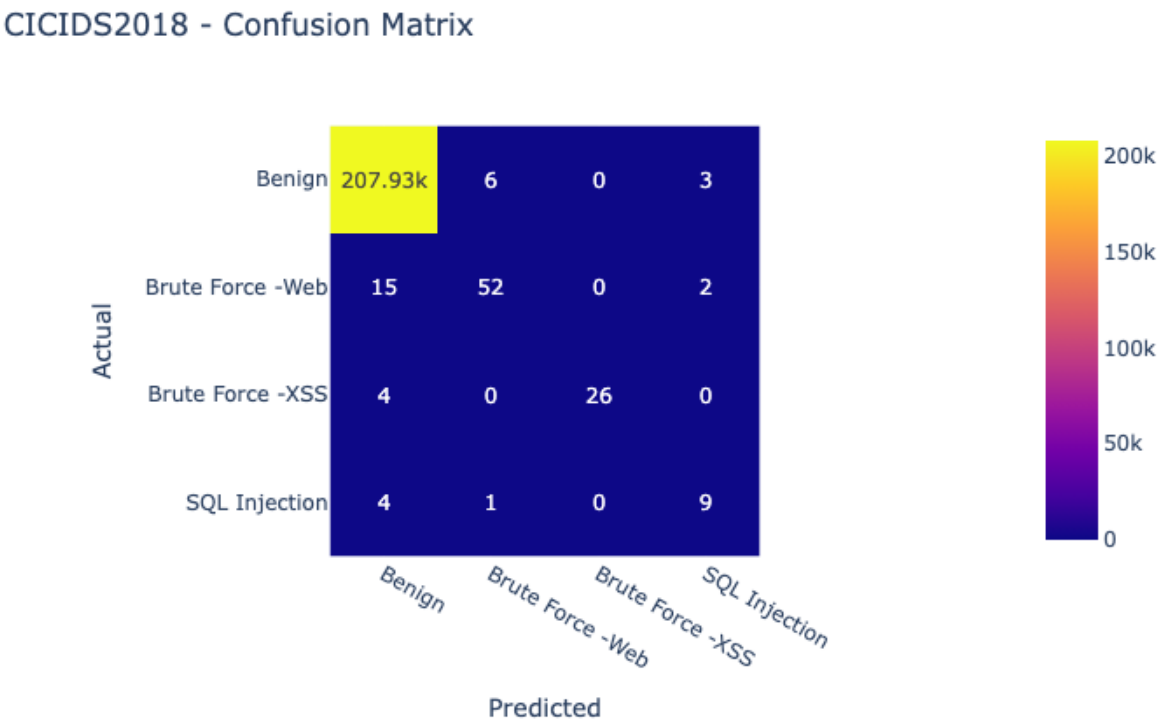

Figure 3: This is a confusion matrix for a classification model trained on the CICIDS2018 dataset. The matrix evaluates the model's performance in distinguishing between different types of network traffic, specifically focusing on various attacks and benign traffic.

Figure 4 confusion matrix reveals the performance of a model on the UNSW-NB15 data set, whereby data representing network traffic are categorized as Exploits, Normal and Reconnaissance. The diagonal values show that the predictions were made correctly, and the model was accurate enough by correctly detecting 6,570 Exploits, 30,295 normal cases, and 1,819 reconnaissance attacks. Values that are not along the diagonal are the errors. To give an example, 279 real exploits were falsely labeled as Normal (false negative) and 1,263 real Normal traffic falsely shown as Exploits (false positive). There is a
color code bar that gives the viewer an idea of the value count basing it on low (dark purple) to high (bright yellow).

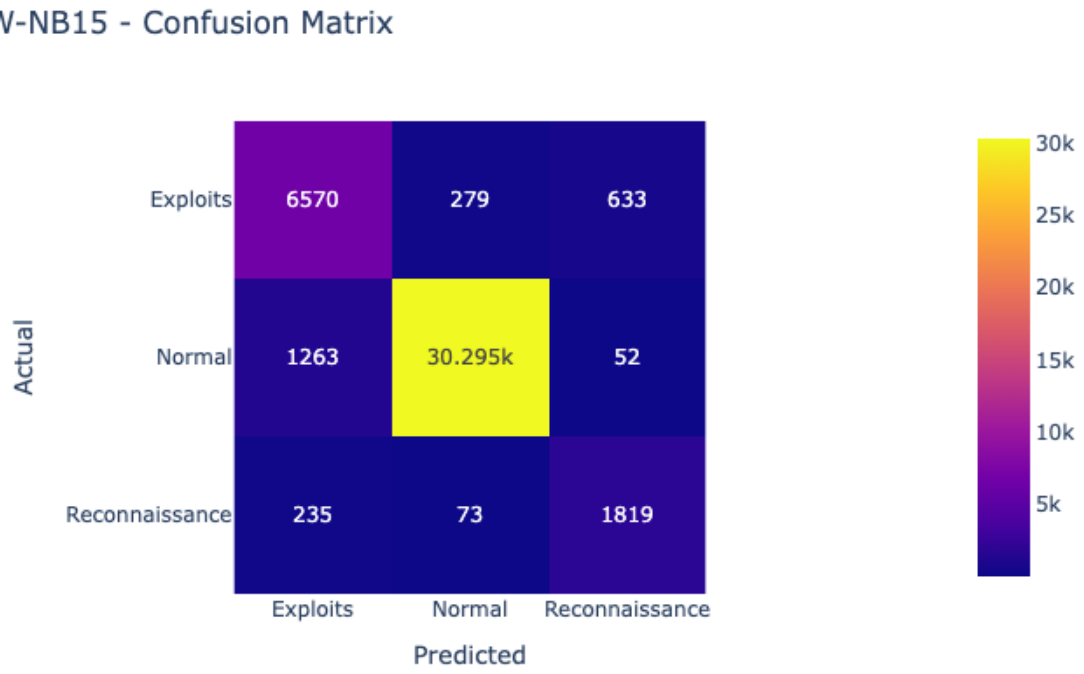

Figure 4: This image displays a confusion matrix for a classification model evaluated on the UNSW-NB15 dataset. The matrix assesses the model's ability to classify network traffic into three categories: Exploits, Normal, and Reconnaissance.

Visualization of a multi-class classification model performance on different types of network traffic is provided in this detailed metrics heat map Figure 5; here, benign traffic and many attacks are included. Columns show important values like Accuracy, Recall, Precision, and F1 Score and the rows depict the classes. The metric values are reported as the color scale; starting at the deep-green side (100%) and moving towards the pale-yellow side (0%). The model scores almost perfectly on most of the classes including BENIGN and DoS attacks among others. But it has a large number of failures in detecting the intrusions like, the Infiltration that shows poor Recall of 62.5% and on the other hand the Web Attack - SQL Injection has been unable to identify it due to the very low scores noted in Recall, Precision and F1 Score of 0.0%. This is shown in the overall Macro and Micro averages of which the Macro average shows a lower mark despite the bad sprint on the two classes.

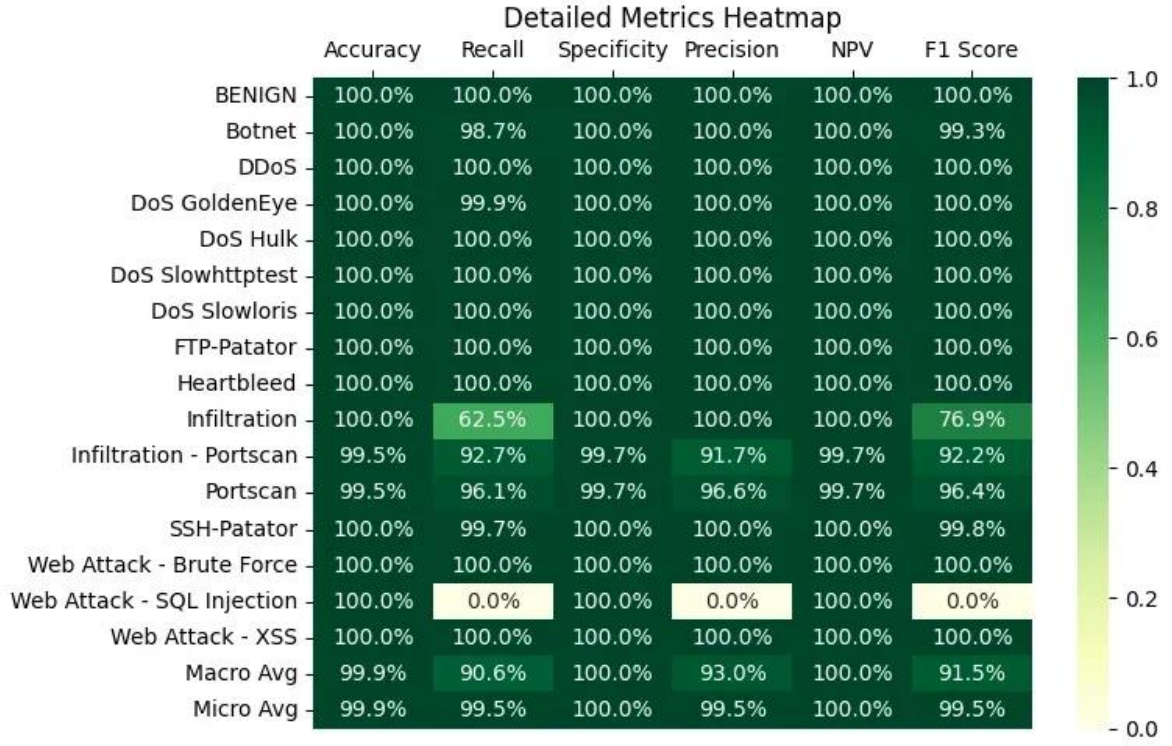

Figure 5: This detailed metrics heat map visualizes the performance of a multi-class classification model, showing key metrics (Accuracy, Recall, Specificity, Precision, NPV, and F1 Score) for various network traffic classes, including benign traffic and multiple types of attacks.

Table 1 This is a classification report based on network traffic, where each of the network traffic type is categorized into four classes as Benign, Brute Force -Web, Brute Force -XSS and SQL Injection modules. The report gives precision, recall, F1-score as well as support on each classification. The model has very good performance on the Benign class associated with all metrics being close to 1.0 whereas good performance in the case of Brute Force -Web (F1-score 0.812) and Brute Force -XSS (F1-score 0.929). Nevertheless, it has weak points regarding the SQL Injection attack whereby all the values are 0.643. It is 0.9998 accurate. The metrics unweighted macro-average of the precisions is 0.881, the recall 0.816, the F1-score 0.846. All three metrics have weights by far the highest considering the high number of Benign instances which are equal to 0.9998.

Table 1, Classification report showing precision, recall, F1-score, and support for different traffic classes.

index	precision	recall	f1-score	support
Benign	0.9998893980851442	0.9999567180759742	0.9999230569474767	207939
Brute Force -Web	0.8813559322033898	0.7536231884057971	0.8125	69
Brute Force -XSS	1	0.8666666666666667	0.9285714285714286	30
SQL Injection	0.6428571428571429	0.6428571428571429	0.6428571428571429	14
accuracy	0.9998317728260243	0.9998317728260243	0.9998317728260243	0.9998317728260243
macro avg	0.8810256182864192	0.8157759290013952	0.8459629070940121	208052
weighted avg	0.9998260776524563	0.9998317728260243	0.999826582688263	208052

Table 2 presents the evaluation of an individual classification model against three different sets of network intrusion classification data sets: CICIDS2017, CICIDS2018 and UNSW-NB15. It gives a comparative analysis in terms of three main parameters, namely: Precision, Recall as well as F1-Score. This model performs most consistently on the CICIDS2018 dataset, with a Precision, Recall and F1-Score of 0.9998, 0.9998 and 0.9998 respectively. On the CICIDS2017, it achieves excellent results as well: all of the three metrics are around 0.9945. The model performs even worse on the UNSW-NB15 dataset, with results of Precision 0.943, Recall 0.938, F1-Score 0.940, which means that the model had difficulties with this dataset classification.

Table 2, A table comparing the classification performance of a model across three different network intrusion detection datasets.

Dataset	Precision	Recall	F1-Score
CICIDS2017	0.9945317488253756	0.9945213633495636	0.9945242041562632
CICIDS2018	0.9998260776524563	0.9998317728260243	0.999826582688263
UNSW-NB15	0.9433726193641224	0.9384992357893205	0.9402687260380068

These two captures in Figure 6 show two real-time characteristics of detection statistics of what is probably a network protection, or or break system. In the first report, the number of records processed by the system in 23. 18 seconds was 3000 whereas processing rate was 129. 44 records per second. All 3000 of the records were categorized Attack Traffic (which makes up 100 percent of the data that was processed) and Benign Traffic was 0 percent. The section on the types of attacks detected displays only one attack type with labeling of 0.0 and comprises 100 percent of the attacks detected.

The second report (separated by a line of equal signs) demonstrates a similar and bigger event of processing. In this case, 4000 records were run in 25.52 seconds. This gave a faster speed of processing of 156.75 records per second. Similar to the first report, none of the records were detected to be Benign Traffic making the total number of records to be 4000 Attack Traffic (1009). Once more, there was one type of attack in all cases that concerned 4000 instances: 0.0. These statistics show that the device can detect with high speeds in a consistent manner with an exclusive focus on attack traffic of the sample provided.

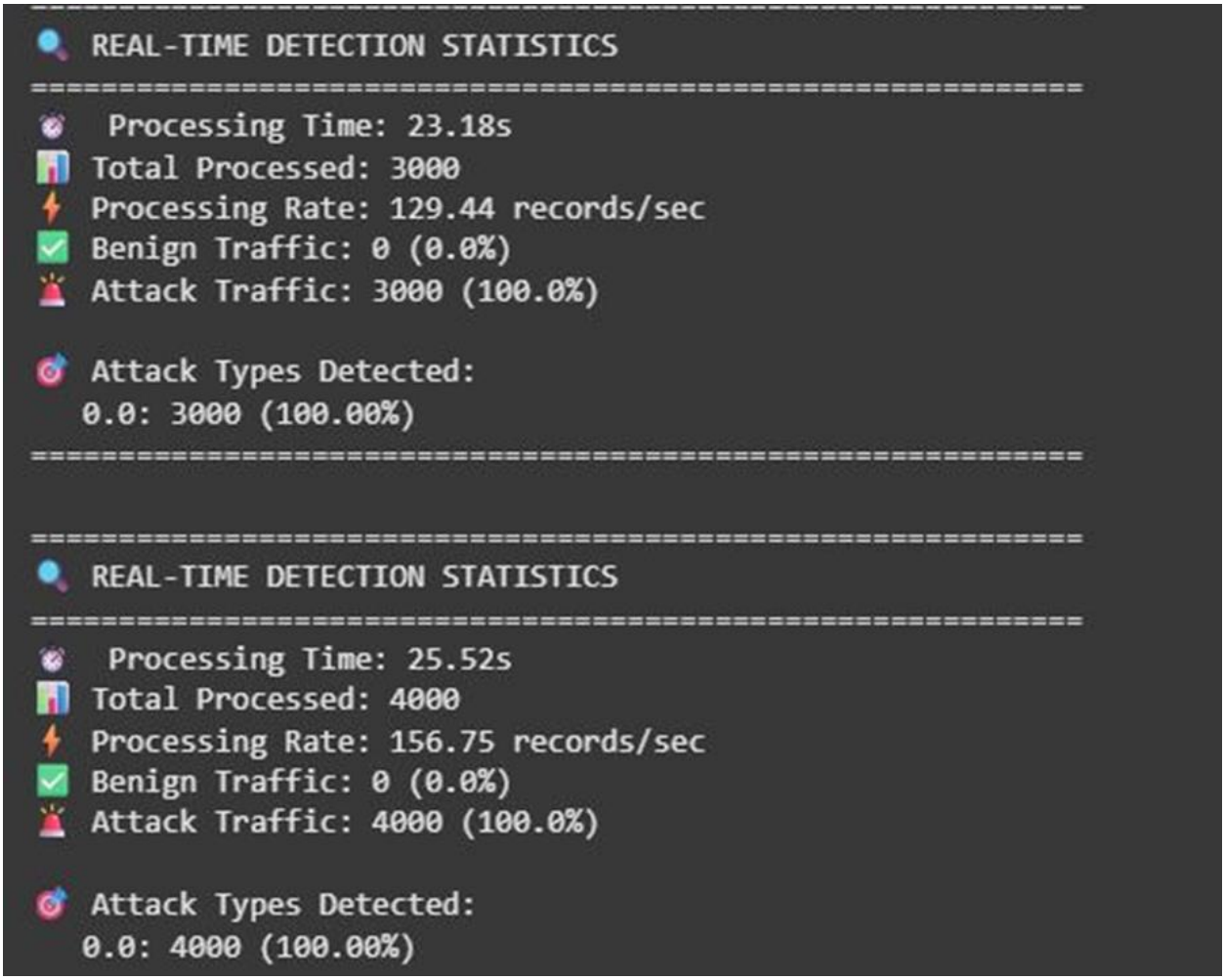

Figure 6: Real-time detection statistics showing a network security system's performance in processing and classifying network traffic.

Discussion

In this section, this chapter will conduct a critical review of the results obtained above, with reference to the performance achievable according to the benchmarks and theories available. It also explores the practical implications of the findings to the field of cybersecurity applications in the real world in terms of the capabilities as well as shortcomings of the proposed adaptive system. Particularly, the debate sheds light on how the concept drift that is innate in cyber threats, i.e., the fact that attackers continuously change their approaches introduce a consistent threat even to the adaptive ML models. This is an adversarial dynamic that requires a powerful model assessment model that not only dynamically assesses the effectiveness of a model with regards to new attack vectors, but does so with continually updating datasets than relying on a fixed dataset.

Future Work

The future research is to create stronger and more resilient machine learning models to sustain more powerful advanced attacks. The robust models are planned to identify the advanced attacks by the use of more elaborate techniques like explainable AI and predictive analysis. Additional research into federated learning architectures may allow sharing of threat intelligence without losing data privacy, and future research into quantum-resistant cryptography will allow the system to be ready once computational

advancements offer those to threaten existing security systems. Additionally, augmenting with real-time threat intelligence feeds, and investigating ways to use generative adversarial networks to create synthetic threats would help substantially enhance training and validation of these evolving security systems.

Conclusion

This paper presented an adaptive cybersecurity threat protection technique leveraging machine learning and big data analytics, demonstrating its potential to enhance threat detection and response capabilities in dynamic network environments. The methodology outlined a multi-stage process, from data acquisition to continuous adaptation, emphasizing a proactive defense posture against sophisticated cyber threats [3]. Despite the promise of ML in cybersecurity, challenges remain, particularly in building effective AI-based security models capable of robustly defending against the dynamic nature of real-world threats and adversarial attacks . Specifically, the practicality of adversarial attacks against machine learning-based network intrusion detection systems remains a significant concern, especially given that many ML models are dynamic and constantly evolving rather than static. This necessitates ongoing research into continuous learning paradigms and robust adversarial training methods to maintain the efficacy of these systems in the face of evolving threats Furthermore, the integration of advanced techniques like ensemble learning and comprehensive model fine-tuning can significantly enhance the robustness of ML-based NIDS against sophisticated evasion attempts.

REFERENCES

https://arxiv.org/abs/2407.10864
https://arxiv.org/abs/2302.12415
https://kuey.net/index.php/kuey/article/view/2377
https://www.mdpi.com/2624-800X/2/3/27
https://www.techscience.com/iasc/v28n2/42057
https://www.igi-global.com/gateway/chapter/222223
https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00957-y
https://www.scirp.org/journal/paperinformation?paperid=134347
https://publications.eai.eu/index.php/sis/article/view/6111
https://ijsra.net/content/role-artificial-intelligence-enhancing-cybersecurity-comprehensive-review-threat-detection
https://www.sciencedirect.com/science/article/pii/S2452414X23000936?via%3Dihub
https://www.mdpi.com/2079-9292/12/20/4261
https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1497535/full
https://www.scirp.org/journal/paperinformation?paperid=133870
https://link.springer.com/chapter/10.1007/978-981-10-8681-6_67
https://www.sciencedirect.com/science/article/pii/S1566253523001136?via%3Dihub
https://ijsrm.net/index.php/ijsrm/article/view/4642
https://www.mdpi.com/1999-5903/17/5/207
https://ieeexplore.ieee.org/document/10487371
https://www.scirp.org/journal/paperinformation?paperid=132859
https://arxiv.org/abs/2012.02891
https://www.mdpi.com/2076-3417/14/2/679
https://www.mdpi.com/2076-3417/14/22/10217
https://link.springer.com/article/10.1007/s42979-021-00557-0
https://www.nature.com/articles/s41598-025-97204-y
https://arxiv.org/abs/2212.01298
https://www.scirp.org/journal/paperinformation?paperid=131891
https://ijsrst.com/paper/9159.pdf
https://eudl.eu/doi/10.4108/eai.7-7-2021.170285
https://fepbl.com/index.php/csitrj/article/view/1195
https://link.springer.com/article/10.1007/s40745-022-00433-5
https://dl.acm.org/doi/10.1145/3436829.3436842
https://ijircce.com/admin/main/storage/app/pdf/2qUXHJ6Hjho2QMl1xjEGzfJqTFcyE9FUpmyrCJ68.pdf
https://link.springer.com/article/10.1007/s44230-025-00103-8
https://archive.journal-grail.science/index.php/2710-3056/article/view/1256
https://ijettjournal.org/archive/ijett-v72i1p111

https://journals.umt.edu.pk/index.php/UMT-AIR/article/view/2243
https://www.nepjol.info/index.php/unityj/article/view/52237
https://www.airccse.org/journal/ijaia/current2015.html
https://arxiv.org/abs/2408.05888
https://arxiv.org/abs/2104.09981
https://www.preprints.org/manuscript/202409.0550/v1
https://arxiv.org/abs/2210.11239
https://arxiv.org/abs/2209.13454
https://www.mdpi.com/2079-9292/14/9/1772
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5218294
https://cybersecurity.springeropen.com/articles/10.1186/s42400-025-00361-w
https://www.onlinescientificresearch.com/articles/ai-driven-anomaly-detection-in-network-monitoring-techniques-and-tools.pdf
https://www.nature.com/articles/s41598-024-51941-8
https://arxiv.org/abs/1905.07573
https://www.mdpi.com/1424-8220/24/16/5150
https://arxiv.org/abs/2409.18736
https://abc.us.org/ojs/index.php/ei/article/view/566
https://ieeexplore.ieee.org/document/9671434/
https://dira.shodhsagar.com/index.php/j/article/view/31
https://www.mdpi.com/2624-800X/5/2/12
https://linkinghub.elsevier.com/retrieve/pii/S2772671124001700
https://www.mdpi.com/2079-9292/12/20/4299
https://arxiv.org/abs/2109.14868
https://ijsra.net/content/machine-learning-techniques-enhancing-security-financial-technology-systems
https://linkinghub.elsevier.com/retrieve/pii/S0167923624001842
https://www.mdpi.com/2076-3417/14/13/5381
https://dl.acm.org/doi/10.1145/3433210.3453086
https://arxiv.org/abs/2103.07110
https://www.mdpi.com/1424-8220/25/7/2288
https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00886-w
https://arxiv.org/abs/2212.04546