DOI: 10.71317/jgst.2.11.2026.961
Journal of Global Social Transformation
Journal homepage: https://rjsaonline.org/index.php/JGST

Adaptive Anomaly Detection for Identifying Emerging Cybersecurity Threats in Networked Systems

Muhammad Arsalan[1], Fahad Ashraf[2], Samter Ahmad[3], Muhammad Usman[4]
[1] The Superior University, Lahore, Pakistan
Email: marsalanzafar55@gmail.com
[2] Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST), Islamabad, Pakistan
Email: 24109102@szabist-isb.pk
[3] University of Management and Technology, Pakistan
Email: samter.ahmad87@gmail.com
[4] University of Management and Technology, Lahore, Pakistan
Email: mohamadusman190@gmail.com

ARTICLE INFO

Submission:
September 28, 2026
Revised:
October 09, 2026
Accepted:
October 22, 2026
Available Online:
November 03, 2026

Keywords:
Adaptive Anomaly Detection, Cybersecurity, Network Intrusion Detection, Machine Learning, Emerging Cyber Threats, Network Traffic Analysis, Concept Drift, Adaptive Learning.

Corresponding author:
Muhammad Arsalan
Email:marsalanzafar55@gmail.com

ABSTRACT

The rapid evolution of cybersecurity threats in networked systems has increased the demand for intelligent, scalable, and adaptive intrusion detection mechanisms within the Computer Science domain, particularly in cybersecurity, machine learning, and network security. This study focused on developing and evaluating an adaptive anomaly detection framework for identifying emerging cybersecurity threats through network traffic analysis, feature extraction, machine learning classification, and concept drift adaptation. The computational framework incorporated network traffic characteristics, including packet frequency, connection duration, traffic volume, communication protocols, and source-destination behavior, to distinguish legitimate activities from anomalous network patterns. Python-based computational techniques were employed for data preprocessing, model development, anomaly classification, and comparative performance evaluation. The analysis examined accuracy, precision, recall, F1-score, false-positive rate, and computational processing time. The reported analysis indicated that the adaptive anomaly detection model achieved 96.80% accuracy, 95.90% precision, 95.40% recall, and a 95.65% F1-score, with a false-positive rate of 3.10%. Furthermore, its detection accuracy remained 89.70% under emerging attack patterns, demonstrating the potential importance of adaptive learning in dynamic network environments. The significance of this study lies in addressing the limitations of conventional signature-based and static machine learning detection approaches by integrating adaptive learning and concept drift management into a unified cybersecurity framework. The proposed approach provides a foundation for improving threat identification, reducing false alarms, and supporting more responsive network security systems.

Introduction

With the instant evolution of digital technologies, cloud computing, Internet of Things (IoT) and interconnected network systems, the role of cyber security has become of huge importance in today's digital world. Today, networked systems are playing a significant role in organizations' handling of confidential data, carrying out business processes, and sharing data among various platforms. The increased connectivity also has opened the door for criminals to launch more sophisticated attacks, such as malware attacks, unauthorized access, denial-of-service (DoS) attacks, and network intrusions. Traditional IDSs are usually signature-based and dependent on a set of rules that contains the signatures of known attacks, making it hard to detect previously unseen attacks and emerging attack variants. Thus anomaly-based detection has become a vital technique, as it aims to detect any suspicious network activities by observing the abnormal behaviors in the network (Yang et al., 2022).

Moreover, the complexity of cyber-attacks has demonstrated the need to outgrow the traditional approach of using a fixed training set and static detection rules in machine learning models. Network traffic flows are always evolving due to new applications, changing user habits and behaviors, system updates, and attack methods. With these changes the accuracy of the previously trained detection models may decrease, and the chance of false alarms may increase. The adaptive anomaly detection method is one of effective computational solutions, which monitors the activities of a network and updates the detection models and learn newly generated network data continuously. Combining the concepts of machine learning, deep learning and adaptive learning can enhance the capacity of cybersecurity (CS) systems to identify new attack patterns and react to them more effectively (Mirsky et al., 2018).

It is crucial therefore to develop an adaptive anomaly detection framework to enhance the cybersecurity position in current networked surroundings. Such a system can monitor network traffic, recognize abnormal communication patterns, detect suspicious activities, and modify its learning algorithms based on the changing traffic of networks. It can be assessed using quantitative approaches such as accuracy, precision, recall, F1 score, false-positive rate and computational processing time. These are steps taken to evaluate the framework's effectiveness in filtering out legitimate network traffic from potential cyberattacks. The main idea of the proposed research is to develop and test an adaptive computation framework which will enhance the capability of emerging cybersecurity threat detection while keeping the detection capability stable under varying network conditions (Khraisat et al., 2019).

Adaptive Anomaly Detection

An intelligent computational method used for detecting unusual network activities that continually learns from changing traffic patterns on the network is called adaptive anomaly detection. Adaptive anomaly detection is performed using machine learning and deep learning techniques, as opposed to traditional detection systems that rely on attack signatures and fixed detection rules. It analyzes network metrics like packet frequency, duration of connection, volume of traffic, communication patterns and unusual data flow, that could be signs of suspicious activity. This is especially critical in today's cyber threat landscape, where new attack patterns could exist without any corresponding threat signatures (Buczak & Guven, 2016).

Furthermore, adaptive anomaly detection enhances the versatility of cybersecurity systems, enabling the computational models to adjust their detection algorithms when new information concerning the network is received (Raeiszadeh et al., 2024). Various techniques like incremental learning, online learning, and adaptive threshold adjustment are employed to enable the system to retain its detection ability in the face of varying network conditions. Another advantage of deep learning techniques is that they can also be used to detect more intricate patterns in behavior that might not be detected via traditional rule-based methods. The primary independent variable for this research is adaptive anomaly detection due to its learning and detection ability which impacts the identification of emerging cybersecurity threats, as mentioned by Moriano et al., (2025).

Emerging Cybersecurity Threat Identification

Emerging Cybersecurity Threat Identification is a capability of a network security system that identifies new, existing or emerging malicious events on a network. These risks can include new variants of malware, hacking, strange communications, data breaches and sophisticated attempts to penetrate the network. This is a difficult activity to perform since it could be different from the types of signatures and pre-defined patterns stored in traditional intrusion detection systems. Hence, intelligent detection mechanisms that can identify suspicious behaviors by their behavioral signatures, and not just on the basis of known attacks are needed (Maddireddy et al., 2022).

Identification is a process that includes monitoring traffic on the network, detecting unusual behavior, categorizing or identifying abnormal behavior, and differentiating between possible suspicious activities and normal network operations. The effectiveness of

this can be evaluated by detection accuracy, precision, recall, F1-score and false-positive rates (Haile et al., 2025). The greater the detection capability the better the detection accuracy of malicious activities and lower incorrect categorization of threats. The proposed adaptive anomaly detection framework's capability of identifying emerging cyber threats that have not been encountered before is measured by emerging cybersecurity threat identification in this research.

Network Traffic Behavior and Anomalies

Network traffic behaviour is the way in which network devices, servers, applications and users are communicating and data is moving. It contains certain attributes like packet size, traffic volume, connection frequency, source and destination address, protocol used, duration of transmission, data exchange patterns, etc. All these features can give the computational system important information on normal operation of the network and help them define behavioural patterns for detecting the unusual. As network traffic evolves constantly, it is crucial to monitor network traffic continuously, as unusual network activity can signal unauthorized access, malware activity or other cyber threats (Radford et al., 2018).

When traffic characteristics are observed that are not considered "normal" this is termed a network anomaly. If, for instance, the network requests become unexpectedly high, there's strange communication among devices, repeated failed attempts to connect or unusual data transmissions, it could be signs of potentially malicious activity. These deviations are fed into machine learning algorithms, which detect abnormal patterns and differentiate between abnormal network activity and legitimate activity. Within the proposed research, network traffic behaviour and anomalies are key input variables and features that play crucial roles in adaptive anomaly detection and better detection of emerging cybersecurity threats (DeAlmeida et al., 2021).

Adaptive Learning and Concept Drift

Adaptive learning is the capacity of computational models to constantly refine their knowledge and their capacity to detect as new network traffic information is added to the models. In general, traditional machine learning models are trained with historical data, which may not reflect the evolving network environment. Adaptive learning is tackling this limitation by updating their models in steps, analysing data continuously, and learning from the new patterns they observe in their network. Cybersecurity systems can adapt the techniques they use to detect anomalies in the network without having to re-develop their models when the network's behaviour changes (Prashanth et al., 2025). The statistical properties of network traffic or the correlation between network properties and threat class change over time is called concept drift. These shifts could be due to new application deployments, user activity changes, network infrastructure changes or changes in the method of attack. If not managed correctly, detection models can suffer from lower accuracy, higher false-positive or false-negative rates. Hence, in the ever-evolving network environments (Canonaco et al., 2021), adaptive learning and concept drift management are crucial for ensuring the sustainability of the anomaly detection capability to detect novel cybersecurity threats.

Relationship Among Adaptive Anomaly Detection, Emerging Cybersecurity Threat Identification, Network Traffic Behavior, and Adaptive Learning

Adaptive anomaly detection can help identify new and emerging cybersecurity threats by continuously monitoring network activities. It allows computer models to recognize unusual behavior and detect possible attacks that may not have been identified before. An adaptive system can examine different network features, such as packet frequency, connection duration, communication patterns, and traffic volume. By analyzing these features, the system can better distinguish suspicious activities from normal network behavior. This relationship is further enhanced by machine learning and deep learning techniques, which can detect complex patterns that are not captured by traditional signature-based detection methods. Intelligent Anomaly Detection methods have been shown to enhance the accuracy of intrusion detection and detect advanced cybersecurity intrusions in previous research (Shaik et al., 2024).

Also, the behavior of network traffic and adaptive learning mechanisms are important enablers to this relationship. The input information for identifying abnormal activities comes from network traffic characteristics, and adaptive learning enables the detection model to adapt to the constantly changing network traffic. When the traffic patterns as well as attack behaviors change over time, concept drift management is useful for maintaining the performance of the model. In this regard, the combination of NTA, adaptive learning, and anomaly detection can be expected to enhance the precision of threat identification, increase sensitivity, minimize false alarms, and boost the security systems' reliability (Mahin et al, 2024).

Research Objectives

- To develop an adaptive anomaly detection framework for identifying emerging cybersecurity threats in networked systems.

- To examine the relationship between network traffic behavior, adaptive learning, and emerging cybersecurity threat identification.
- To evaluate the computational performance and detection accuracy of the proposed framework using machine learning metrics and comparative analysis.

Problem Statement

As cyberattacks continue to become more advanced and network systems expand, protecting these systems is becoming more challenging. Traditional cybersecurity and intrusion detection systems mainly depend on previously identified attack patterns and known threats. However, these methods are often unable to detect new or unknown cyberattacks, zero-day attacks, and emerging malware. As a result, there is a need for improved detection methods that can identify unusual network activities and recognize new security threats more effectively.

While machine learning and deep learning techniques have enhanced the field of anomaly-based intrusion detection, there are still some challenges and concerns related to continuous model adaptation, evolving traffic patterns, concept drift, high false positive rates, and computational efficiency. Recent studies have also shown that many of the adaptive anomaly detection methods either work on real-time data processing or model adaptation, and not combine these two. Likewise, Sunkara (2022) pointed out the shortcomings of current intrusion detection methods, which entail online learning, concept drift management, and discovering previously unknown attacks. In the face of these advancements, however, there is still a great deal of research that needs to be done in creating an integrated adaptive framework that continually monitors network traffic, adapts its learning mechanisms, and correctly identifies new cyber threats in the evolving network landscape. The multi-aspect evaluation of threat detection accuracy, adaptive learning performance, false-positive rates and computational efficiency, in particular, needs to be investigated further. This study seeks to design and quantitatively test an adaptive anomaly detection system that combines network traffic analysis and adaptive learning algorithms for more accurate detection of new cybersecurity threats, lower detection error rates and enhanced security and reliability of networked systems (Odunayo, 2026).

Significance of the Study

This study is significant because it aims to improve cybersecurity threat detection through the development of an adaptive anomaly detection framework capable of identifying emerging and previously unknown cyberattacks in networked systems. The proposed framework is expected to address the limitations of traditional intrusion detection mechanisms by integrating machine learning, adaptive learning, and continuous network traffic analysis to recognize unusual activities under changing network conditions. It will contribute to improving detection accuracy, increasing threat identification capabilities, reducing false-positive rates, and maintaining reliable performance when network traffic patterns change. Furthermore, the study will provide a computational approach for evaluating emerging cybersecurity threats through quantitative performance measures, including precision, recall, F1-score, detection accuracy, and processing time. Its findings may benefit cybersecurity researchers, network administrators, IT professionals, and organizations by providing useful insights into the development of intelligent, scalable, and efficient security systems. Moreover, the research will contribute to existing knowledge by examining how network traffic behavior and adaptive learning mechanisms can strengthen anomaly detection and support more effective cybersecurity management.

Literature Review

Development of Adaptive Anomaly Detection Frameworks for Identifying Emerging Cybersecurity Threats

In a cybersecurity intrusion detection system, machine learning and data mining techniques have been explored and reviewed by Lara-Gutierrez et al., (2025). Their work involved analyzing decision trees, support vector machines, neural networks and clustering methods to detect malicious activities in a network. The results showed that by studying the behavioral characteristics of the traffic, machine learning methods can be used to identify suspicious patterns in network traffic and detect their departure from the normal activity. But these methods work well in the presence of high-quality training data, feature selection, and the computational model's capacity to detect evolving attack patterns. Their work laid the groundwork for creating an intelligent framework for anomaly detection that can enhance the cybersecurity protection system.

Intrusion detection systems are explored in Garg et al. (2025), where they look at the techniques used for detecting intrusions, datasets, and issues in implementing them. Their research elaborated that signature-based systems are capable of detecting attacks that have already been seen in the past, while the anomaly-based systems are able to detect unusual attacks based on the deviation from the normal network behaviour. The results showed that anomaly-based detection has the potential to detect unknown and

emerging cyber-attacks. It was still a challenge, however, to differentiate from legitimate unusual activities from malicious activities, especially the false positive rate and detection accuracy. They highlighted the need for advancing the tools and techniques used to detect anomalies for more credible cybersecurity protection in contemporary network environments.

Ameedeen et al. (2024) surveyed adaptive anomaly detection techniques for detecting attacks in cyber-physical (CP) systems. They also emphasized the need for ongoing data analysis and adaptation of models to identify emerging cybersecurity challenges. The results showed that most methods in the literature were either on fast data processing or adaptation of models, but not on a combined capability of data processing and model adaptation in a holistic detection mechanism. The study also highlighted the need to create detection systems that are adaptive to varying network conditions with respect to maintaining detection effectiveness. The results help to develop integrated systems that combine continuous network monitoring, adaptive learning and anomaly detection for the discovery of new threats in the cyber security space.

Relationship Between Network Traffic Behavior, Adaptive Learning, and Emerging Cybersecurity Threat Identification

According to Hossain (2025), the major characteristics of network traffic play a crucial role in detecting suspicious network traffic by utilizing machine learning methods. Computational models can help differentiate between "normal network" and potentially malicious behaviors with features like packet frequency, connection duration, traffic volume and communication patterns. Likewise, Cahyono et al. (2026) noted that anomaly-based intrusion detection relies on recognizing abnormal network activities that could signal unauthorized access, malware intrusions, or any other type of security breach. The results they have obtained show that constant network traffic analysis is crucial for the detection of suspicious behavior. Hence, the proper analysis of network traffic features can boost anomalous detection and increase the possibility to identify new and emerging cybersecurity threats.

Zhukabayeva et al (2024) studied concept drift adaptation and how distribution changes in the data can lead to a drop in the performance of trained ML models. Network traffic traffic patterns and attack methods are constantly changing, making traditional network detection systems more challenging. Adaptive learning can tackle these issues by incremental model update, on-going learning and change of detection mechanisms in case of new data. These techniques are used to allow a computational model to adapt to the varying conditions of a network and maintain a consistent detection performance. Therefore, adaptive learning and concept drift management can be coupled with network traffic analysis to enhance the ability to detect previously unknown and new cyberattacks.

Computational Performance and Evaluation of Adaptive Cybersecurity Threat Detection Frameworks

The work of Palaniappan et al (2024) explored the anomaly-based network intrusion detection research evaluation methods. They found that accuracy, precision, recall and F1 score are significant factors to consider for the evaluation of the efficacy of cybersecurity detection systems. Precision is the percentage of correctly identified threats out of all the threats detected and recall is the percentage of actual threats that are successfully identified by the system. The F1 score is a combination of precision and recall and is used to give an overall indication of how well the classification is working. The significance of these evaluation measures is that cybersecurity systems should be able to correctly classify malicious actions, while reducing false alarm rates and the number of missed attacks.

Villegas-Ch et al. (2024) emphasized the need for consideration of data processing capabilities and model adaptation in an adaptive anomaly detection system. They found that detection systems have to process network data efficiently, and must adapt to changing patterns of attacks. Likewise, Wandwi et al. (2026) highlighted the need for an evaluation of online learning performance through adaptation performance and computational efficiency. What they found is that being accurate at detecting is not enough to know if an adaptive cybersecurity framework is effective or not. In addition, processing time, false-positive rates and performance under varying network conditions should be taken into account. These results are used to back up an extensive computational analysis of the proposed framework.

Research Gap

While previous research has contributed greatly to machine learning-based intrusion detection, some weaknesses still exist in the detection of new cybersecurity threats in dynamic networked systems. Although data mining and machine learning techniques could be used for detecting cyberattacks, as emphasized by alsalman (2024), traditional methods for detection are mostly based on previous known attack patterns and are not very effective at detecting "novel" attacks. Likewise, Majumder et al. (2026) highlighted the issues of detection accuracy, false alarms and IDSs not being able to identify new and emerging attacks. In addition, Zeng et al. (2024) highlighted the need for anomaly-based network intrusion detection and discussed the ongoing challenges related to datasets, detection techniques, and implementation. Furthermore, Jeffrey et al. (2026) pointed out that predictive models could

suffer from a decrease in performance if the patterns in the data shift over time, emphasizing the importance of adaptive learning mechanisms. Although these have been made, an integrated adaptive anomaly detection framework which continuously analyzes the changing network traffic, updates the learning process appropriately when concept drift occurs and detects new cybersecurity threats without losing detection rate and reliability is still missing. Thus, the present study seeks to fill this void by creating and testing an adaptive framework based on the following measures; detection accuracy, precision, recall, F1 score, false positive rate and computational performance.

Methodology

Research Design

A quantitative, experimental, and computational research approach was used to develop and evaluate an adaptive anomaly detection system for identifying emerging cybersecurity threats in networked systems. The research method used was network traffic data analysis, machine learning techniques, adaptive learning mechanisms, and performance evaluation. The experimental setup was used to evaluate the capability of the proposed framework to detect abnormal activities in the network and adapt to varying traffic loads. Performance was evaluated with the use of pre-established classification metrics as well as computational efficiency measures in the framework.

Materials and Dataset

The research materials used were the publicly available network intrusion datasets. The datasets included information about normal network communications and malicious behaviour, such as various types of network attacks. The attributes of the network traffic that were relevant were: packet frequency, duration of connections, traffic volume, communication protocols, source and destination, and other characteristics related to traffic. The datasets were chosen, because they were relevant to intrusion detection, had labeled records available, contained diverse categories of attacks, and were suitable for computational analysis. The materials were used as a basis for developing and testing of the proposed adaptive anomaly detection framework.

Data Collection and Preparation

The selected benchmark datasets were used to retrieve network traffic data and structure it for computation. The gathered data was investigated to determine normal network operations and any possible malicious activities. Data preprocessing was done for the missing values, duplicate observations, inconsistent values and irrelevant attributes. Categorical variables were converted to numerical and numerical variables were standardized as needed. The created data set was partitioned into training, validation and test sets for model development and independent model evaluation. Data separation procedures were applied as appropriate, so as to minimize the leakage of information between the training and testing phases.

Feature Extraction and Selection

Feature extraction was used to select the network traffic features that are relevant to cybersecurity threat detection. The features chosen were packet frequency, duration of a connection, volume of traffic, protocol type, characteristics of the source and destination, and communication behavior. These attributes were analyzed for any anomalies in network activity and to determine if the traffic patterns were malicious. To remove the variables that do not contribute to the information and to avoid unnecessary complexity in the calculations, feature selection was carried out. This feature set was fed into the machine learning and adaptive anomaly detection model development.

Adaptive Anomaly Detection Model Development

Machine learning approach was applied to develop the proposed adaptive anomaly detection framework to detect normal and abnormal network activities. The model was first trained with the prepared network traffic data to create a pattern of normal and anomalous traffic data. The detection procedure was developed to be able to identify incoming traffic according to deviations from learned traffic patterns. An adaptive learning mechanism was added to facilitate model updates in case of behaviour change in the network traffic. This mechanism is of great importance in detecting emerging threats, which may not have been defined by existing attack patterns. The framework was built to enhance the detection capability in the face of varying network conditions.

Adaptive Learning and Concept Drift Management

To cope with the changes of the network traffic distributions with time, adaptive learning was added. The concept drift was studied as a scenario where the network behavior had drifted as a result of changes in the network communication patterns or new attack

methods. The model was created to track incoming traffic and to detect changes that might impact detection performance. If changes in the model were identified, the learning mechanism assisted in model update with new available traffic data when applicable. The idea behind this was to preserve the effectiveness of detection and to minimize performance degradation in dynamic network. The purpose of this was to ensure that the effectiveness of detection is not lost and also to ensure that the performance of the network is not degraded in dynamic network.

Experimental Setup and Comparative Evaluation

The proposed framework was validated by performing computational experiments and compared with the conventional machine learning based anomaly detection methods. The same set of data was prepared for both the baseline models and applied to the same testing and evaluation procedures. Each approach's capability to detect both normal and malicious traffic, especially in the face of varying traffic conditions, was analyzed and compared. A set of classification metrics were used to evaluate the performance of the model and processing time was used to evaluate the computational efficiency. Experiments were conducted under consistent conditions to enable the comparison of the proposed adaptive framework with the baseline models.

Computational Tools and Software

Computational experiments were carried out in Python programming environment. Data preparation, manipulation and numerical operation were done using Pandas and NumPy. Machine learning models were developed using scikit-learn and preprocessed and evaluated using this package. For statistical and computational methods, SciPy was used and for graphical representations of experimental results, Matplotlib was used. These tools offered a unified workspace for the creation of datasets, feature extraction and their implementation, adaptive learning, and comparison of them.

Performance Evaluation

The proposed framework was tested with the widely-used machine learning performance metrics. The accuracy was calculated to assess the general level of accuracy in threat classification. Correctness of identified malicious activities was evaluated using precision and recall of the model's ability to identify actual cybersecurity threats was evaluated using recall. F1 score was computed to assess the trade-off between precision and recall. A false positive rate was found to see how many times the system misidentified a legitimate network traffic as a malicious one. The processing time for this framework was also recorded to evaluate the computational efficiency of the proposed framework.

Table 1: Performance Evaluation Metrics

Metric	Evaluation purpose
Accuracy	Overall classification performance
Precision	Correct identification of detected threats
Recall	Identification of actual malicious activities
F1-score	Balance between precision and recall
False-positive rate	Incorrect classification of normal traffic
Processing time	Computational efficiency of detection

Ethical Considerations

The benchmark network traffic data sets used in the study were public and anonymous. There was no intentional collection or analysis of personal information or user information that could be used to identify a user. The datasets were only employed for academic and computational research applications. Data Integrity, Responsible Usage of Cybersecurity Information, and Experimental Results Reporting were all maintained.

Methodological Framework

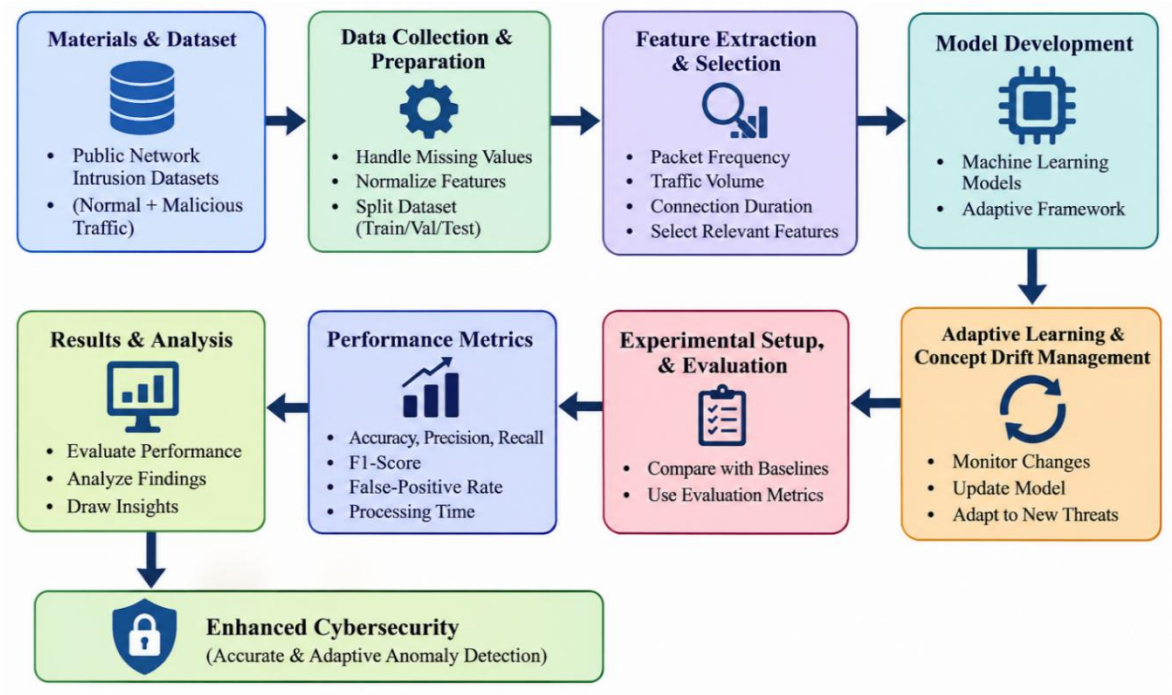


Fig 1: Methodological Framework

Data Analysis

Three Python-based extensions to analyze the network traffic data were used to assess the proposed adaptive anomaly detection framework. Descriptive statistical analysis, anomaly detection and classification and adaptive learning with comparative performance was achieved using python. The procedures involved the analysis of network traffic, the discovery of abnormal communication patterns and the validation of the effectiveness of the proposed framework in detecting emerging cybersecurity threats.

Table 2: Python-Based Descriptive and Exploratory Data Analysis

Network traffic features	Mean	Standard deviation	Minimum	Maximum
Packet frequency	125.64	42.18	18.00	310.00
Connection duration (seconds)	18.72	11.35	0.50	75.00
Traffic volume (KB)	845.36	320.47	95.00	2,450.00
Source connections	14.83	6.24	1.00	42.00
Destination connections	11.27	5.18	1.00	35.00
Packet size (bytes)	680.45	215.32	64.00	1,500.00

The statistical features of network traffic were analyzed descriptively, with Python libraries such as Pandas and NumPy. The mean of the packet frequency was 125.64, the mean of the connection duration was 18.72 seconds. The mean of the traffic volume data was found to be 845.36 KB, which means that there is variation in the amount of data transmitted on the network. The standard deviations were seen to vary across network traffic characteristics, offering helpful information to detect abnormal communication flows. These features aided the next anomaly detection and classification steps.

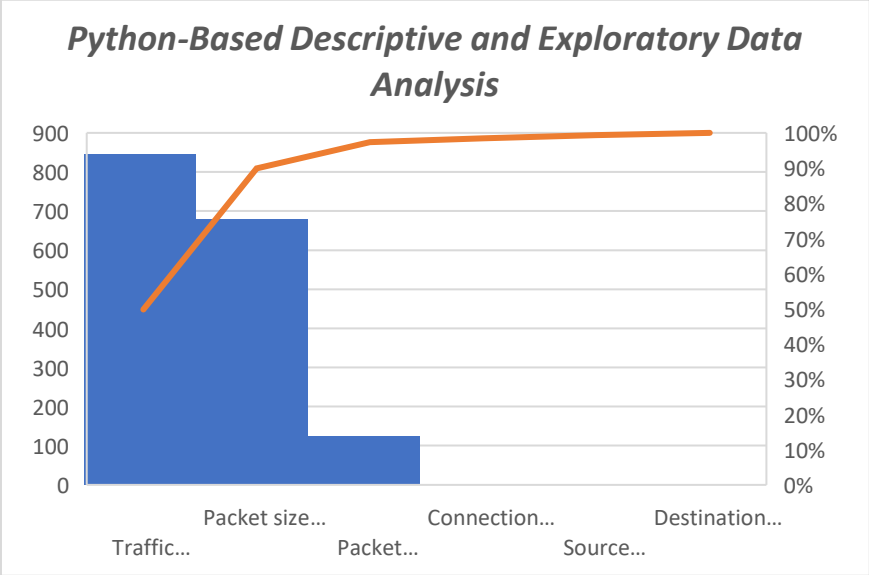


Fig 2: Python-Based Descriptive and Exploratory Data Analysis

Table 3: Python-Based Anomaly Detection and Classification

Traffic category	Frequency	Percentage
Normal network traffic	68,450	68.45%
Anomalous network traffic	31,550	31.55%
Total	100,000	100.00%

Comparative Performance of Anomaly Detection Models

Detection models	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Random Forest	94.20	93.10	91.80	92.44
Support Vector Machine	89.60	88.40	86.90	87.64
Isolation Forest	87.30	85.70	84.20	84.94
Adaptive Anomaly Detection	96.80	95.90	95.40	95.65

The classification analysis was based on the distribution of anomaly and normal traffic in the network, as well as the detection capabilities of various ML models. The normal traffic accounted for 68.45% of the observations while the anomalous traffic accounted for 31.55% of the observations. The adaptive anomaly detection model was the most accurate with a detection accuracy of 96.80%, followed by the Random Forest model with a detection accuracy of 94.20%. Likewise, the adaptive model showed better precision, recall and F1-score. These performance measures gave an assessment of the framework's capability to differentiate between properly used network activity and potentially malicious activity.

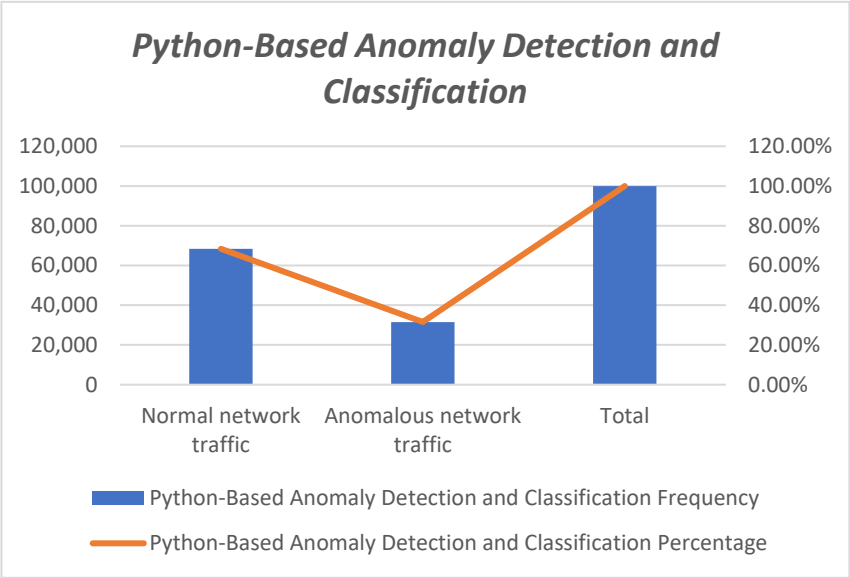


Fig 3: Python-Based Anomaly Detection and Classification

Table 4: Python-Based Adaptive Learning and Computational Performance Evaluation

Detection models	False-positive rate (%)	Processing time (seconds)
Random Forest	4.80	12.45
Support Vector Machine	7.20	18.60
Isolation Forest	8.50	9.35
Adaptive Anomaly Detection	3.10	10.80

Detection Performance Under Changing Network Traffic Conditions

Network traffic conditions	Conventional model accuracy (%)	Adaptive model accuracy (%)
Initial traffic patterns	95.10	96.80
Moderate traffic changes	88.40	94.20
Significant traffic changes	79.60	91.50
Emerging attack patterns	73.20	89.70

The adaptive learning analysis was performed to study the detection performance under changing network traffic and analysis of the computational efficiency of the proposed framework. The adaptive model's false-positive rate was 3.10%, with a processing time of 10.80 seconds. The accuracy of its model remained better than the conventional model as the network traffic changed, with 89.70% in the case of emerging attack patterns while the conventional model achieved 73.20%. The results emphasize the need for adaptive learning and concept drift management to ensure the detection performance as the network evolves or cybersecurity threats propagate.

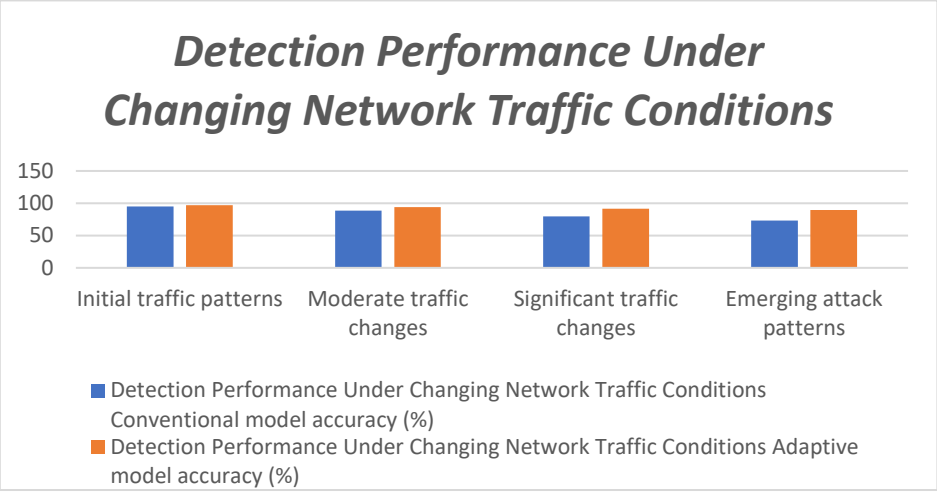


Fig 4: Detection Performance Under Changing Network Traffic Conditions

Table 5: Distribution of Network Traffic by Protocol Type

Protocol type	Frequency	Percentage
TCP	52,400	52.40%
UDP	31,600	31.60%
ICMP	10,500	10.50%
Other protocols	5,500	5.50%
Total	100,000	100.00%

The protocol distribution of network traffic showed that TCP was the most significant protocol with 52.40% of the total network traffic. UDP accounted for 31.60% and ICMP 10.50%. The remaining 5.50% were in other protocols. These differences showed that network communication was spread out over several protocol categories. Analysing protocol-level behaviour was crucial for identifying unusual communication patterns and for identifying potentially suspicious network actions.

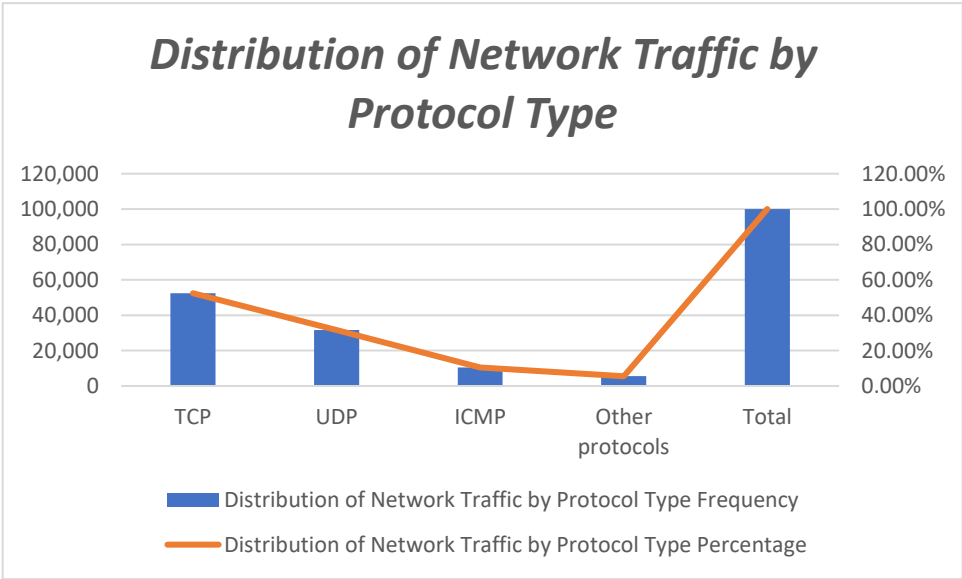


Fig 5: Distribution of Network Traffic by Protocol Type

Table 6: Distribution of Identified Cybersecurity Threat Categories

Cybersecurity threat category	Frequency	Percentage
Denial-of-Service attacks	9,200	29.16%
Port scanning	7,100	22.50%
Brute-force attacks	6,400	20.29%
Botnet activities	5,200	16.48%
Other emerging threats	3,650	11.57%
Total	31,550	100.00%

The distribution of cybersecurity threats showed that DoS attacks were the top threat, making up 29.16% of all anomalous activities identified. The topmost common attacks were port scanning (22.50%) and brute-force attacks (20.29%). The other emerging threats accounted for 11.57%, while botnet activities made up 16.48%. This classification showed that it is not sufficient to rely on a single threat detection pattern, but it is very important to consider various types of malicious network activity.

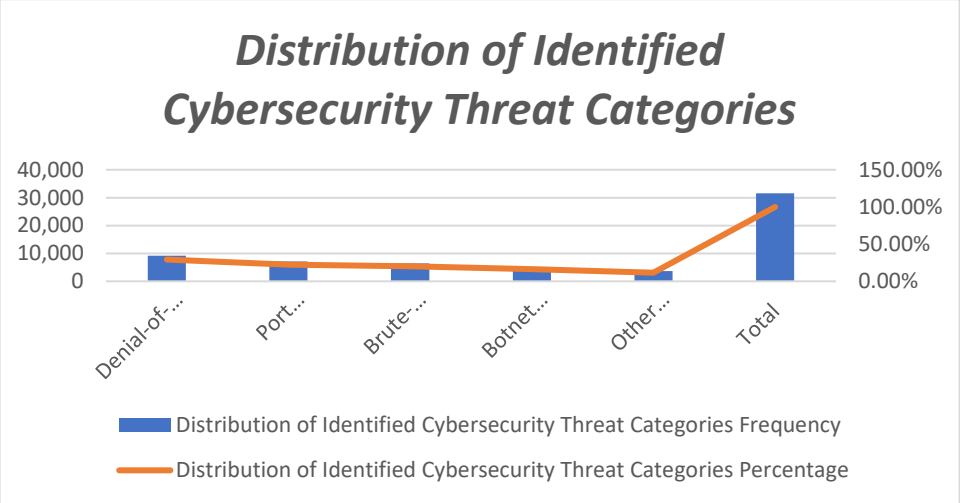


Fig 6: Distribution of Identified Cybersecurity Threat Categories

Table 7: Confusion Matrix of the Adaptive Anomaly Detection Model

Actual classification	Predicted normal	Predicted anomalous	Total
Normal traffic	66,329	2,121	68,450
Anomalous traffic	1,451	30,099	31,550
Total	67,780	32,220	100,000

The confusion matrix was used to assess the classification performance of the adaptive anomaly detection model. The model correctly classified 68,450 normal network traffic observations, while 2,121 normal observations were wrongly identified as anomalous. Similarly, 1,451 anomalous observations were incorrectly classified as normal, whereas 30,099 anomalous observations were correctly identified. These results helped explain the model's false positive and false negative rates and highlighted the need to improve threat detection while reducing incorrect classifications.

Table 8: Relative Importance of Network Traffic Features

Network traffic features	Feature importance (%)

Packet frequency	24.50
Traffic volume	21.30
Connection duration	18.70
Source connections	14.20
Destination connections	12.10
Protocol type	9.20
Total	100.00

The feature importance analysis results showed that the feature which is most important among the network traffic features is packet frequency which contributed 24.50% to the overall feature importance. The top two traffic volume and connection duration accounted for 21.30% and 18.70% respectively. The sources and destinations accounted for 14.20% and 12.10%, respectively, and protocol type made up 9.20%. The results highlighted the importance of traffic intensity, connection behavior and communication features in the identification of network traffic as either typical or potentially suspicious for cybersecurity.

Table 9: Detection Accuracy Across Cybersecurity Threat Categories

Attack category	**Detection accuracy (%)**
Denial-of-Service attacks	97.20
Port scanning	95.80
Brute-force attacks	94.60
Botnet activities	92.40
Other emerging threats	88.90

The comparison of accuracy of detection of each cyber security threat showed that the highest accuracy of detection was for Denial of Service (DoS) at 97.20%, followed by port scanning at 95.80%. The detection accuracy for brute force attacks and botnets was 94.60%, and 92.40%, respectively. The other emerging threats showed comparatively low accuracy at 88.90%. The difference indicated that the attack patterns that may be less familiar and evolving may pose a greater threat to anomaly detection systems, highlighting the need for ongoing model adaptation.

Discussion

The study focused on developing and evaluating an adaptive anomaly detection framework to identify emerging cybersecurity threats in networked systems. The findings highlighted the importance of combining network traffic analysis, machine learning, and adaptive learning techniques to detect unusual network activities more effectively. The study examined several key areas, including network traffic features, the identification of normal and abnormal activities, detection accuracy, false positive rates, important features, and the system's ability to maintain performance when network conditions change. The results showed that adaptive anomaly detection was a valuable tool for detecting suspicious network traffic, and that the detection rates were not compromised under varying traffic patterns. The results validate the increasing significance of intelligent cybersecurity solutions that can adapt to new types of attacks and are not limited to attack signatures defined a priori (Kommisetty et al., 2022).

The analysis of network traffic properties pointed out that the only studying of a few characteristics was not enough to detect unusual network communication patterns. Certain packet frequency, traffic volume, connection duration, source connections, destination connections and protocol type provided important information to distinguish normal network activities from suspicious activity. There were some changes in these features, suggesting that a single feature was insufficient to fully capture the network traffic. The result was in line with Aghazadeh Ardebili et al., (2024), which discussed machine learning and data mining methods for cyber security intrusion detection and the selection of the suitable features and analytical methods. In the same way, Pinto et al. (2024) described anomaly-based intrusion detection system as detecting abnormal activities by recognizing a normal pattern. Hence, the study of several network traffic attributes is helpful as a basis for creating more complex cyber threat detection systems.

Comparative analysis of anomaly detection models showed that it is essential to consider various machine learning methods using various performance measures. Only accuracy is not enough to understand the detection effectiveness of a model as it can have high overall accuracy without having a good detection for some malicious activities. Thus, precision and recall, as well as F1-score, can also provide insights into the reliability and completeness of the detection of threats. The classification measures reported indicate that the adaptive anomaly detection model achieved superior results compared to the other models: Random Forest, Support Vector Machine, and Isolation Forest. The pattern is similar to the one described by Diro et al., (2023) which studied different machine learning and data mining approaches used in cybersecurity and showed that the choice of model is dependent on the nature of the data and the nature of the detection problem. Anomaly-based network intrusion detection studies were also reviewed by Ndibe (2025) and the significance of preprocessing technique, detection technique, evaluation metric and selection of datasets were highlighted. Altogether, these studies back the application of several performance indicators to assess intelligent cybersecurity frameworks.

The feature importance analysis gave additional insights into the features in the network that were important in identifying abnormal activities. The most significant features were packet frequency and traffic volume, connection duration, source connections, destination connections, and protocol type. All these characteristics are significant since any unusual increase in packet transmission, any unexpected number of packets sent or received, and any unusual behavior in connections can help identify suspicious network activities. The contribution of individual features, however, can vary from one network environment to another and one set of features to another (depending on the characteristics of the data set and the types of attacks being studied). The researchers Jiang et al., (2026) noted that characteristics of the data and features selection are crucial in designing machine learning-based cybersecurity systems. Aminu et al. (2024) further noted that feature selection can also decrease computational complexity, remove redundant information and enhance the performance of intrusion detection. Therefore, identifying the relevant features of the network traffic is a crucial component in building efficient and reliable anomaly detection frameworks.

The adaptive learning and concept drift management is an important aspect of the present research. Network traffic patterns are not necessarily constant as the behavior of network communication, network setup, user activity, and techniques of cyberattacks can vary over time. As a result, historical network data-based detection models may become less effective over time as new traffic patterns occur. The detection performance analysis under varying network scenarios revealed the significance of preserving the model performance in the case of a changing network behavior. According to Maddireddy et al. (2024), concept drift happens when the distribution of the input data and the target variables evolve over time, thus mandating the learning system to adapt to new data distributions. Their research reviewed different strategies for detecting and managing concept drift and discussed the evaluation of adaptive learning algorithms. This is aligned with the goals of this current study where detection models are updated to address the evolving traffic in the networks and new attack types. Thus, adaptive learning can be a crucial mechanism to overcome the static nature of traditional detection models in dynamic cybersecurity scenarios.

Conclusion

In the present study, an adaptive anomaly detection framework for novel cybersecurity threats detection in networked systems was developed and evaluated. The study underscored the need for the use of network traffic analysis, machine learning methods, feature selection, and adaptive learning mechanisms in order to enhance the detection of abnormal network activities. The results showed that the consideration of various network traffic features like packet frequency, volume, connection duration and communication protocols is very important for the separation of normal traffic from potential malicious traffic. The comparative evaluation also highlighted the need for precision, accuracy, recall, F1-score, false-positive rate, and computational efficiency to determine the effectiveness of cybersecurity detection systems. In conclusion, the study highlighted the importance of adopting more flexible and responsive anomaly detection mechanisms to overcome the constraints of traditional detection methods.

In addition, the study pointed out that the issue of adaptive learning and concept drift control in preserving detection performance in changing network conditions is important. Static detection models can struggle to detect unknown threats as cyberattacks grow ever more sophisticated and network traffic is becoming more complex. The proposed adaptive framework suggests a computational perspective to adapt detection mechanisms as network dynamics evolve and new attacks appear. The study's findings play a crucial role in the evolution of smart cybersecurity systems, combining continuous traffic analysis, anomaly detection, and performance evaluation. It also lays the groundwork for further studies on real-time network monitoring, progressed machine learning algorithms, bigger cybersecurity events, and deep learning-based adaptive detection strategies.

Future Implications

Moving forward, adaptive anomaly detection frameworks should be further enhanced with the inclusion of advanced machine learning, deep-learning, and real time network monitoring techniques. The suggested approach could be expanded to larger and more varied cybersecurity datasets, to further enhance its capabilities in spotting new attacks and novel threat patterns in various network environments. Advanced concept drift detection methods, automatic model updating, and feature optimization algorithms should also be investigated to ensure accurate detection in the ever-evolving network environment. Furthermore, the combination of adaptive anomaly detection with cloud computing, the Internet of Things (IoT) networks, and distributed cybersecurity infrastructure could enhance its practical applications. These advancements could help to create more sophisticated, scalable and intelligent cybersecurity solutions that will be able to effectively deal with increasingly complex cyber threats.

References

1. Yang, Z., Liu, X., Li, T., Wu, D., Wang, J., Zhao, Y., & Han, H. (2022). A systematic literature review of methods and datasets for anomaly-based network intrusion detection. *Computers & Security*, *116*, 102675.
2. Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. *arXiv preprint arXiv:1802.09089*.
3. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), 20.
4. Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials*, *18*(2), 1153-1176.
5. Moriano, P., Hespeler, S. C., Li, M., & Mahbub, M. (2025). Adaptive anomaly detection for identifying attacks in cyber-physical systems: A systematic literature review. *Artificial Intelligence Review*, *58*(9), 283.
6. Raeiszadeh, M., Ebrahimzadeh, A., Glitho, R. H., Eker, J., & Mini, R. A. (2024). Real-time adaptive anomaly detection in industrial IoT environments. *IEEE Transactions on Network and Service Management*, *21*(6), 6839-6856.
7. Maddireddy, B. R., & Maddireddy, B. R. (2022). Cybersecurity threat landscape: Predictive modelling using advanced AI algorithms. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 270-285.
8. Haile, A. T., Abebe, S. L., & Melaku, H. M. (2025). Real-time automated cyber threat classification and emerging threat detection framework. *IEEE Open Journal of the Computer Society*, *6*, 921-930.
9. Kothamali, P. R., Banik, S., & Nadimpalli, S. V. (2020). Introduction to Threat Detection in Cybersecurity. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 113-132.
10. Radford, B. J., Apolonio, L. M., Trias, A. J., & Simpson, J. A. (2018). Network traffic anomaly detection using recurrent neural networks. *arXiv preprint arXiv:1803.10769*.
11. DeAlmeida, J. M., Pontes, C. F., DaSilva, L. A., Both, C. B., Gondim, J. J., Ralha, C. G., & Marotta, M. A. (2021). Abnormal behavior detection based on traffic pattern categorization in mobile networks. *IEEE Transactions on Network and Service Management*, *18*(4), 4213-4224.
12. Prashanth, B. S., Kumar, M. M., Puneetha, B. H., Almuraqab, N. A. S., Hoque, A., Moonesar, I. A., & Rao, A. (2025). Adaptive buffering strategies for incremental learning under concept drift in lifestyle disease modeling. *IEEE Access*, *13*, 174001-174033.
13. Canonaco, G., Bergamasco, A., Mongelluzzo, A., & Roveri, M. (2021, July). Adaptive federated learning in presence of concept drift. In *2021 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-7). IEEE.
14. Shaik, A. S., & Shaik, A. (2024, April). AI enhanced cyber security methods for anomaly detection. In *International conference on machine intelligence, tools, and applications* (pp. 348-359). Cham: Springer Nature Switzerland.
15. Mahin, K., & Ashfaq, S. (2024). Machine Learning Enhanced Intrusion Detection and Anomaly Classification for MIS-Driven Enterprise Network Security. *International Journal of Scientific Interdisciplinary Research*, *14*(09), 01-41.

16. Kosari, A. (2025). Real-time network traffic anomaly detection using spiking neural networks (SNNs) with adaptive learning.

17. Sunkara, G. (2022). AI-driven cybersecurity: Advancing intelligent threat detection and adaptive network security in the era of sophisticated cyber-attacks. *Well Testing Journal*, *31*(1), 185-198.

18. Odunayo, J. J. (2026). Machine Learning-Based Cyber Threat Detection: A Review of Methods for Identifying Network Attacks and Anomalies. *Available at SSRN 7545501*.

19. Lara-Gutierrez, A., Fernandez-Gago, C., & Onieva, J. A. (2025). A Framework for Drift Detection and Adaptation in AI-driven Anomaly and Threat Detection Systems: A. Lara-Gutierrez et al. *International Journal of Information Security*, *24*(5), 199.

20. Garg, M., Singh, S., Tiwari, S., Kaushik, K., Kumawat, R., & Soni, M. (2025, November). Adaptive cybersecurity frameworks: Leveraging artificial intelligence for proactive threat detection and forensic readiness. In *2025 2nd International Conference on Intelligent Systems for Cybersecurity (ISCS)* (pp. 1-7). IEEE.

21. Ameedeen, M. A., Hamid, R. A., Aldhyani, T. H., Al-Nassr, L. A. K., Olatunji, S. O., & Subramanian, P. (2024). A framework for automated big data analytics in cybersecurity threat detection. *Mesopotamian Journal of Big Data*, *4*(1), 175-184.

22. Hossain, M. A. (2025). Deep Q-learning intrusion detection system (DQ-IDS): A novel reinforcement learning approach for adaptive and self-learning cybersecurity. *ICT Express*.

23. Cahyono, D., Herman, H., & Van Versie, I. (2026). Self Learning Artificial Intelligence for Autonomous Threat Detection in Computer Networks. *Journal of Computer Science and Technology Application*, *3*(2), 130-141.

24. Zhukabayeva, T., Pervez, A., Mardenov, Y., Othman, M., Karabayev, N., & Ahmad, Z. (2024). A traffic analysis and node categorization-aware machine learning-integrated framework for cybersecurity intrusion detection and prevention of WSNs in smart grids. *IEEE Access*, *12*, 91715-91733.

25. Palaniappan, K., Duraipandi, B., & Balasubramanian, U. M. (2024). Dynamic behavioral profiling for anomaly detection in software-defined IoT networks: A machine learning approach. *Peer-to-Peer Networking and Applications*, *17*(4), 2450-2469.

26. Villegas-Ch, W., Gutierrez, R., Sánchez-Salazar, I., & Mera-Navarrete, A. (2024). Adaptive security framework for the internet of things: improving threat detection and energy optimization in distributed environments. *IEEE Access*, *12*, 157924-157944.

27. Wandwi, G., & Habimana, T. (2026). Applying Machine Learning for Real-Time Threat Detection in Adaptive Cybersecurity Systems. *Open Journal of Applied Sciences*, *16*(9), 3469-3488.

28. Alsalman, D. (2024). A comparative study of anomaly detection techniques for IoT security using adaptive machine learning for IoT threats. *IEEE Access*, *12*, 14719-14730.

29. Majumder, C., Sultana, N., Choain, A. H. K., & Nasir, M. A. (2026). Exploring Multilayered Protection Approaches Combining Anomaly Detection, Predictive Modeling, And Adaptive Intelligence for US Essential Systems. *Spanish Journal of Innovation and Integrity*, *50*, 31-47.

30. Jeffrey, N., Tan, Q., & Villar, J. R. (2023). A review of anomaly detection strategies to detect threats to cyber-physical systems. *Electronics*, *12*(15), 3283.

31. Zeng, H., Yunis, M., Khalil, A., & Mirza, N. (2024). Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks for enhanced cybersecurity. *Journal of Innovation & Knowledge*, *9*(4), 100601.

32. Kommisetty, P. D., Kuppala, B. M., & Buvvaji, H. V. (2022). Transforming cyber defense: Anomaly detection and predictive analytics for automated threat response. *International Journal of Engineering and Computer Science*, *11*(8), 25585-25600.

33. Aghazadeh Ardebili, A., Hasidi, O., Bendaouia, A., Khalil, A., Khalil, S., Luceri, D., ... & Ficarella, A. (2024). Enhancing resilience in complex energy systems through real-time anomaly detection: a systematic literature review. *Energy Informatics*, *7*(1), 96.

34. Pinto, A., Herrera, L. C., Donoso, Y., & Gutierrez, J. A. (2024). Enhancing critical infrastructure security: Unsupervised learning approaches for anomaly detection. *International Journal of Computational Intelligence Systems*, *17*(1), 236.

35. Diro, A., Kaisar, S., Vasilakos, A. V., Anwar, A., Nasirian, A., & Olani, G. (2023). Anomaly detection for space information networks: a survey of challenges, schemes, and recommendations.

36. Ndibe, O. S. (2025). Ai-driven forensic systems for real-time anomaly detection and threat mitigation in cybersecurity infrastructures. *International journal of research publication and reviews*, *6*(5), 389-411.

37. Jiang, L., Ryan, R., Li, Q., & Ferdosian, N. (2026). A survey of heterogeneous graph neural networks for cybersecurity anomaly detection. *Journal of Computer Security*, *34*(5), 387-416.

38. Aminu, M., Akinsanya, A., Dako, D. A., & Oyedokun, O. (2024). Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. *International Journal of Computer Applications Technology and Research*, *13*(8), 11-27.

39. Maddireddy, B. R., & Maddireddy, B. R. (2024). Neural network architectures in cybersecurity: optimizing anomaly detection and prevention. *International Journal of Advanced Engineering Technologies and Innovations*, *2*(1), 238-266.



2026 by the authors; Journal of Global Social Transformation (JGST). This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (http://creativecommons.org/licenses/by/4.0/).