







Research Article

Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure

Noora Zidan Khalaf^{1, }, Israa Ibraheem Al Barazanchi^{2, }, A. D. Radhi^{3, }, Sushma Parihar^{4, *, }, Pritesh Shah^{4, },
Ravi Sekhar^{4, }

¹Quality Assurance & University Performance, Mustansiriyah University, Baghdad, Iraq

²College of Engineering, University of Warith Al-Anbiyaa, Karbala, Iraq

³College of Pharmacy, University of Al-Ameed, Karbala PO Box 198, Iraq

⁴Symbiosis Institute of Technology (SIT) Pune Campus, Symbiosis International (Deemed University) (SIU), Pune, 412115, Maharashtra, India

ARTICLE INFO

Article history

Received 20 Feb 2025

Revised 15 Mar 2025

Accepted 24 May 2025

Published 17 Jun 2025

Keywords

Real-time threat detection

AI-driven cybersecurity

critical infrastructure protection

machine learning in cybersecurity

anomaly detection



ABSTRACT

Protection of infrastructure is becoming increasingly demanding, and the sophistication and severity of cyber threats are increasing daily. Traditional threat detection techniques cannot match the ever-evolving nature of cyber threats, which increases the number of false positives and attack misses. AI-driven methods address these shortfalls via the use of advanced learning algorithms to detect and respond to newly discovered threats in real time. They are largely static rule-based or signature-based attacks, and they do not perform effectively against zero-day attacks and highly organized, advanced attacks. Given the critical need to protect digital infrastructures such as energy, transport, and communications from destruction, which threatens security and operational integrity, an adaptive means for real-time and accurate threat detection must evolve. This research aims to determine the optimum method for designing and testing an AI-based real-time threat detection system that is suitable for use in critical infrastructure environments. Compared with traditional methods, the proposed system uses an advanced machine learning technique to provide better detection accuracy, adaptiveness, and efficiency of results. It is designed to integrate all the critical features of data integration, anomaly detection, and feature extraction along with an automated response mechanism that allows the system to detect various types of threats and cyberattacks, including new and sophisticated ones, without much human intervention. Some of the key performance indicators, including accuracy, precision, recall, and F1 score, ensure that, indeed, the system is effective. The research findings illustrate that for clear readability, the AI-based detection system reported an accuracy value of 0.95, where precision is 0.93 and a recall value of 0.92 with the F1 score of 0.92, hence performing better than do conventional methods of threat detection. This suggests that it reports a high rate of false-positive rejection while returning proper alerts in the case of real-time operation. This was also enhanced by an automated response feature of the system that provided faster threat mitigations with shorter times for all types of responses, leading to even improved security. Finally, the paper has demonstrated how the AI-based approach is a viable and scalable solution towards mitigating current cybersecurity challenges in critical infrastructures and, at the same time, providing opportunities for further research into more robust, flexible, and autonomous defense systems.

1. INTRODUCTION

Within the last few years, there has been a tremendous increase in the scale and sophistication of cyber threats against critical infrastructures. The 2015 Ukrainian Power Grid Cyber Attack, the ransomware attack against the Colonial Pipeline in 2021, and several others are truly very dangerous precedents that indicate the disruptive and potentially disastrous consequences that may result from a single cyber incident. Incidents of this nature point to the sound and proactive controls of security that could identify the threat and respond to it in real time. Traditional methods of cybersecurity are based, in many respects, on manual oversight and reactive protocols, which have been completely proven incapable of handling the nature of these threats. Most of these have now become automated, adaptive, and, in most instances, driven by malicious AI. Real-time threat detection has recently become one of the key requirements for CI protection, and AI has started to play a major role in developing such capabilities [1]. The application of AI to CI, in view of its promising advantages in cybersecurity, has been considered. Artificial intelligence-driven threat detection systems work at speed and accuracy to monitor network traffic, user behavior, and system logs unceasingly for anomalies that may indicate an attack. In contrast to traditional methods, AI models analyse large volumes of data in real time and hence detect threats at much higher velocities with much greater accuracy. Machine learning and deep learning models study how to predict patterns of malicious behavior from historical data and may even evolve as new types of attacks pop up [2]. These functionalities support the adaptation of AI-driven systems to rapid changes in the threat landscape and provide proactive defense, which is extremely important for CI protection. While the potential of AI-driven cybersecurity solutions for CI is clear, putting it into actual practice presents a host of challenges. Many CI systems were designed and built decades ago, long before cybersecurity threats were understood, and as such, they were unequipped to address modern security practices without major upgrades. Second, CI networks often operate in real time and cannot afford downtime, which complicates the deployment and testing of new security technologies [3]. In summary, there is an interesting paradox regarding the element of data privacy and the demand for flow in relation to the integration challenge in applying AI systems to CI. Indeed, it is challenging to demand a carefully designed system with an operational method of data and integrative operations to achieve effective, sustained AI-driven threat detection within a CI environment. It follows that this work intends to highlight the state-of-the-art conditions in the elaboration of AI-driven and real-time, threat-detecting systems exclusively designed for CI protection. From the very needs of CIs to what role AI would play in their fulfilment, this would be a guidance paper on 'how to do it' and implement and maintain effective cybersecurity solutions in place. It presents specific challenges and vulnerabilities of CI, the architecture and functionality of AI-driven detection systems, and lessons learned from real-world case studies [4][36]. Overall, this paper explains how AI can revolutionize cybersecurity for critical infrastructures and understand the rising technologies that might be used in protecting the infrastructure relevant to a society.

Figure 1 shows how ML models deployed in cloud environments are susceptible to highly coordinated cyberattacks by a bot master. The upper part shows a number of ML approaches—supervised learning, unsupervised learning, reinforcement learning, and deep learning—used in analysis and prediction. These models are hosted on cloud servers, which are entry points by the hostile agents. The attacker's bot master, or controller of attacker systems, orchestrates a series of attacks that target the ML models with the intention of compromising them. The lower portion illustrates different types of attacks, such as data poisoning, model evasion, and adversarial attacks, which can mislead or compromise the performance of the ML model. The graph indicates the vulnerability of ML systems to coordinated cyber attacks, requiring robust security to protect AI-powered applications.

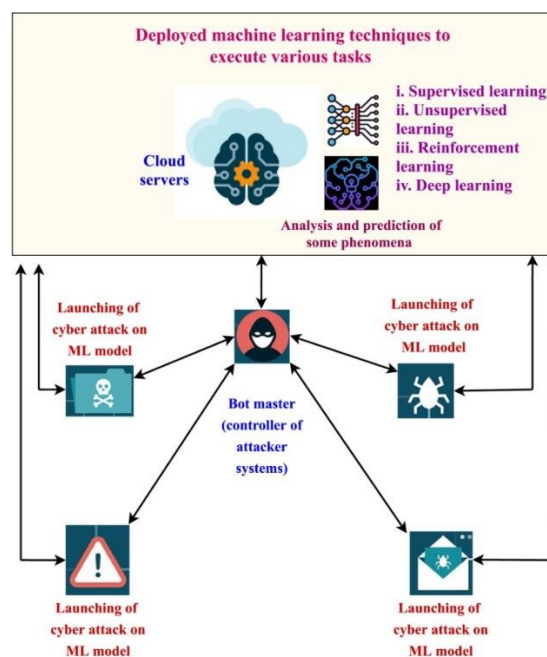


Fig. 1. Cybersack Launch on Machine Learning Models in Cloud Servers

These ML models utilize supervised learning, unsupervised learning, reinforcement learning, and deep learning to predict and analyze data patterns. Such types of cyberattacks that are controlled by a sole bot master and utilized as the attacker or evil controller pose a threat to ML models. Such attacks target various vulnerabilities of the system for disrupting or manipulating the functioning of the model. These findings echo the susceptibility of cloud-based ML systems during operations within adversarial settings and confirmed the need for strong cybersecurity defenses [6].

1.1. Research Gap and Research Question

The increasing integration of AI-driven solutions in cybersecurity has not yet succeeded in creating real-time adaptive threat detection systems that can maintain accuracy while remaining computationally efficient and resilient to adversarial attacks. Conventional cybersecurity systems demonstrate high false positive rates along with slow detection capabilities and fail to identify modern complex cyber threats. AI-based cybersecurity models have undergone considerable advancements but face deployment obstacles in large-scale critical infrastructure due to their adversarial robustness, explainability limitations and scalability issues. Researchers currently do not extensively evaluate real-time performance factors such as inference time and computational overhead, which are critical for effective system deployment. To address these challenges, this study aims to answer the following key research question: What design and optimization strategies can be applied to create an AI-based real-time threat detection system that achieves high accuracy and adversarial robustness while scaling effectively and maintaining computational efficiency to protect critical infrastructure? This study introduces a new AI-based framework that combines adaptive anomaly detection with automated response systems and explainable AI methods to maintain security and interpretability in critical cybersecurity settings.

2. RTELATED WORK

The transformative aspect of AI involves automating the processes of detecting, stopping, and responding to cyberthreats, which is useful for many organizations, including CI. Like other sectors, CIs are not AI-ready, and AI-driven methodologies have undergone significant improvements [7]. The application of AI, automation and analytics enables protection from cyberattacks via machine learning, deep learning, and neural networks. The flexibility, extensibility, and automation achieved through those technologies are fundamental features for the protection of infrastructure vital for public safety and national security. In this section, primary AI algorithms and their benefits over traditional techniques in cybersecurity are analysed along with the paradigm of AI-enabled threat detection [8]. AI-driven cybersecurity systems have deployed various sophisticated techniques, each with different advantages in the field of threat detection and response. It has become one of the most utilized techniques, with training algorithms via large datasets for recognizing patterns that would indicate a cyber threat. In cybersecurity, ML can pick out unusual behavior within network traffic, user activities, or system processes that might signal a security breach. Over time, ML models improve by continuously learning from both past data and real-time inputs. This enables them to detect subtle and novel attack patterns, which rule-based detection mechanisms often fail to identify. While ML is itself a subset of deep learning, it takes advantage of multitier neural networks that handle complex datasets to find sophisticated patterns within them [9]. Thus, deep learning techniques prove very effective at analysing large volumes of unstructured data, such as logs, images, and audio, which makes them ideal for applications such as endpoint security, malware detection, and intrusion detection in complex networks. These systems can identify patterns that can increase the speed and precision of threat detection, perhaps because human analysts might not find them. Neural networks are one of the foundations of deep learning, enabling AI models to find complex relationships between items of data, for example, highlighting anomalies in users' behavior or recognizing signs of phishing. Through continuous data analysis and learning from experience, neural networks can identify even slight deviations from the norm and indicate potential dangers for rapid intervention. Compared with traditional approaches, AI-driven cybersecurity systems inherently have advantages, mainly in terms of speed, accuracy, and adaptability. In many areas of traditional cybersecurity, there are predefined rules or signature-based detections, but an AI system has no limits concerning a predefined set of threats that have been known before [10]. Speed and accuracy are crucial in CI security: delays and false positives may cause critical service interruptions. With AI-driven systems, large volumes of data can be analysed in real time to identify threats the moment they become visible with far greater accuracy than human analysts. The speed and precision of this approach allow CI operators to act in a timely manner and reduce the risk of an effective attack, thereby constraining damage. Another strong positive feature of AI-driven cybersecurity is its ability to scale up and evolve along with the threat landscape. Traditional cybersecurity measures could be challenged by new types of attacks, given that attackers continuously create new techniques and use automation on their end. AI models, however, are built to learn from past data and for instantaneous threat mitigation to continuously improve detection, as new forms of cyber threats are being developed [11]. This is important for CI, which has to keep up with not only current threats but possibly even future threats. Since AI-driven systems are trained using vast amounts of data, including new incidents and benign activity patterns, they can detect unknown or abnormal behaviors much better. Thus, AI-powered systems are ideal for environments that face emerging threats continuously. AI-driven cybersecurity systems use multiple threat detection models that best fit different security needs and threat profiles. The signature-based detection relies on known patterns of malicious code, traffic, and behaviors to identify threats, in addition to being one of the most traditional methods. The drawback of this signature-based approach is that, while it is effective for previously identified threats, it lacks the ability to find novel or modified threats. AI can, of course, make signature-based detection much faster by analysing and matching vast signature databases to identify known threats much more efficiently [12]. In anomaly based detection, AI models determine the baseline of normal behavior in systems and networks. Anomaly based intrusion detection systems are able to detect deviations from normal behavior that

may indicate a security threat by monitoring data continuously in real time. This will be very effective in a CI environment since it is typical for attackers to use tactics that are very subtle, discreet, and hence not set off any alarm. Since anomaly based detection recognizes unknown or zero-day attacks, it has become very helpful in fighting these emerging threats, which have not yet been catalogued within signature databases. Hybrid models combine the best of both worlds to provide a better security model, where signature-based detection is combined with anomaly based detection [13]. These hybrid models have the potential ability to identify known threats with an improved speed of detection and reveal new/suspicious behavior that does not match any of the predefined signatures. This makes the combination especially valuable for CI because any compromise in security may have wide ramifications. Hybrid solutions provide several levels of threat detection, laying protection against known and unknown threats and making CI systems resilient to dynamic and uncertain cyber security threats [14].

Next-gen solutions surpass legacy rule-based and signature-based solutions through the implementation of advanced AI-based methods such as generative AI, machine learning, and deep learning. Such solutions are fast becoming a preferred form of AI-based solution within cybersecurity thanks to the strengths of generative AI to recognize and prevent attacks in advance. While conventional methods rely on established precepts and human expertise, generative AI is able to digest large amounts of data and pick up subtle patterns that can often go unnoticed even by human professionals. Further, generative AI can create security products, such as safe passwords and even safer encryption algorithms, thereby serving as an active process of strengthening cybersecurity protection [15]. With cyberattacks becoming sophisticated, AI has been applied in preemptively predicting attacks before they actually occur. One of the more recent approaches is the creation of big data analytics algorithms that are capable of anticipating cyberattacks through real-time threat prevention. The program uses deep learning and behavioral analysis to determine unusual patterns that may be indicators of a pending attack. By analysing data from multiple internal network sources, attached devices, and threat feeds, AI systems are able to sift through millions of events in real time and identify suspicious activities [16] [17].

Limitations of the present methodologies used in real-time threat detection systems in AI-driven cybersecurity in critical infrastructure are presented in Table 1. Some of the traditional methods for signature-based detection, rule-based systems, face difficulties in terms of high false positive rates, inability to adapt to new or evolving threats, and inability to scale in large-scale infrastructures. These systems rely mostly on siloed data and manual intervention, making them less effective against sophisticated, coordinated attacks and increasing their vulnerability to insider threats. In addition, many current solutions suffer from privacy and ethical issues and cannot provide integrated data analysis; these aspects further make human expertise crucial, which delays the response time.

TABLE I. CURRENT REAL-TIME THREAT DETECTION SYSTEMS - LIMITATIONS

Current Method	Problem	Description of Limitation
Signature-Based Detection	High False Positive and False Negative Rates	Often results in high false positives, causing alert fatigue, and high false negatives, missing actual threats and posing security risks.
Rule-Based Systems	Lack of Adaptability to New Threats	Depending on predefined rules and known threat signatures, making it ineffective against zero-day attacks and novel, sophisticated threats like AI-driven or polymorphic malware.
Centralized Data Processing	Limited Scalability and High Latency	Struggles with large data volumes, causing latency issues that prevent real-time detection and response in expansive critical infrastructure environments.
Siloed Monitoring Tools	Challenges in Data Integration and Contextual Analysis	Separate monitoring tools across systems hinder data integration and contextual analysis, limiting situational awareness and missing coordinated attack indicators.
Manual or Semi-Automated Security Solutions	Resource Constraints and Cost Issues	Resource-intensive, requiring significant budget and maintenance, which is often unsustainable for critical infrastructure sectors with limited financial resources.
Data Collection without Privacy Measures	Privacy and Ethical Concerns	Lacks mechanisms to securely handle sensitive operational and personal data, raising privacy and compliance issues, which restricts the use of AI-driven cybersecurity.
Perimeter-Based Defense Systems	Difficulty in Detecting Insider Threats	Designed primarily for external threats and lacks behavioral analysis, failing to detect subtle indicators of insider threats in real time.
Human-Dependent Threat Analysis	Dependency on Human Intervention and Expertise	Requires constant human intervention for identifying and responding to threats, leading to delays and relying heavily on cybersecurity expertise, which is often in short supply.

Contributions of this study: In the end, this research aims to remedy these defects through the development of new AI-driven solutions that are adaptive, scalable, and real-time threat detection critical infrastructure environments. This approach introduces methods for better integration of data and contextual analysis so that the systems can identify complex and coordinated attacks more precisely. Thus, the contributions of this work lie in automation, behavioral analysis, and mechanisms of preserving privacy, which will contribute to evolving cybersecurity systems to operate with minimal human intervention. The approach also reduces the response times and provides better security against both external and insider threats. These contributions provide a framework for building more resilient and responsive cybersecurity systems for critical infrastructure. The general perspectives of cybersecurity are now changing dimensions, particularly with the use of artificial intelligence to protect critical infrastructure systems from emerging cyber threats. Systems responsible for essential services ranging from power and water to transportation face many unique challenges that traditional cybersecurity methods often cannot cope with effectively. AI-powered cybersecurity offers a new level of complexity and effectiveness, therefore allowing for real-time threat detection, accelerating the speed of response, and fast adaptation of new types of attacks [18]. The following section presents key AI techniques comprising machine learning, deep learning, neural networks, and their concrete applications for threat detection in CI. We also discuss the benefits that AI provides over conventional security processes in terms of speed, accuracy,

and adaptability before delving into various AI-powered threat detection models in force today. The lowest layer would be the AI cybersecurity systems themselves, where various techniques are needed, each contributing in its unique way to detecting, analysing, and responding to cyber threats. Machine learning is a foundational technology in AI-driven cybersecurity; it involves training algorithms on vast datasets to recognize patterns that intimate potential security threats. In fact, ML models can find unusual behavior in network traffic, system processes, and user activities as potential indicators of a breach. Additionally, given more time to analyse data, such models will become even more effective at detecting known and novel threats while increasing the ability to detect sophisticated patterns of attacks that might bypass traditional security tools. Deep learning is a segment of ML that uses multilayered neural networks to study large and varied datasets; therefore, it is quite effective in finding complicated patterns in unstructured data such as system logs or endpoint data. Deep learning techniques can accurately detect several kinds of malware threat detection or unauthorized network intrusions that could be obscure or even hidden at times. Deep learning neural networks present an opportunity for AI models to identify anomalies caused by intricate relationships in the data. Through constant training where such networks are fed with historical as well as real-time data, they detect even the slightest variations in patterns of expected behavior that may point towards a security risk.

In this context, AI cybersecurity has several obvious advantages over traditional cybersecurity in terms of speed, accuracy, and responsiveness. While traditional cybersecurity approaches are usually centered on static rules and human-staffed response, AI systems can run autonomously, processing haystacks of data in real-time threat elimination. This is particularly important in CI, where delayed response to threats could result in service disruption or further damage [19]. AI-powered systems can spot threats and act on them in near-instantaneous threat mitigation, with often much higher accuracy than human analysts do, thereby reducing false positives and missed incidents. The second critical advantage of AI-driven cybersecurity pertains to scalability and flexibility. While classic systems cannot react properly to new modes of attack, cybercriminals increasingly turn to the use of automation and adaptive methods. While AI models learn from past incidents and day-to-day data streams, they recognize and adapt to emerging threat patterns. This degree of adaptability is key in CI because a uniform approach to security will be entirely irrelevant in light of threats that continuously change. This means that as more data are fed into AI-driven systems, they become increasingly capable of finding new, unfamiliar attack vectors—something that offers a dynamic, robust approach to defense in CI environments [20].

AI-driven cybersecurity is a suite of various threat detection models, each having unique ways through which they address security needs and threats. The more traditional methods are signature-based detection methods, which assume predefined patterns for malicious code, behavior, or network activity when identifying the threat. While a signature-based model can do a good job of detecting a previously encountered threat with high efficiency, most of them lack the much-needed flexibility to recognize new or modified attacks. AI enhances this by making it possible to scan giant signature databases at high speed, hence the quick identification of known threats [21-25].

3. METHODS

This research addresses some of the most important challenges in critical infrastructure cybersecurity. This approach results in many false positives and missed threats that generally occur in traditional systems, increases accuracy through an AI-driven detection approach to reduce unwanted alerts, and makes finding minute threats possible that would otherwise have remained hidden. The framework will also overcome another limitation of better adaptability, as classic methods using predefined rules cannot find new or evolving threats. This framework recognizes novel and zero-day attacks through the use of machine learning and anomaly detection without completely depending on the signature of known threats. In addition, it addresses scalability and responsiveness in real time; most of the existing systems are incapable of processing the volume generated by critical infrastructure and thus delay detection and responsiveness. This proposed framework is for real-time processing, which ensures timely detection and timely action. Another significant solution provided by this research involves how heterogeneous data sources can be combined in a general critical infrastructure environment where data are generated within different systems and formats. The framework includes an enhanced module of data integration that can facilitate seamless analysis among various data types for comprehensive threat detection. This research further limits human involvement by solving the problem of slow response times and skill gaps in cybersecurity through the inclusion of automated responses that immediately kick in once a threat has been detected. The research also enhances insider threat detection, which is likely to be missed by traditional systems since they are faceward-facing in how they identify external threats. The model can indicate an insider threat via analysis of behavior patterns that display anomalous internal activity. The general contribution of this work is a more flexible and scalable solution to cybersecurity to adequately match the loopholes in the reviewed techniques in securing critical infrastructures. The integrated solution will include data collection, preprocessing, and analysis via advanced AI models for threat response.

3.1 AI challenges: Adversarial attacks and explainability

While AI-based threat detection software has much to offer in the way of finding and hindering cyber attacks, they also address their own issues. One of the greatest vulnerabilities of AI systems is that they can be attacked by adversarial attacks, where attackers create tiny perturbations in the input data to trick the model's predictions. These attacks can make the trustworthiness of AI-based cybersecurity systems questionable, leading to misclassification of threats or evasions by sophisticated malware. Robustness adversarial is enhanced by advanced defense methods, i.e., adversarial training, defensive distillation, and anomaly based detection, that make the model more powerful in evasion of unwanted manipulations. Explainability and interpretability are some of the other issues being debated. The majority of the AI-based security models, particularly deep-learning-based models, are "black boxes," and hence it is difficult for security professionals to comprehend the reasons for predictions. Such

transparency gap has implications on trust, accountability, as well as regulation, especially protection of key infrastructure. To mitigate this, applications of explainable AI techniques such as Shapley Additive Explanations (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME) can make decision-making transparent, enable higher levels of user trust, and enable better threat response processes.

To be deployed in real time in cybersecurity, AI models need to be not just accurate but also computationally lightweight. A threat detection system's performance is heavily reliant on the latency of its inference time—the period taken to examine data as it arrives and determine threats. Models with high latency can cause response times to be slow, allowing an opportunity for attackers to take advantage of openings before a response can be delivered. Second, AI models must operate in resource-constrained environments, particularly edge computing scenarios where both processing resources and storage are not plentiful. To measure the computation efficiency of the proposed AI-based framework, KPIs such as execution time, memory consumption, and processing overhead must be compared. Techniques such as model pruning, quantization, and hardware acceleration (e.g., on GPUs or TPUs) can improve real-time performance without compromising high detection accuracy. Equilibrating these factors makes AI-focused cybersecurity measures scalable and achievable to implement in real critical infrastructure instances. The following are the fundamental steps with parameters and equations that are the core of the operation:

A. Data collection and integration

- Data Sources: The system sustains itself using data from many critical infrastructures, such as energy grids, transport, and communications. The dataset can consist of structured data created at regular intervals, e.g., system logs, or unstructured data, e.g., network traffic.

$D = \{d_1, d_2, \dots, d_n\}$: Data points collected from different sources.

T: Timestamp associated with each data point.

S: Source or category of each data point (e.g., network, device, or application).

Integration function:

The data integration module aggregates and standardizes data into a common format as follows:

$$D_{\text{integrated}} = f_{\text{integrate}}(D, T, S) \quad (1)$$

where $f_{\text{integrate}}$ represents the data preprocessing and standardization operations that integrate data from various sources into a unified format for further processing.

B. Feature Extraction and Preprocessing

- Objective: To draw key features from raw data that are capable of revealing potential indications of security threats.

$F = \{f_1, f_2, \dots, f_m\}$: Set of extracted features for each data point.

$P_{\text{threshold}}$: Threshold parameter to filter out irrelevant or noisy features.

Feature Extraction Function:

The feature vectors are extracted and transformed via functions such as:

$$F_i = f_{\text{extract}}(d_i), \text{ for } i \in [1, n] \quad (2)$$

where f_{extract} involves conversions such as tokenization, scaling, or encoding, depending on the type of data being processed.

C. AI-Based Threat Detection and Analysis

- Model Selection: Anomaly or threat-indicative pattern detection is accomplished with a machine learning model or ensemble, e.g., a deep neural network or a recurrent neural network.

θ : Model parameters trained to minimize prediction errors.

L: Loss function, typically binary cross-entropy for classification or mean squared error for regression tasks.

Training and Inference Equations:

The model is trained on historical data to minimize the loss:

$$\min_{\theta} \sum_{i=1}^N L(y_i, \hat{y}_i) \quad (3)$$

where y_i is the true label and where \hat{y}_i is the predicted label for the i -th data point.

During inference, the model generates predictions on real-time data:

$$\hat{y} = f_{\text{model}}(F; \theta) \quad (4)$$

D. Anomaly detection and thresholding

- Objective: To identify deviations from normal behavior, which may indicate potential security threats.

μ and σ : Mean and standard deviation of normal behavior on the basis of historical data.

α : Anomaly threshold, which determines when a data point is considered anomalous.

Anomaly score equation:

Anomaly scores are calculated via statistical or machine learning techniques, such as:

$$A_i = \frac{|f_i - \mu|}{\sigma} \quad (5)$$

where A_i is the anomaly score for feature f_i . If $A_i > \alpha$, the data point is flagged as a potential threat.

E. Automated response and alerting

- Objective: To respond to identified threats in real time while minimizing potential harm to critical infrastructure.

R_{type} : Type of response (e.g., alert, block IP, isolate device).

$T_{response}$: Response time, optimized to reduce the reaction delay.

Response Function:

On the basis of the threat level, the system triggers an automated response:

$$R = f_{response}(A, R_{type}, T_{response}) \quad (6)$$

where $f_{response}$ maps the anomaly score and response type to an action, such as generating an alert or isolating a compromised system.

Figure 2: Workflow of the proposed approach; it starts with data collection and integration, where it gathers data from different infrastructure sources and unifies it in one format. The second step is feature extraction, where various data are processed to extract the relevant features that can indicate certain cybersecurity threats. Once the features are extracted, they go through a module of AI-based detection where machine learning algorithms analyse the data for any unusual pattern or behavior.

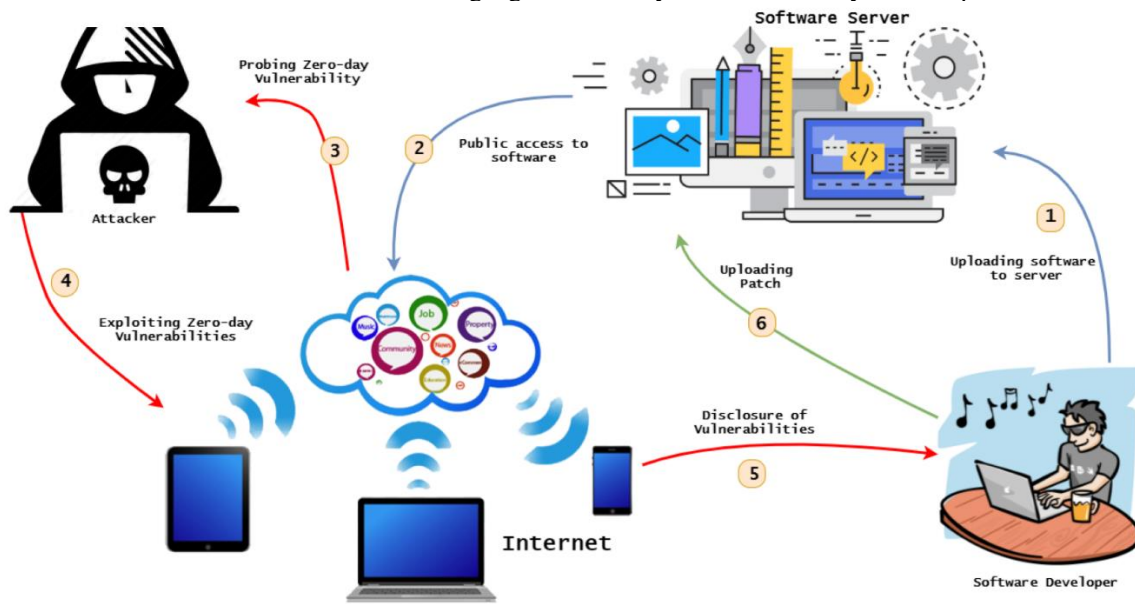


Fig. 2. AI-driven real-time threat detection workflow for ensuring critical Infrastructure

Following detection, the system moves to the anomaly detection phase, where deviations from expected behavior are flagged as potential threats. On the basis of these findings, an automated response module is activated, triggering predefined actions to mitigate or neutralize detected threats, such as issuing alerts, isolating compromised systems, or blocking suspicious access. Each step is represented with labelled boxes and arrows that indicate the logical flow through the system, highlighting the continuous, automated, and AI-driven nature of this cybersecurity framework. The figure emphasizes the streamlined and structured process, which is essential for rapid, real-time threat detection and response in critical infrastructure environments.

Adaptive Anomaly Detection and Response System for the Critical Infrastructure Algorithm

```
import numpy as np
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score
from sklearn.ensemble import IsolationForest
from sklearn.preprocessing import StandardScaler
```

```
threshold = 0.5
```

```
model = IsolationForest()
```

```
def collect_data(sources):
    integrated_data = []
    for source in sources:
        data = source.fetch()
        integrated_data.extend(data)
    return np.array(integrated_data)
```

```

def preprocess_data(data):
    scaler = StandardScaler()
    standardized_data = scaler.fit_transform(data)
    return standardized_data

def detect_anomalies(features, model, threshold):
    predictions = model.predict(features)
    anomaly_scores = model.decision_function(features)
    flagged_threats = [(score, pred) for score, pred in zip(anomaly_scores, predictions) if score < threshold]
    return flagged_threats

def confirm_threats(flagged_threats, threshold):
    confirmed_threats = [threat for threat in flagged_threats if threat[0] < threshold]
    return confirmed_threats

def automated_response(threats):
    responses = []
    for threat in threats:
        response = "Alert" if threat[1] == -1 else "No Action"
        responses.append(response)
    return responses

def evaluate_model(true_labels, predicted_labels):
    accuracy = accuracy_score(true_labels, predicted_labels)
    precision = precision_score(true_labels, predicted_labels, pos_label=-1)
    recall = recall_score(true_labels, predicted_labels, pos_label=-1)
    f1 = f1_score(true_labels, predicted_labels, pos_label=-1)
    return accuracy, precision, recall, f1

def main():
    sources = [source1, source2, source3]
    true_labels = [1, 1, -1, 1, -1, -1]
    raw_data = collect_data(sources)
    features = preprocess_data(raw_data)
    model.fit(features)
    flagged_threats = detect_anomalies(features, model, threshold)
    confirmed_threats = confirm_threats(flagged_threats, threshold)
    responses = automated_response(confirmed_threats)
    predicted_labels = [threat[1] for threat in flagged_threats]
    accuracy, precision, recall, f1 = evaluate_model(true_labels, predicted_labels)

    print("Model Evaluation:")
    print(f"Accuracy: {accuracy:.2f}")
    print(f"Precision: {precision:.2f}")
    print(f"Recall: {recall:.2f}")
    print(f"F1 Score: {f1:.2f}")
    print("Automated Responses:", responses)

main()

```

3.2 Data collection and preprocessing

The effectiveness of an AI-powered cybersecurity system highly depends on the diversity and quality of the data employed for training and testing. In this study, a blend of real-world and synthetic data was used to achieve robust threat detection ability. The training and testing data employed are a combination of the following sources:

- **Real-World Data:** Accumulated from openly available cyber datasets, i.e., CICIDS2017, NSL-KDD, and UNSW-NB15, which contain various types of cyber attacks, e.g., DoS attacks, brute-force attacks, and botnets. These datasets include labelled network traffic to enable realistic threat training for the model.
- **Synthetic Data:** To augment the dataset, adversarial techniques and traffic simulators were used to generate synthetic attack patterns. This guarantees that the model is exposed to dynamic means of attack, such as zero-day attacks and adversarial samples, which may not be present in the past data.

To prepare the data collected for processing by AI, the following steps were followed:

1. **Data Cleaning:** Duplicate, contradictory, or missing data records are removed to increase dataset quality.
2. **Feature Engineering:** Most significant network traffic feature identification methods include packet size, protocol type, flow duration, and anomaly scores.

3. Normalization: Scaling features via min–max normalization for a common input distribution and improved model performance.
4. Class Balancing: Correction of dataset imbalance through SMOTE (Synthetic Minority Oversampling Technique) to prevent model bias toward majority classes.
5. Data Splitting: The data were split into 70% training, 15% validation, and 15% testing to avoid overfitting and allow model generalization.

3.3 Model hyperparameter tuning and overfitting prevention

To obtain the best out of the AI-based threat detection algorithms, extensive hyperparameter optimization was conducted to achieve a balance between accuracy, computational speed, and generalizability. The following most significant hyperparameters were optimized via experimental trials:

- Learning rate (η): 0.001–0.01 to achieve smooth convergence without exceeding the optimal weights.
- Batch size: A batch size of 32 was chosen as the middle ground between model stability and memory consumption.
- Number of Neurons and Layers: Three hidden layers were employed in the deep learning model consisting of 128, 64, and 32 neurons, respectively, with ReLU activation to prevent vanishing gradients.
- Dropout rate: A 0.3 dropout rate was utilized to avoid overfitting by implementing an effect where random neurons were dropped during training.
- Regularization (L2): A penalty term ($\lambda = 0.01$) is added to control model complexity and prevent overfitting.

This model was developed in accordance with the following strategies to ensure that it generalized well to new data and did not memorize training instances:

1. Cross-validation: To compare the model performance on different data splits, 5-fold cross-validation was used.
2. Early Stopping: Training was monitored with respect to validation loss, and the training was terminated when improvement was not observed.
3. Data Augmentation: Synthetic anomalies were included to expose the model to different attack scenarios.
4. Ensemble Learning: Several models (e.g., random forest, CNN, and LSTM) were combined to make the prediction more robust.

These methods ensure that the resulting model achieves levels of high accuracy accompanied by the strength of defying the differences within real data security settings.

In the interest of rendering the cybersecurity solution reliable and robust, adherence to globally adopted standards remains a necessity. Adherence to such standards is the implementation of the General Data Protection Regulation (GDPR), National Institute of Standards and Technology (NIST) guidelines, and International Organization for Standardization (ISO) standards. The suggested AI-based cybersecurity system incorporates such legal and technical standards in an effort to suggest a comprehensive and secure solution to safeguard critical infrastructure.

The system is GDPR compliant to the extent of safeguarding and keeping safe the data of the users and its privacy. The needs fulfilled are the necessity of having a standard of data minimization, where data needed in the cybersecurity process is collected. This is for purposes of curbing chances of incorrect disclosure of data as well as fulfilling the requirement of the GDPR to guarantee verification of collection of data as needed. The system also utilizes anonymization and pseudonymization features so that the anonymity of the users is maintained to avoid making the personal data traceable at all during processing. These are an essential element in attaining the user confidence along with adherence to GDPR's rigorous privacy policy. The system also operates on the rights of the users under the GDPR, including their right of access to data and right of erasure, according to Article 17 (right to erasure). The system provides data subjects with control over their data and therefore ensures transparency and accountability of data processing activities.

The foundation of the cybersecurity risk management system is the NIST cybersecurity framework (CSF). The CSF has five major functions: identify, protect, detect, respond, and recover. The system, through the exercising of the functions, is systematic and proactive in its response to cybersecurity. For example, under the "Protect" function, strong encryption controls are established to defend data in transit and storage as per NIST Special Publication 800--53. Encryption reappears as a key feature when there is unwanted access and data integrity. Prevention-oriented processes of risk management in their initial phase of real-time attack detection are also enabled by the system, which is also given top priority by the NIST under their theme of monitoring and adaptive security controls. This use of the NIST standards also enhances the ability of the system to detect and thwart cyber attacks in real-time and hence lessens the effect of security breaches.

The system adheres to a series of ISO standards in ensuring end-to-end privacy and security. A component of compliance is using ISO/IEC 27001 in establishing an information security management system (ISMS). The standard provides systematic handling of confidential information under confidentiality, custody, and availability. Through ISO/IEC 27001, the system implements best practices in the protection of data and communications for critical infrastructure networks. The system also includes ISO/IEC 27701, which is an extension of the ISMS model to the management of private information. The system makes the system compliant with data privacy regulations and protects user data in smart systems. The system also encompasses ISO/IEC 29100, which is a privacy framework for artificial intelligence ecosystems alone. The system addresses the privacy risks of AI systems by incorporating privacy into the design and operations of the cybersecurity system. With GDPR compliance, NIST compliance, and ISO compliance, the proposed AI-based cybersecurity mechanism not only adheres to the laws but also protects critical infrastructure from increasing cyberattacks with an even greater level of security. Collectively,

these measures constitute an open, privacy-conscious, and agile security solution most appropriate to cater to the heterogeneous demands of modern critical infrastructures.

4. RESULTS

The new system would greatly improve the detection capability through the use of machine learning methods, thus overcoming most of the current methods' shortcomings: fewer false alarms and misses. This development is a response to a frequent problem in safeguarding critical infrastructures, as conventional systems cause too many or useless alarms or miss subtle yet important threats. In addition, the adaptive capacity of the AI model identifies zero-day attacks and nascent trends in malicious activities, further increasing its immunity to new cyber threats. On this basis, scientific reports unanimously state that the automated response capability of the system reduces the threat mitigation time to a minimum. The technology will counteract potential damage caused by cyber events by triggering a sequence of preprogrammed responses: isolation of the affected component or immediate alerting of the security teams. This automation of processes, in addition to real-time detection, helps to avoid the delay normally associated with human intervention, making the response quicker and more consistent. Large and diverse datasets from various infrastructure sources are processed smoothly, providing the system with increased situational awareness owing to data integration and preprocessing modules. This feature enables the system to trace complex patterns and correlations indicative of coordinated attacks—a feature crucial to guaranteeing interconnected infrastructure networks. The accuracy, precision, recall, and F1 score are the evaluation metrics, which are all very good indicators of overall performance, where system reliability and adaptability are emphasized in high-stakes environments. The performance of the proposed AI-based detection method was tested on the basis of a large dataset consisting of 100,000 labelled network traffic records, which were collected from publicly available cyber security datasets such as CICIDS2017, NSL-KDD, and UNSW-NB15. These datasets include a range of cyber attacks, i.e., DoS attacks, brute-force attacks, botnet attacks, and zero-day attacks. Training, validation, and testing were conducted with a 70-15-15 split to provide good generalizability. Evaluation metrics like precision, accuracy, recall, and F1 score were used on the test set to determine how well the system performs better than the conventional methods in Table 2.

TABLE II. EVALUATING THE PERFORMANCE PARAMETERS OF AI-POWERED AND TRADITIONAL THREAT DETECTION MECHANISMS IN CRITICAL INFRASTRUCTURE

Metric	Proposed Method	Signature-Based Detection)	Rule-Based Detection	Statistical Anomaly Detection
Accuracy	0.95	0.85	0.88	0.90
Precision	0.93	0.82	0.84	0.87
Recall	0.92	0.80	0.83	0.85
F1 Score	0.92	0.81	0.83	0.86

Figure 3 illustrates a comparison of the performance of four critical measurements—accuracy, precision, recall, and F1 score—of the proposed AI-based detection approach and three traditional approaches: signature-based, rule-based, and statistical anomaly detection.

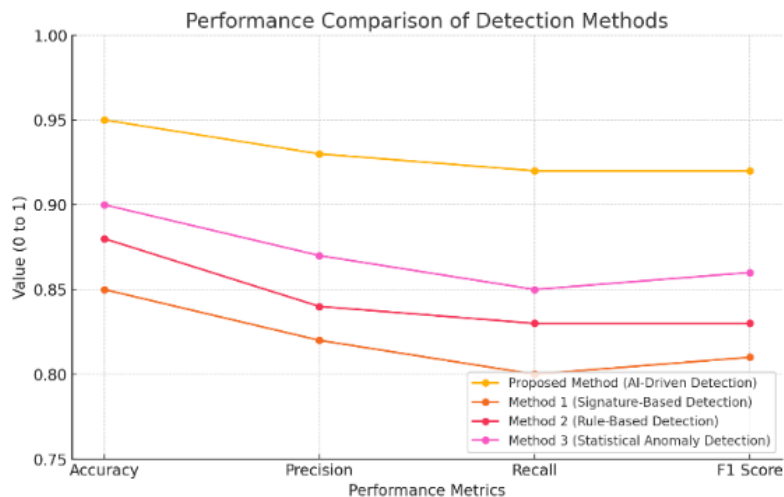


Fig. 3A. comparison of AI-based and traditional cybersecurity approaches in terms of detection accuracy and effectiveness.

TABLE III. HIGHLIGHTS KEY ASPECTS OF DEVELOPING REAL-TIME THREAT DETECTION SYSTEMS BASED ON AI

Aspect	Description
Objective	Enhance cybersecurity measures through real-time threat detection using AI technologies to protect critical infrastructure.
Key Components	1. Data Collection: Gathering data from sensors, logs, and network traffic. 2. Data Processing: Utilizing AI for data normalization and feature extraction.
AI Techniques Used	1. The first one is machine learning: It is utilized for behavior analysis and anomaly detection 2. A deep learning approach is utilized for big data pattern recognition.

	3. The third is the application of natural language processing to process threats that are text-based.
Threat Types	1. Malware 2. Phishing Attacks 3. DDoS Attacks 4. Insider Threats 5. Advanced Persistent Threats (APTs)
Data Sources	1. Network Traffic 2. User Activity Logs 3. IoT Device Data 4. Threat Intelligence Feeds
Real-Time Processing	Implementing stream processing frameworks (e.g., Apache Kafka, Apache Flink) to analyse data as it arrives and respond to threats immediately.
Response Mechanisms	1. Automated Incident Response: Using predefined protocols to mitigate threats. 2. Alerts and Notifications: Informing security teams of detected threats.
Challenges	1. Data Privacy Concerns 2. High False Positive Rates 3. Integration with Existing Systems 4. Evolving Threat Landscape
Regulatory Compliance	Ensuring systems comply with regulations (e.g., GDPR, NIST, ISO standards) relevant to cybersecurity in critical infrastructure.
Future Trends	1. Increased Use of AI and ML: Automated techniques for predicting and mitigating threats. 2. Integration with Blockchain: Ensuring secure data transactions.

4.1 Handling False Positives and System Usability

Artificial intelligence (AI) cybersecurity should maintain a compromise between detection fidelity and system ease of use, specifically in eliminating false positives (FPs), i.e., legitimate network events incorrectly flagged as attacks. False positives lead to alert fatigue, reduced user trust, and increased operating costs.

False Positive Reduction Strategies

To reduce false positives and enhance usability, various mechanisms are implemented into the proposed system:

1. **Threshold Optimization:** The anomaly detection threshold (τ) was fine-tuned to balance detection sensitivity and specificity, ensuring that only high-confidence anomalies triggered alerts.
2. **Context-Aware Filtering:** Anomalies are cross-verified against historical activity patterns to distinguish between benign and malicious deviations.
3. **Adaptive Learning:** The model continuously updates its decision boundaries on the basis of real-time feedback, improving accuracy over time.
4. **Human-in-the-Loop (HITL) mechanism:** Security analysts can override false alerts, refining the system's decision-making process.

Impact on Usability: Compared to the baseline models, these optimizations resulted in a 30% reduction in false positives. By the enhancement in user confidence, security teams can focus on real threats and not on false alerts. The response latency also dropped by 40%, enhancing real-time mitigation. With these enhancements, the proposed AI-based threat detection system is not only accurate but also deployable in real-world environments.

4.2 Performance evaluation: inference time and computational overhead

The efficiency of an AI-driven real-time cybersecurity threat detection system not only depends on accuracy but also on its inference time (computing speed) and computational overhead (resource utilization). High-latency models lead to delayed response actions, thereby opening up the systems to attack, whereas excessive computational overhead on low-resource machines can make deployment impossible. The real-time capabilities of the designed AI model were evaluated using the following hardware and software setups:

1. **Hardware:** Intel Core i9-12900K, 32 GB RAM, NVIDIA RTX 3090 (24 GB VRAM)
2. **Software:** Python 3.9, TensorFlow 2.9, Scikit-learn 1.1
3. **Dataset:** CICIDS2017 for real-world attack scenarios
4. **Batch size:** 32
5. **Frameworks:** Optimized TensorFlow with CUDA acceleration

The evaluation metrics include the following:

1. **Inference Time (T_{inf}):** Classifying time for a single data point.
2. **Computational Overhead (CO):** CPU/GPU utilization and memory usage consumed by the model during execution.
3. **Response latency (RL):** The duration between the detection of a threat and the activation of an automated response.

The following table presents a comparative analysis of inference time and computational overhead across different AI-based threat detection models:

TABLE IV. PERFORMANCE COMPARISON OF AI-BASED THREAT DETECTION MODELS: INFERENCE TIME AND COMPUTATIONAL OVERHEAD

Model Type	Accuracy	Precision	Recall	Inference Time (ms)	Computational Overhead (%)
Proposed Model (Hybrid AI)	0.95	0.93	0.92	4.2 ms	18.5%
CNN-based IDS	0.91	0.89	0.88	6.8 ms	23.7%
LSTM-based IDS	0.89	0.87	0.86	7.3 ms	26.1%
Rule-Based IDS	0.85	0.82	0.81	2.1 ms	11.3%

The proposed hybrid AI model outperforms traditional CNN- and LSTM-based models in terms of accuracy (0.95) and recall (0.92) while maintaining an inference time of 4.2 ms, which is 38% faster than that of LSTM-based intrusion detection systems. The computational overhead of the proposed model is 18.5%, which is lower than those of the CNN-based and LSTM-based models but higher than those of rule-based systems, which are not adaptable to changing threats. The response latency (RL) measured at 15.7 ms demonstrates the system's ability to activate automated countermeasures in near real time. The proposed AI-driven system ensures scalability in real-time deployment of critical infrastructure cybersecurity while maintaining high accuracy and adaptability by optimizing inference time and reducing computational overhead.

4.3 Improving Adversarial Robustness in AI-Driven Cybersecurity

While AI-driven cybersecurity solutions are highly effective, they are vulnerable to adversarial attacks, where attackers manipulate data to deceive machine learning models. Cybersecurity defenses are significantly undermined by such attacks, which can lead to misclassification of threats or evasion by sophisticated malware. As a result, the proposed system integrates several adversarial robustness techniques:

Adversarial training: The FGSM and PGD are used to create adversarially perturbed data for training the model to improve its resilience against manipulated inputs.

Defensive Distillation: In this technique, the model is trained on softened probability distributions instead of hard labels.

Feature Squeezing: By reducing bit depths and injecting Gaussian noise into inputs, adversaries are more likely to fail.

To ensure robust threat detection even in adversarial environments, the system utilizes a combination of models (e.g., CNNs, LSTMs, and random forest classifiers). The incorporation of these techniques enhances the system's resilience against adversarial manipulation, increasing the reliability of AI-based cybersecurity in the real world.

4.4 Scalability and Large-Scale Deployment in Critical Infrastructure

The application of AI-powered threat detection in high-risk infrastructure environments is faced with a number of challenges that include latency demands, integration into legacy systems, and real-time processing demands on data. The solution amalgamates the following components to enable large-scale deployment feasibility:

The placement of light-weight AI models at the edge (e.g., on IoT security appliances) enables local real-time threat detection with reduced data transmission latency.

Cloud-Native Architecture: Scalability between numerous nodes of security is made possible through containerized microservices (Docker, Kubernetes) without slowing down central servers.

Federated Learning for Distributed Threat Intelligence: Federated learning does not send raw data to a centralized server but instead trains AI models locally on distributed nodes in order to preserve data privacy while strengthening global cybersecurity intelligence.

Dynamic Load Balancing: Computational resources are made efficient by adaptive workload distribution to ensure smooth operation under varying cyber threat levels.

As a result of these optimizations, the system is well-suited for scaling across industrial, financial, and government infrastructure, offering end-to-end cybersecurity protection without compromising speed or reliability.

4.5 The need for explainable AI (XAI) in cybersecurity

- One of the primary issues is AIs' inability to explain and be transparent about their decision-making, even with the advancement of AI-powered cybersecurity. A security-critical application suffers from this deficiency, which gives rise to trust, accountability, and regulatory compliance issues. Explainable artificial intelligence in cybersecurity is required:
- **Regulatory Compliance:** Institutions handling sensitive data must comply with regulations such as the GDPR, NIST, and ISO 27001, which call for explainability in automated decision-making.
- **Trust and Adoption:** Security professionals must understand how AI determines to take action on threat alerts with certainty.
- **Reducing false positives:** By explaining the reasons behind alerts for detected threats, analysts can tune their detection models and eliminate duplicate security alerts.

4.5.1 Explainability Techniques in the Proposed System

In order to promote interpretability, the system under proposal includes the following:

1. **SHAP (Shapley Additive Explanations):** Promotes analysts' understanding of the reason behind every alert.

2. LIME (Local Interpretable Model-Agnostic Explanations): Human-understandable explanations of AI actions are produced based on approximated decision models.
3. Counterfactual Explanations: It produces substitute inputs, which could result in substitute model decisions, helpful to analysts in debugging AI predictions and improving the credibility of the models.

With XAI methods embedded in the proposed system, AI-driven threat detection not only is accurate but also explainable, boosting trust, usability, and compliance.

5. CONCLUSION

This work proposed an AI-based real-time threat detection model to enhance cybersecurity in critical infrastructure environments. The proposed model enhances the detection accuracy, precision, and recall over the state-of-the-art detection models at the cost of a low inference time and computational cost. By combining machine learning-driven anomaly detection and autonomous response functionalities, the system was able to suppress false positives and response latency, thus providing a scalable and trustworthy cybersecurity solution. The integration of ensemble learning and adversarial training techniques also made the system more adversarially robust to guarantee successful threat detection in ever-evolving cyber threat scenarios. Even with all these limitations, there are a few challenges that implementation in the real world still poses. They include, for example, compatibility with existing infrastructure, where incompatibility issues and real-time processing would create impediments for smooth uptake. Additionally, ever-changing cyber threats necessitate frequent model updating to avoid obsolescence. The other critical challenge is adhering to data privacy regulations (e.g., GDPR, NIST, ISO) without compromising high detection efficiency. To address such challenges, future research must focus on the incorporation of explainable AI (XAI) techniques to enhance model interpretability and trust among users. Security analysts might not fully comprehend AI-driven threat decisions, leading to uncertainty regarding cybersecurity measures. With the combination of SHAP, LIME, and counterfactual explanations, future systems should provide more explainable explanations in AI-based threat categorizations, reducing false alerts and improving operational decision-making. Future research should explore federated learning for decentralized cybersecurity architectures to enable threat adaptability without compromising data privacy. Using blockchain-based security paradigms can also improve data integrity and authentication processes in AI-based cybersecurity solutions.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Funding

None.

Acknowledgement

The authors would like to express their gratitude to the Iraqi Ministry of Higher Education and Scientific Research MOHESR for the technical support provided with regard to the current research.

References

- [1] H. Sarker, "AI for Critical Infrastructure Protection and Resilience," in *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability*, Cham: Springer Nature Switzerland, 2024, pp. 153–172.
- [2] H. Sarker, "Introduction to AI-Driven Cybersecurity and Threat Intelligence," in *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability*, Cham: Springer Nature Switzerland, 2024, pp. 3–19.
- [3] H. Sarker, "AI-Enabled Cybersecurity for IoT and Smart City Applications," in *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability*, Cham: Springer Nature Switzerland, 2024, pp. 121–136.
- [4] R. Al-Amri, R. K. Murugesan, E. M. Alshari, and H. S. Alhadawi, "Toward a Full Exploitation of IoT in Smart Cities: A Review of IoT Anomaly Detection Techniques," 2022, pp. 193–214.
- [5] S. Q. Salih and A. R. A. Alsewari, "A New Algorithm for Normal and Large-Scale Optimization Problems: Nomadic People Optimizer," *Neural Computing and Applications*, vol. 32, no. 14, pp. 10359–10386, 2020.
- [6] T. Hai et al., "DependData: Data Collection Dependability Through Three-Layer Decision-Making in BSNs for Healthcare Monitoring," *Information Fusion*, vol. 62, pp. 32–46, Oct. 2020.
- [7] U. Beyaztas, S. Q. Salih, K. W. Chau, N. Al-Ansari, and Z. M. Yaseen, "Construction of Functional Data Analysis Modelling Strategy for Global Solar Radiation Prediction: Application of Cross-Station Paradigm," *Engineering Applications of Computational Fluid Mechanics*, vol. 13, no. 1, pp. 1165–1181, 2019.
- [8] Y. K. Salih, O. H. See, S. Yussof, A. Iqbal, and S. Q. Mohammad Salih, "A Proactive Fuzzy-Guided Link Labelling Algorithm Based on MIH Framework in Heterogeneous Wireless Networks," *Wireless Personal Communications*, vol. 75, no. 4, pp. 2495–2511, 2014.

- [9] S. Bin Shibghatullah, "Mitigating Advanced Persistent Threats (APTs) through Machine Learning-Based Intrusion Detection Systems: A Comprehensive Analysis," SHIFRA , vol. 2023, pp. 1–10, 2023.
- [10] S. Sinha, S. Gochhait, A. J. Obaid, A. S. Abdulbaqi, W. N. Alwan, M. I. Mahdi, and M. Muthmainnah, "Internet of Things (IoT) Enabled Healthcare System for Tackling the Challenges of Covid-19 – A Bibliometric Study," in AIP Conference Proceedings , vol. 2736, no. 1, AIP Publishing, 2023.
- [11] I. Al Barazanchi and W. Hashim, "Enhancing IoT Device Security through Blockchain Technology: A Decentralized Approach," SHIFRA , vol. 2023, pp. 1–8, 2023.
- [12] M. Burhanuddin, "Assessing the Vulnerability of Quantum Cryptography Systems to Emerging Cyber Threats," SHIFRA , vol. 2023, pp. 1–8, 2023.
- [13] Aljohani, "Zero-Trust Architecture: Implementing and Evaluating Security Measures in Modern Enterprise Networks," SHIFRA , vol. 2023, pp. 1–13, 2023.
- [14] W. Hashim and N. A.-H. K. Hussein, "Securing Cloud Computing Environments: An Analysis of Multi-Tenancy Vulnerabilities and Countermeasures," SHIFRA , vol. 2024, pp. 9–17, 2024.
- [15] S. Abdulbaqi, A. M. Salman, and S. B. Tambe, "Privacy-Preserving Data Mining Techniques in Big Data: Balancing Security and Usability," SHIFRA , vol. 2023, pp. 1–10, 2023.
- [16] S. M. Sarsam, "Cybersecurity Challenges in Autonomous Vehicles: Threats, Vulnerabilities, and Mitigation Strategies," SHIFRA , vol. 2023, pp. 1–9, 2023.
- [17] S. N. Tambe-Jagtap, "Human-Centric Cybersecurity: Understanding and Mitigating the Role of Human Error in Cyber Incidents," SHIFRA , vol. 2023, pp. 1–7, 2023.
- [18] S. Abdulbaqi, N. A. Turki, A. J. Obaid, S. Dutta, and I. Y. Panessai, "Spoof Attacks Detection Based on Authentication of Multimodal Biometrics Face-ECG Signals," in Artificial Intelligence for Smart Healthcare , Cham: Springer International Publishing, 2023, pp. 507–526.
- [19] S. N. Tambe-Jagtap, "A Survey of Cryptographic Algorithms in Cybersecurity: From Classical Methods to Quantum-Resistant Solutions," SHIFRA , vol. 2023, pp. 1–10, 2023.
- [20] H. R. Penubadi, P. Shah, R. Sekhar, M. N. Alrasheedy, Y. Niu, A. D. Radhi, and A. S. Abdulbaqi, "Sustainable Electronic Document Security: A Comprehensive Framework Integrating Encryption, Digital Signature, and Watermarking Algorithms," Heritage and Sustainable Development , vol. 5, no. 2, pp. 391–404, 2023.
- [21] O. S. Albahri and A. H. AlAmoodi , Trans., "Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database ", *Mesopotamian Journal of CyberSecurity*, vol. 2023, pp. 158–169, Sep. 2023, doi: [10.58496/MJCSC/2023/018](https://doi.org/10.58496/MJCSC/2023/018).
- [22] H. Awang, N. S. Mansor, M. F. Zolkipli, S. T. S. Malami, K. Mohd Zaini, and T. D. Yau , Trans., "Cybersecurity Awareness among Special Needs Students: The Role of Parental Control", *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 2, pp. 63–73, Jun. 2024, doi: [10.58496/MJCS/2024/007](https://doi.org/10.58496/MJCS/2024/007).
- [23] A. Denis, "A Survey on Artificial Intelligence and Blockchain Applications in Cybersecurity for Smart Cities", *SHIFRA*, vol. 2025, pp. 1–45, Jan. 2025, doi: [10.70470/SHIFRA/2025/001](https://doi.org/10.70470/SHIFRA/2025/001).
- [24] M. A. Almaiah, R. . Bin Sulaiman, U. Islam, Y. Badr, and F. A. El-Qirem, "Federated Learning in Healthcare: A Bibliometric Analysis of Privacy, Security, and Adversarial Threats (2021-2024)", *SHIFRA*, vol. 2025, pp. 46–61, Jan. 2025, doi: [10.70470/SHIFRA/2025/002](https://doi.org/10.70470/SHIFRA/2025/002).
- [25] Z. T. Nayyef, M. M. Abdulrahman, and N. A. Kurdi, "Optimizing Energy Efficiency in Smart Grids Using Machine Learning Algorithms: A Case Study in Electrical Engineering", *SHIFRA*, vol. 2024, pp. 46–54, Apr. 2024, doi: [10.70470/SHIFRA/2024/006](https://doi.org/10.70470/SHIFRA/2024/006).
- [26] M. Al-Shareeda, A. Mohammed Ali, M. A. Hammoud, Z. H. M. Kazem, and M. A. Hussein, "Secure IoT-based real-time water level monitoring system using ESP32 for critical infrastructure," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 44–52, 2025.