Journal of Computer Science

Review Article

A Succinct Review on Identification of Network Anomalies and Protection in Cyber-Physical Systems

[1]Shalini Kumari, [1]Chander Prabha, [2]Prakash Srivastava, [3]Zeba Khan, [4]Nadim Rana and [5]Mohammad Zubair Khan

[1]Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India
[2]Department of Computer Science and Engineering, Graphic Era (Deemed to be University), Dehradun, India
[3]Department of Computer and Information, Applied College, Jazan University, Jazan, Saudi Arabia
[4]Department of Computer Science, College of Engineering and Computer Science, Jazan University, Jazan, Saudi Arabia
[5]Department of Computer Science and Information, Taibah University, Madinah, Saudi Arabia

Article history
Received: 06-11-2024
Revised: 26-12-2025
Accepted: 27-02-2025

Corresponding Author:
Chander Prabha
Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India
Email: prabhanice@gmail.com

Abstract: Advanced cyberattacks outperform traditional threat detection methods in the rapidly expanding cybersecurity field. Advanced Machine Learning (ML) algorithms can detect network traffic and system problems using AI-based Anomaly Detection (AD) for cybersecurity in real-time. Signature-based systems may overlook new and subtle threats. This paper examines Artificial Intelligence (AI) driven AD systems' design, methodology, and efficacy. The process includes data preprocessing and feature extraction. Unsupervised learning and real-time data streams can detect insider threats and zero-day attacks without attack signature information-AI-based cybersecurity AD strengths and downsides. According to numerous research and trials, its high accuracy and memory in detecting anomalies reduce false positives compared to older methods. Cyber attackers use protected channels to launch attacks. Cryptographic channels obscure legal and malicious network traffic. Alternative studies use AI and traffic information to discover anomalies. Integrating AI, blockchain, and Quantum Computing (QC) can boost cybersecurity. According to research, growing cyber risks require adaptive, scalable, and intelligent AI-powered cybersecurity solutions. Deep generative models can detect novel cyber-physical dangers and minimize Cyber Physical System (CPS) susceptibility without labelled information.

Keywords: Cybersecurity, Anomaly, Artificial Intelligence, Machine Learning, Internet Traffic

Introduction

Humayed *et al.* (2017) have shown that smart manufacturing, electricity grids, and transportation use Cyber-Physical Systems (CPSs) in Industry 4.0. Rich networked actuators and sensors connect a computer, networking, and physical environments in multidimensional CPSs in Industry 4.0. AD is a potential way to monitor CPSs and notify them instantly if abnormalities are identified. Kwon *et al.* (2019) introduced abnormal behaviours, known as anomalies, contamination, intrusions, outliers, or failures, that depart from normal data distribution in diverse applications. Choi *et al.* (2019) introduced that unsupervised learning is preferable to inherent labelling for AD because it is difficult, time-consuming, and often impossible. Li and Wen (2014) introduced the idea that transformation-based unsupervised algorithms struggle with multivariate time series with inherent correlation and nonlinearity. The conventional Internet was vulnerable to sniffing and spoofing attacks using Transmission Control Protocol/Internet Protocol (TCP/IP). With time, the Internet has shared more sensitive corporate and intellectual property data. As TCP and IP do not default to encryption, attackers can steal data or change packets. Due to security risks, Transport Layer Security (TLS) protects internet communication. Contrary to expectations, encrypted Internet traffic is rising. Cyber attackers employ encrypted channels. An encrypted attack survey found 57% in 2020, 80% in 2021, and above 85% in 2022.

Wang *et al.* (2017) introduced the Deep Packet Inspection (DPI) in the packet attack detection environment needs updation. Analyzing plaintext and

packet payload data can detect network traffic anomalies. Van Ede *et al.* (2020) use key data in packets to detect abnormalities. However, it cannot be used on encrypted communication because it uses payload data. Today's digital world sees more and more cyberattacks. Conventional signature-based cybersecurity methods cannot adapt to changing threats.

Traditional techniques assess threats reactively based on attack patterns. Advanced persistent attacks and zero-day exploits are difficult to detect. High-performance ML algorithms for identifying abnormal behaviour analyze vast amounts of realtime data. Even without symptoms, our proactive method detects unusual cyber-attack patterns. AI anomaly detection requires ongoing learning and adaptability. ML models can identify network or system activity with the help of large datasets. These skilled models can identify anomalies in realtime data. The dynamic adaptability of this system helps detect zero-day attacks and insider threats that standard methods overlook.

Chandola *et al.* (2009) employ the ideas of feature extraction, data preprocessing, and ML techniques like Clustering, SVMs, and neural networks. AI-based systems can protect against cyberattacks by combining these elements.

This research addresses AI-based AD challenges like huge datasets, processing costs, and adversarial attack sensitivity. Case studies and experiments examine these strategy's pros, cons, and mitigation techniques.

Vyas (2023) introduced the study that AI enhances real-time cybersecurity. Innovative and integrated technology is needed to create intelligent, scalable, and flexible cybersecurity systems. AI-based AD protects digital infrastructures from rising cyber threats. Table (1) presents the DL-AD taxonomy for CPS.

Table 1: Cyber-physical system, Deep learning, AD Taxonomy

Types	Description
Types of Anomalies	Attacks: network communication layer Faults: Control system
Strategies for detection	Data inputs include time-series data, network traffic data, sensor and actuator data, and system calls and logs.
	Design of neural networks: RNN, CNN, GAN, etc., personalized models.
	Scores for anomalies: Errors in prediction, reconstruction, and predicted label

CNN in Table (1) stands for Convolutional Neural Network and is typically used in image and video recognition tasks. It is mainly perfect for identifying patterns and features inside an image.

RNN in Table (1) stands for Recurrent Neural Network; this is a kind of neural network suited particularly to linear data like time series data or natural language; they have a "memory" component, so they can process information in sequence while keeping context.

A neural network used for generative tasks, like creating new images, videos, or text, is called a Generative Adversarial Network (GAN). The discriminator network, which seeks to separate the new data from the real one, and the generator network, which creates the new data, are the two main parts of a GAN. The generator creates the data to deceive the discriminator during their joint training.

Attacks in CPS

CPSs are always at risk of attacks since they run essential infrastructure, including ICS, medical equipment, and power grids. Financial interest, privacy theft, and governmental activity can motivate an attacker. These kinds of attacks can target several CPS parts.

First Part- Layer of network communication: Field devices like actuators and sensors communicate via communication networks. Additionally, data centres receive sensor values and device status, while control systems send commands via the network. Level 0 ($C0$) and 1 ($C1$) communication can be addressed here. These attacks can also alter $S2$, $A2$, and $D1$ (in $C0$ and $C1$ traffic). Further, there are three types of attacks:

- Denial-of-Service (DoS) attacks: Applications for real-time cyber-physical systems are at risk from DoS attacks. Aircraft collisions or inefficient traffic use could result from the lack of ADS-B technology. However, the broadcast function of CPS communication protocols, such as the CAN protocol used in smart car systems, leaves the network open to DoS attacks
- Attacks that involve a Man-In-The-Middle (MITM): Many emerging protocols in CPSs may lack a robust authentication method. CPS Ethernet can be utilized for MITM attacks. Packet content can be changed, and MITM attacks can disclose sensitive data
- Injecting packets: Attackers with network access can inject random packets to give control commands. When given erroneous control commands, operating devices can cause catastrophic damage and even death. An accident may result if the driver commands the engine and brakes incorrectly

Second Part- System for Control: The core of CPSs is control systems, which use sensor data to communicate with actuators or field equipment. Control systems might not have clear protection mechanisms because of harsh operating conditions or insufficient hardware resources. Actuator commands ($A2$) and SCADA data ($D1$) can be altered if control systems are compromised. SCADA stands for Supervisory Control and Data Acquisition. Equipment that handles important and time-sensitive materials or events can be monitored and controlled thanks to this computer-based system that is made to

gather and analyze data in real time. CPS targets two types of attacks:

- Malware: Attackers use malware in control systems to monitor and disclose information over time. Additionally, malware can launch stealthy attacks (e.g., APT) at vital moments. Malware can distort sensor readings. Malware may cause physical damage to gadgets in rare cases
- Fake control signals: Devices may act differently than normal when receiving erroneous control signals. Incorrect operations can damage equipment and reduce its lifespan. Hackers often hide unauthorized access and transmit fake control commands at vital times

Third-Party Faults: Complex systems and diverse components might cause unanticipated problems in CPSs. Usually, flaws occur in two layers:

- Sensor layer: False sensor values are common sensor layer faults. Damage or flaws might cause sensors to produce erroneous values. Previously unknown events may force sensors to function above their capabilities. Sensors on spacecraft may encounter unexpected situations
- Control system: CPSs are characteristically dynamic, resulting in unanticipated scenarios during system design. Different event sequences and timings in PLC code can lead to assembly line collisions in industrial operations

Strategies for Anomaly Detection

Deep Learning-based Anomaly Detection (DLAD) algorithms are developed considering three key aspects.

Input data: DLAD techniques identify anomalies and decide the input data type. The layer and data collection method help identify four input data types. Sensors and actuators' data, time-series data in numerical form, including preprocessed sensor, network, and log data; data on network traffic, system calls and logs; Using semi-supervised and unsupervised learning, DLAD methods handle unlabeled data, especially anomalous data.

Neural network design: DLAD employs several neural network architectures based on tasks and input data. Deep networks—that which Broadbent and Schaffner (2016) refer to as either hybrid combinations (e.g., LSTMCNN) or stacked models (e.g., LSTMS). There are several neural network designs, but we found three fundamental ideas for creating them. First, time-series data is often analyzed using LSTM models—a type of RNN. Second, an autoencoder allows unsupervised learning and addresses distorted data. Third, CNN models can spot context and correlations in multivariate measurement data.

Anomaly scores: There are three steps to gauge the detection mistake. First, there is a prediction error since the deep learning AD method forecasts sensor or actuator values using past data. It gauges the difference between the expected and actual values. Sometimes, projected values differ from anomalous data. Second, Reconstruction errors; the model represents a low-dimensional space by compressing input data into hidden layers. After that, the data is rebuilt to its natural scale. One finds the same error between reconstructed and original values. Usually, one uses a threshold of error to identify aberrant data. Third is a label/class prediction; if labelled data is sufficient in a domain, say the SWaT testbed in ICS, then DLAD models may predict input data labels. The concept is to find anomalies using latent features from neural networks. There are a few ways to adopt this architecture since great manual work is needed to identify large volumes of data.

Types of Anomaly Detection

AD finds expected data patterns. Anomalies are data points that significantly deviate from the dataset in statistical analysis for AD. There are three types of anomalies in Figure (1).

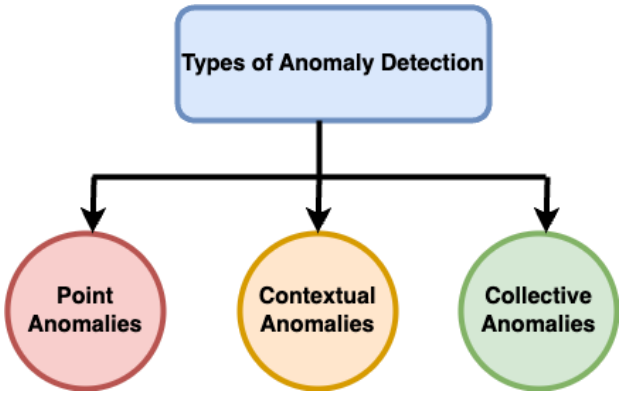

Fig. 1: Types of anomalies

Point Anomalies: Outliers refer to individual data points that deviate significantly from the remaining data.

Contextual Anomalies: Anomalous data instances that deviate from the norm within a particular context but do not exhibit such deviations in other contexts.

Collective Anomalies: A set of linked data points that, taken together, deviate from normal.

Machine Learning Algorithms

Inoue *et al.* (2017) proposed several multiple-learning algorithms for AD. Their learning paradigms help to classify these algorithms. Figure (2) presents several kinds of learning methods.

Supervised ML train models to identify data points as normal or aberrant using annotated datasets. One finds the inclusion of algorithms, including neural networks, SVMs, and decision trees. Approaches of supervised learning provide consistent and quick results. Build AD models with annotated data. Still, much-annotated

training data is needed, including rare and diverse aberrations.

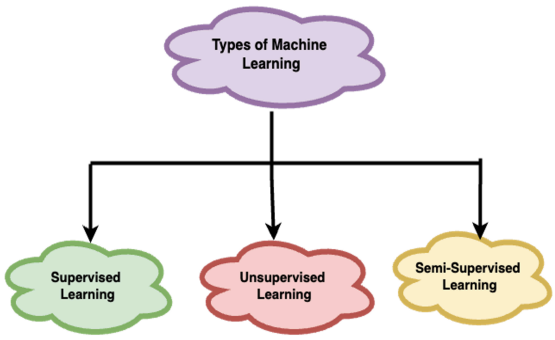

Fig. 2: Types of learning

Unsupervised ML: Unsupervised learning methods to find anomalies without labelled data using inherent patterns and structural identification in data. The techniques used are Principal Component Analysis

(PCA), Isolation Forests (IF), Clustering using KMeans and DBSCAN. Unsupervised learning methods are useful when there is a lack of labelled data since they allow one to identify anomalies in CPS with limited training data. However, people may find it difficult to differentiate between harmless abnormalities and real hazards, leading to higher rates of inaccurate positive identifications.

Semi-Supervised ML: Training models through this method requires limited labelled data and large amounts of unlabeled data. Using this approach yields benefits for situations that involve costly or timeconsuming data labelling processes. Semi-supervised learning strategies provide a solution to link data sets with different labelling levels. They are ideal for detecting anomalies in CPS with minimal labelled data. However, optimizing hyperparameters and model topologies may require significant modification. Table (2) presents some common algorithms that are part of these techniques.

Supervised learning, such as distribution and regression, is widely used when the target is known. Unsupervised learning analyses data and patterns such as clusters and associations. Semi-supervised learning acts as a bridge, taking advantage of both methods, especially in environments where labelled data is limited.

Table 2: ML Algorithm used

Learning Type	Summary	Common Algorithms Used
Supervised	The training process takes place through models that process textual information while each input receives a specific outcome. The learning process enables the model to make predictions after reviewing simulated data entries	Classification: The classifiers implemented in the research included Support Vector Machines (SVM) together with logistic regression and decision trees. Regression: Linear regression, polynomial regression, ridge regression
Unsupervised	It involves training models with unknown data, allowing the algorithm to find patterns and relationships without guidance	Clustering: K-means, clustering process Partial reduction: Principal Component Analysis (PCA), autoencoders Links: Apriori Algorithm, Eclat Algorithm
Semi-Supervised	It combines labelled and unlabeled data for training. It is very useful if it is too expensive or inconvenient to get a well-labeled data feature	Algorithms can be a combination of supervised and unsupervised methods, such as using a small labeled dataset to train a model and then using it on a larger unlabeled dataset to generate false labels

Literature Review

AI-based AD in cybersecurity has been studied for a decade. This literature review discusses AD, cybersecurity ML algorithms, and realtime threat detection.

Evolution of Anomaly Detection Technique: The initial AD methods used statistics and rule-based systems.

Network behaviour comprehension came from Threshold-based detection and statistical profiling, although these methods could not find advanced threats. The AD strategy development is studied using the Bui *et al.* (2021) concept by comparing simple statistical approaches and advanced ML.

Cybersecurity in Machine Learning: The evolution of cybersecurity has been radically transformed through machines that process data for hazardous activity trend identification. The analysis of AD has included evaluation with neural networks, SVMs, and decision trees. Scientists have completed extensive research to show how clustering and Principal Component Analysis (PCA) in unsupervised learning detect irregular patterns in untagged information. A recent study by Jain *et al.* (2023) proved that Hidden Markov Models (HMMs) succeed in detecting network intrusions when researchers focus on time-based data analysis in AD.

Anomaly detection in real-time: Continuous data flows are processed by streaming algorithms for real-time detection. Examine real-time data mining, threat detection, and response. Biggio and Roli (2018) use the concept of AD systems that may leverage live learning and incremental ML model changes to respond quickly to new threats.

Performance and Issues: AI anomaly detection accurately detects known and unexpected threats. AI-based network AD solutions outperformed traditional methods. AI has challenges like huge datasets, computational resources for real-time analysis, and adversarial attacks. Adversarial Machine Learning

(AML) manipulates input data to avoid detection systems.

Applications and Case Studies: Many cybersecurity case studies show AI-based AD applicability. Intrusion Detection (ID) using DL models in Industrial Control Systems (ICS) has shown promise. Detected ICS anomalies with high accuracy and low false positives using a Deep Neural Network (DNN). Sahay and Sinha (2018) discussed that reinforcement learning in adaptive cybersecurity helps AI improve autonomous threat mitigation.

Comparative Analysis

AI-based AD systems are compared to traditional and alternative AI-driven methods. This analysis emphasizes detection accuracy, realtime processing, adaptability, computational efficiency, and adversarial attack resistance (Figs. 3-4). Table (3) shows the comparative analysis of traditional and AI-based AD methods.

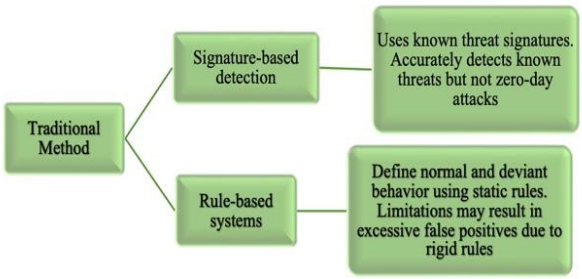

Fig. 3: Traditional AD methods

Table 3: Comparative analysis of traditional and AI-based methods

Standard	Method	Description	Performance
Processing Real Time	Traditional Methods	Efficient for realtime processing but may not react to new threats due to established signatures and criteria	High for recognized threats
	AI-Based Methods	Stream Processing Frameworks (e.g. Kafka, Flink): Enable realtime data ingestion and analysis for rapid threat detection by Vyas (2022)	Elevated for both identified and unidentified hazards. The performance of the system varies, with high performance observed when using stream processing and lesser performance observed when using batch learning
		Online learning models achieve high-performance outcomes through the incremental addition of fresh data.	
		Batch Learning Models: Retrain the entire dataset, rendering them unsuitable for realtime processing	
Adaptability	Traditional Methods	Maintaining efficacy against new threats requires regular upgrades and human interaction.	Low
	AI-Based Methods	Unsupervised and Semi-Supervised Learning: Benefit from adaptability to new data, making them ideal for dynamic contexts	Unsupervised or semi-supervised learning, particularly at a high level
		Reinforcement Learning: Highly adaptable and requires a robust framework for implementation after continuous improvement through environmental interaction	
Adversarial Attack Resilience	Traditional Methods	They are vulnerable to evasion strategies because attackers can change their behaviour to escape detection by specified rules and signatures	Low
	AI-Based Methods	AI models face an increasing security threat because attackers pursue methods to manipulate their operation. Researchers establish defensive model structures together with adversarial training procedures to counter these vulnerability risks.	Enhancing (using adversarial training and robust techniques)
		To improve AI models' robustness, consider employing ensemble approaches and anomaly score calibration to reduce vulnerability to adversarial attacks	

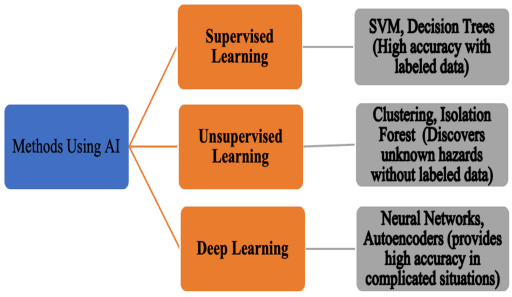

Fig. 4: AI AD methods

The study demonstrates how AI-based AD systems create better real-time cybersecurity through their advantages in system operation. Although traditional methods are simple and efficient in dealing with familiar threats, AI-driven alternatives offer greater adaptability and accuracy, particularly in identifying new and complex attacks. Nevertheless, the processing requirements and ability to withstand adversarial attacks are crucial factors when implementing AI-powered systems. Ensuring a harmonious equilibrium of these aspects is crucial for creating resilient, instantaneous cybersecurity solutions. To improve the analysis of the

article on AD in CPS, various unique perspectives could be incorporated:

- Comparative Analysis of Techniques: A thorough comparison of different AD techniques, including traditional statistical and advanced ML approaches, could shed light on their unique strengths and weaknesses. This would help to contextualize the methodologies discussed and emphasize situations where one approach might be more effective than the other
- Real-World Case Studies: Including real-world case studies highlighting various AD methods across different industries could enhance the discussion. This approach would illustrate the practical implications of the findings and reveal the challenges encountered during real-time implementations
- Interdisciplinary Approaches: Examining how interdisciplinary methods, like combining AI with blockchain and quantum computing, can improve cybersecurity measures would provide a progressive viewpoint. This could showcase creative solutions to the existing challenges in AD systems
- Focus on Interpretability: It is essential to address the interpretability of DL-based AD methods. Exploring how improving interpretability can foster greater user trust and encourage system adoption would offer an important perspective on the limitations of existing models

Network Security Advancements

More recent research has been conducted on network security utilizing new technologies. Cyber threat detection and mitigation are promising with neural network architectures, as stated by Parsamehr *et al.* (2019). Neural networks' ability to recognize complex patterns and behaviours from massive data sources may improve Intrusion Detection Systems (IDS) and prevent network attacks, as shown in Table (4).

Methodology

Real-time cybersecurity implementation of AI-based anomaly detection requires data collection, preprocessing, and feature extraction before selecting and training a real-time model for real-time detection, which would be evaluated and deployed. All stages were created to enhance system performance for threat detection and response in cybersecurity. Figure (5) shows the methodology's steps.

Fig. 5: Flow Diagram

Table 4: Mechanism for network attack prevention

Reference	Prevention Network Attacks	Description
Kumari and Prabha (2024)	Deep Learning	Deep Learning (DL) has improved cybersecurity by making AD systems more flexible. DNNs and DBNs are useful for detecting network traffic irregularities and intrusions because they can evaluate complex, high-dimensional data. Automatically learning hierarchical data representations to capture complex links and dependencies helps DL models detect cyber threats more accurately and robustly
Verkerken (2022)	Generalization and Scalability	Neural networks (NNs) can scale and generalize to huge data volumes and diverse network environments. Unlike signature-based detection methods, neural networks can learn from data and apply their experience to new circumstances. Because they adapt and evolve, neural network-based IDSs can identify complex cyber threats like zeroday exploits and polymorphic malware
Geller *et al.* (2014)	Hybrid ethods	Besides NN models, hybrid systems combining many detection methods are gaining popularity. Hybrid Intrusion Detection Systems (HIDSs) combine NNs, rule-based systems, anomaly-based methods, and ensemble learning to maximize their benefits and minimize their drawbacks. A HIDS can use an NN to detect anomalies and rule-based filters to verify and improve results. This reduces false positives and improves detection accuracy
Anitha *et al.* (2023)	Realtime Detection	Realtime cyber threats demand fast detection and response to adapt to shifting tactics and limit impact. Near-real-time threat detection with neural network-based IDSs prevents security incidents. Realtime network traffic monitoring and analysis allows neural network-based IDSs to detect potential attacks and take immediate action to mitigate them
Vasa (2022)	Limitations and Issues	Cybersecurity is possible with neural network-based IDSs, but they must overcome obstacles. Comprehending their conclusions is difficult because neural network models are opaque, especially in deep neural networks. Explainability is crucial for decision-making and accountability. Therefore, the incapacity of neural network-based IDSs to be applied in real life hinders their acceptance
Nagaraj *et al.* (2023)	Security and Robustness	Neural network model flaws allow adversaries to change or escape detection, limiting IDS efficacy. Researchers are studying adversarial training and defence mechanisms to strengthen neural network-based IDSs. To prevent unauthorized access, carefully assess the privacy and security of important neural network model training data

Data Collection: The initial phase involves collecting varied datasets to identify normal and abnormal network dynamics.

Data Preprocessing: Effective data preparation ensures data quality and consistency. It includes:

- Data Cleaning: Remove noise, handle missing numbers, and fix errors
- Normalization: Scaling data for comparability across features
- Segmentation: Breaking down continuous data streams into manageable sessions

Feature Extraction: The ability to effectively extract features is crucial for revealing meaningful patterns:

- Metrics like frequency, standard deviation, and mean are calculated and stored in the statistical features
- Time-series analysis involves collecting data over a period of time and then identifying patterns, trends, and outliers
- Deriving relevant characteristics from domain-specific information involves understanding network protocols and user behaviours

Model Selection and Training: Training and selecting suitable algorithms requires optimal performance from ML models because model selection and training need proper algorithm selection and optimization. Neural Networks, Support Vector Machines, K-means clustering, and Isolation Forests form the core group of ML methods, which receive evaluation consistent with data type and detection targets. The process of both model selection and training relies critically on the distinct separation of the dataset between training and validation groups. The process of model parameter enhancement through grid or random searches defines hyperparameter tuning.

Evaluation: The accuracy of the AD system relies on regular performance evaluations. The model's efficacy is evaluated by calculating measures including recall, accuracy, precision, F1 score, and area under the curve (AUC-ROC). The benchmarking process involves comparing the system to existing benchmarks and other systems that detect anomalies. Identifying and analyzing false positives and negatives is necessary to improve the models and decrease errors.

Performance evaluation metrics: Comparing the attack dataset input features to outputs validates the trained model. Accuracy, precision, recall, F1 score, and true positives and negatives are used to evaluate the model. Ji *et al.* (2024) Load the trained model and forecast each attack dataset's input feature to evaluate model performance. Compare each forecast to the output to get the mean squared loss.

Determine θ as the mean squared error threshold. A mean square error loss value below θ indicates a normal message and matches expectations. A mean square error loss value above θ indicates an aberrant message, deviating from expectations:

- True Positive (TP): Refers to cases where the model accurately recognizes positive instances as positive
- False Positive (FP): Indicates situations where the model erroneously classifies negative cases as positive
- True Negative (TN): Refers to situations where the model correctly classifies negative instances as negative
- False Negative (FN): Denotes instances of false negatives, where the model incorrectly classifies positive cases as negative

Accuracy is determined by dividing the number of accurately predicted samples by the total number of samples in the model. A higher accuracy rating signifies a higher level of model performance. The accuracy can be determined by applying the following formula:

$$Accuracy = TP + TN/TP + FP + TN + FN \quad (1)$$

Precision is a metric that quantifies the ratio of accurately predicted positive cases to all the samples projected as positive by the model. A high precision rate indicates high accuracy in the model's predictions of positive cases. The calculation can be determined using the following equation:

$$Precision = TP/TP + FP \quad (2)$$

Recall quantifies the ratio of accurately predicted positive examples to all actual positive examples. A high recall score demonstrates the model's ability to identify positive examples accurately. The calculation is performed in the following manner:

$$Recall = TP/TP + FN \quad (3)$$

Using the F1 score evaluates model performance by combining two parameters: precision and recall. Measurement of the F1 score requires a specific calculation method:

$$F1Score = 2 \times Precision \times Recall/Precision + Recall \quad (4)$$

False Positive Rate (FPR) is an evaluation index that evaluates the percentage of normal data mistakenly categorized as anomalies by an anomaly detection model. FPR measures the system's capacity to prevent false positives from normal data being misclassified as anomalous data:

$$FPR = FP/FP + TN \quad (5)$$

The True Negative Rate (TNR) measures the anomaly prediction of normal data and can be used to evaluate a model's false positive rate:

$$TNR = TN/TN + FP \quad (6)$$

The False Negative Rate (FNR) measures a model's ability to predict anomaly data as normal:

$$FNR = FN/TP + FN \quad (7)$$

ROC-AUC, the area of the ROC curve according to the threshold, is an evaluation index that shows the model's precision and FPR change rate. The closer ROC-AUC is to 1, the better the model distinguishes normal and abnormal data. The Matthews Correlation Coefficient (MCC) measures binary classification model performance by considering all confusion matrix values (TP, TN, FP, and FN). When analyzing binary classification problems, MCC provides more information than F1-score and accuracy since it examines the balancing ratio of TP, TN, FP, and FN. Model performance improves with greater values:

$$MCC = TP \times TN - FP \times FN / \sqrt{(TP + FP)\ (TP + FN)\ (TN + FP)\ (TN + FN)} \quad (8)$$

ML and DL model training errors are called losses. Regression models use Mean Squared Error (MSE) and Mean Absolute Error (MAE), while classification models use cross entropy. The model predicts better with lower loss values.

Impact of Benchmarks on Anomaly Detection Effectiveness

Benchmarks are essential for improving the effectiveness of AD systems, especially in CPS. They offer a standardized framework that allows for evaluating and comparing various AD methods, ensuring that researchers can measure their performance under uniform conditions. Here are several ways benchmarks influence the effectiveness of AD.

Diversity of Data Types: Effective benchmarks should include a range of data types, such as sensor data, actuator data, network data, and control system log data. This variety enables a more thorough assessment of how effectively different algorithms can manage diverse inputs and situations.

Performance Metrics: Using established performance metrics like recall, accuracy, precision, F1 score, and area under the curve (AUC-ROC) is crucial. These metrics offer measurable insights into a system's performance, helping researchers pinpoint the strengths and weaknesses of their models.

Real-World Relevance: Benchmarks that incorporate real-world anomalies and labelled datasets, such as the SWaT testbed, are essential for evaluating the practical effectiveness of AD methods. They ensure that the algorithms can successfully recognize both familiar and new threats in realistic environments.

Adaptability and Resilience: Benchmarks should also assess how effectively anomaly detection systems can adapt to realtime data streams and withstand adversarial attacks. This is crucial for maintaining the systems' effectiveness in dynamic and potentially hostile environments.

Role of AD in Detecting Network Anomaly in CPS

Due to the growing dependence on digital infrastructure, the consequences of security breaches have become more severe, affecting various aspects such as personal privacy and national security. Conventional security measures, typically rule-based and unchanging, must be revised when confronted with dynamic and sophisticated cyber threats. This deficiency has stimulated the pursuit of more advanced and intelligent solutions, resulting in the incorporation of ML techniques. With its capacity to acquire knowledge from data, adjust, and recognize patterns, ML presents a potential opportunity to revolutionize network anomaly detection. Through the utilization of machine learning, systems have the potential to identify new or developing threats that escape detection by traditional mechanisms. This theoretical investigation aims to gain a comprehensive understanding of the role of ML in network anomaly detection. This framework aims to integrate existing knowledge and practices while also striving to advance the field by proposing innovative approaches and methodologies. Figure (6) shows the AD in detecting network anomalies in CPS.

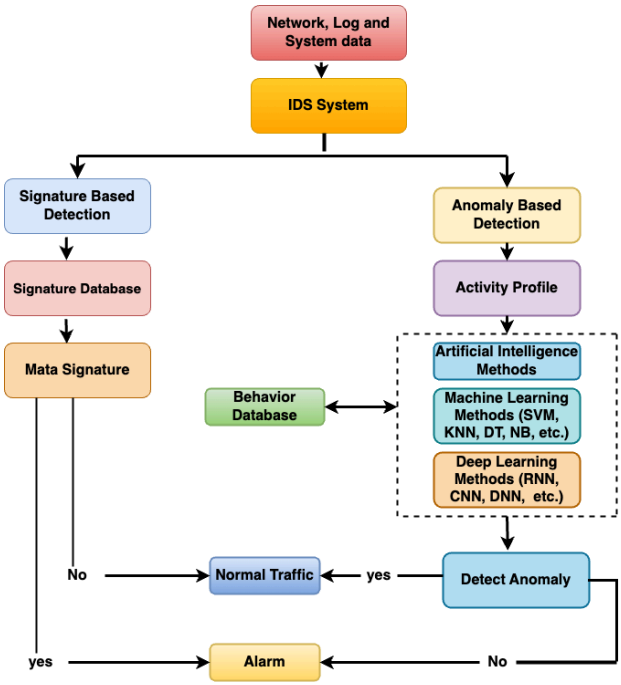

Fig. 6: AD in network anomaly in CPS

The architecture of an Intrusion Detection System (IDS). The system first consumes data from the network, logs, and the system itself. After that, the IDS System processes the data using two primary detection methods:

- Detection Based on Signatures: This technique compares incoming data with a Signature Database

to identify malicious behaviour patterns. An alert will be set off if a match is detected

- Anomaly-Based Detection: This method generates an Activity Profile and investigates using AI techniques. There are two main types of AI methods:
- RNN, CNN, and DNN, which are deep learning methods
- ML methods (including SVM, KNN, DT, and NB)

These AI methods communicate with a Behaviour Database to identify suspicious activity in network traffic. Based on the results of both detection methods, the system then makes decisions. The traffic is considered normal if neither approach detects any threats. But if either of those things detects something dangerous, then an alarm goes off. The IDS can better detect both old and new security threats because of this dual-approach technology, which merges signature-based and anomaly-based detection.

Analytical Discussion

Although AI-based AD systems provide substantial benefits compared to conventional methods, their successful deployment in real-time cybersecurity requires careful consideration of various constraints and downsides. The challenges include data requirements, computing demands, model interpretability, and vulnerability to sophisticated attacks, among other factors.

AI models, especially DL algorithms, need lots of labeled and unlabeled data for normal and pathological behavior classification. Data quality and relevance affect AI model performance. Carlini and Wagner (2017) use the concept of Noisy or irrelevant data can weaken models and cause anomaly detection errors. Training and inference of complex models, especially deep learning architectures, need plenty of computer resources. GPUs and TPUs are usually pricey.

AI models for real-time data from massive, distributed networks must scale. High detection accuracy and low latency processing demand complicated optimization and durable infrastructure. Decisions made by deep learning AI algorithms are opaque. Hinton *et al.* (2012) introduced the idea that cybersecurity specialists' reputations suffer from ambiguity.

Root Cause Analysis can obscure why a model labels an activity as uncommon for threat response. Root cause research and mitigation are difficult with opaque AI models. Liu *et al.* (2024) introduced that AI-based anomaly detection systems may tire security specialists and alert them with false positives.

Abadi *et al.* (2016) uses the concept of models may miss sophisticated attacks, resulting in false negatives. Consistency between sensitivity (actual positive rate) and specificity (real negative rate) must be revised. Attackers can make AI models think irregularities are normal.

Kumari and Prabha (2023) uses the concept of Adversarial training and AD ensembles, which must be researched to protect AI models from adversarial approaches. Integrating AI-based anomaly detection into cybersecurity systems takes planning. Data retraining, upgrades, and monitoring keep AI systems running. Maintenance needs resources.

Advanced ML algorithms utilizing AI-based AD have demonstrated encouraging outcomes in realtime cybersecurity by accurately identifying network traffic and system problems. Shruti *et al.* (2024) introduced that AI-powered AD systems have shown exceptional accuracy and memory in identifying anomalies, reducing false positives compared to conventional methods. By employing unsupervised learning algorithms and continuously analyzing realtime data streams, these systems may identify previously unknown attacks and internal security breaches without depending on predefined attack patterns, thus demonstrating their exceptional ability to detect threats. These systems encounter issues like handling massive datasets, managing computational burdens, countering adversarial attacks, and adopting efficient mitigation measures. Proposing the integration of AI, blockchain, and Quantum Computing (QC) as a feasible technique to improve cybersecurity defences indicates a promising future approach to address cyber threats. Kaur and Ramkumar (2022) stated that systems have succeeded overall, but their generative models may need help differentiating attack patterns that closely resemble normal data or deviate from the normal distribution near the normal cluster in latent space.

AI-powered AD systems improve the accuracy of identifying irregularities and decrease the occurrence of incorrect positive detections. Semi-supervised ML combines labelled and unlabeled data to discover anomalies. The evaluation measures comprise recall, precision, F1 score, and AUC-ROC.

Deep Learning-Based Anomaly Detection Limitations

While DLAD research is progressing rapidly, there is still an opportunity to improve current systems. The absence of interpretability: Shrivastava and Pancham (2021) introduced AD methods that can be interpreted to allow users to understand the cause of a detection result. Conventional machine learning approaches generally exhibit high interpretability. As an illustration, it can analyze the decision path of methods based on decision trees and investigate the subset to which the input sample belongs. DLAD approaches priorities by enhancing detection accuracy (precision and recall). Therefore, the discussion and study of the model's interpretability are limited.

High construction and maintenance costs: The cost of DLAD procedures is mostly due to two factors. The computing resources of CPSs devices are typically insufficient for running DL models. GPUs cost a lot. Secondly, developers invest significant time in creating and maintaining neural network models. Researchers must develop models based on specific CPS designs and anomalies during the design stage. Tuning hyperparameters during training is hard. The transfer of parameters during maintenance strains the communication network of CPSs.

Poor Data Quality: Sufficient high-quality input data is a prerequisite for DLAD methods that operate as data-driven systems. The analysis establishes three obstacles related to training data which affect CPS programs. First, CPS's surroundings are changing. Physical system components added or removed might result in newly discovered vulnerabilities. Generally, no indication is provided to distinguish between standard data patterns and attack data types. Manually produced samples include all uncommon cases. Quick alterations disrupt the point and contextual anomalies detected by DLAD methods. These detection systems tend to operate ineffectively when the same cases of continuous collective anomalies occur.

DLAD methods can be compromised. The neural model used in DLAD calls for data maintenance from CPS databases. There are two primary categories of attacks based on two distinct approaches: Poisoning strike through tampered training data and biased model detection findings, and Adversarial attacks, which degrade CPSs undetected by DLAD.

The practical implementation of AI-driven AD systems in Cyber-Physical Systems (CPS) faces several significant challenges. Organizations must manage the complexities of incorporating these tools into existing Operational Technology (OT) environments while maintaining seamless operations. Humayed *et al.* (2017) note that deploying CPS requires careful consideration of legacy systems and protocols that may not have modern security features. Resource demands pose a major obstacle, necessitating careful evaluation of computational and human resources. DL-based AD systems often require substantial computational power and memory, which may not be available in resource-limited CPS environments. Integrating with the current security framework introduces unique challenges.

Inoue *et al.* (2017) argue that organizations must ensure the smooth integration of new AI-driven detection systems with existing security technologies, such as firewalls, SIEM systems, and traditional IDS/IPS solutions. This integration must be achieved without creating new vulnerabilities or undermining existing security measures. The training and skill requirements are also demanding. Bui *et al.* (2021) highlight that organizations need personnel skilled in cybersecurity and machine learning to implement and maintain these systems effectively. This includes expertise in data preprocessing, model selection, hyperparameter tuning, and ongoing system improvement.

Moreover, the resource implications extend beyond the initial deployment. Liu *et al.* (2024) emphasized that organizations must dedicate resources for continuous model training and updates to maintain detection accuracy in response to new threats and changing system behaviours. This requires ongoing computational resources and skilled individuals who can interpret model outputs and adjust system parameters. Effectively executing these tasks is crucial for the success of AI-driven anomaly detection in CPS.

Improving Deep Anomaly Detection Methods

Benchmarks with enough labelled and real-world anomalies: Few benchmarks exist in CPSs for comparing DLAD algorithms. While specific datasets, such as SWaT, are commonly utilized, DLAD algorithms are often customized and adapt processed data independently. Benchmarks in specific CPS domains, such as aerial systems, might enhance evaluation. Various techniques can evaluate performance on the same benchmark. Identify many benchmark requirements:

1. Cover enough data types. The provision of sensor, actuator, network, and control system log data is ideal. Based on design goals, DLAD methods can use any data. Models demonstrate best performance on specific data categories, including sensor time-series information that can operate independently
2. Label anomalies. The evaluation of DLAD methods becomes challenging because abnormal events lack proper labelling. Researchers need to build attack and fault simulation models. Attack situations that are complete and verified allow detection systems to work more efficiently with less data processing involved. Simulation exists for specific fields like the smart grid, but real-world measurements and anomalies create better descriptions of system status

Improve running performance in real time: Various research studies have evaluated the performance capabilities of DLAD approaches in smart vehicles. Smart cars require immediate response because catastrophic accidents could occur. Other CPS systems require practical implementations of DLAD methods, and their running performance must be considered fundamental. The system's design contains two aspects that need improvement. (1) Allow real-time input measurements. The operation of DLAD approaches depends on realtime system measurements combined with live traffic data rather than offline dataset inputs. The data volume, sampling rate, and coherent format should be defined according to network capacity and

computational power. The detection speed of DLAD methods improves substantially when utilized on edge devices because these devices possess superior computational power. (2) Take realtime actions. Detecting anomalies is critical, but administrators should also find methods to prevent severe failures. Designing and training DLAD models requires the adoption of particular steps.

Find the abnormal device or cause: Current DLAD algorithms have great detection performance (e.g., true positives, accuracy). However, the location and source of the anomaly are often unknown. Even if DLAD algorithms detect anomalies, users lack knowledge of their origin and handling. In addition, anomalies in different CPS components have varying effects. We propose that DLAD approaches enhance detection granularity to the component level. Convlstm is used to identify anomalies in sensors and actuators. Once an anomaly is found, the infected device is also identified. Taking specific precautions could avert the loss. Additionally, this process can be automated without user intervention.

Neural network architectures can be adapted to suit various CPSs and situations: Different CPSs have common data kinds and abnormalities. Industrial Control Systems (ICS) often collect sensor time-series data. Anomalies in sensor and actuator changes can disrupt time relations in data. Attacks on the CAN bus system in Intelligent Transportation Systems (ITS) are common. LSTM and CNN capture time and context information, such as packet order and content.

Enhanced Quantum Blockchain and Quantum Computing Aspects in CPS

Peng *et al.* (2008) use the concept that Digital signature crackers pose an imminent threat. A thief may impersonate any user, take their digital assets, and forge any digital signature using Shor's algorithm and a quantum computer. Most experts agree that developing a large-scale universal quantum computer will take at least ten years. Still, some researchers believe it could be done sooner with emerging quantum computational devices with limited capabilities. This research is also ongoing at quantum computing businesses D-Wave Inc. and Zapata Computing Inc. Due to their fast solution times, a few individuals using quantum computers can control Bitcoin mining and censor transactions. Stewart *et al.* (2018) show these groups could double-spend by undermining lawful transactions or preventing their blockchain entries. Recent studies in Singapore, Austria, France, and the UK consider a realistic assault scenario.

Cryptocurrencies will crash without protocol updates when quantum computers are used. The quantum safety and quantum internet deal with security aspects related to blockchain and are discussed below.

Blockchains with quantum safety: Quantum cryptography is an enhancement method for blockchain security systems. Under quantum communication, attacks are prevented because the system operates authentically. The methods encode and send bits through photons as part of their transmission process. The quantum states require fundamental physics to remain unchanged during measurement or replication, according to Kiktenko *et al.* (2018). An eavesdropper can be immediately identified during any attempt at eavesdropping. Through quantum cryptography, all blockchain peer-to-peer encryption, together with digital signatures, can be substituted. However, the complexity and cost of quantum cryptography networks will limit their use. This technique is safe in blockchains if all nodes are connected pairwise, ensuring direct communication and no node can be confident. Current Internet connections use one-way cryptography and many intermediate nodes for security. Untrusted intermediary stations can securely relay signals between two parties using new device-independent quantum communication protocols. Fibre optic photon losses are another issue. Modern quantum key distribution systems are limited to tens of miles by these limits. A quantum repeater is proposed using teleportation and optical memory to distribute entangled states between communicating parties. A viable gadget still needs to be present despite the study. One-way functions can be tightened till then. Some proposals take time to reverse using conventional and quantum computers. Although insecure, these could buy time on the present gear. They will be understood eventually.

Blockchain quantum Internet: Chapron (2017) states that Blockchain processes can be more secure and efficient than quantum networks. A "quantum Internet" connects quantum computers using quantum communications. Complete quantum blockchains would be possible. Recent Swedish, Israeli, and Russian preprints show that avoiding computationally difficult verification and consensus phases may increase speed and security. Quantum Bitcoin could be secured using the quantum mechanics no-cloning theorem. Bank notes could contain quantum information to avoid forgery. Quantum Internet is decades away. Processing massive amounts of data requires full-scale quantum computers and a quantum communication network. 'Blind quantum computation' follows. Users with conventional computers can perform algorithms on remote quantum computers without exchanging data or algorithms. The technology would enable public cloud quantum-computing platforms, making blockchains more economical and accessible.

Quantum Computing's Effect

Three methods of encryption are used in contemporary cryptography: Symmetric, asymmetric, and hash functions. Symmetric cryptography's

encryption and decryption processes rely on the same secret key. It doesn't work with blockchain since all the nodes in the network can read the message, even if their sole job is to check if the new data is genuine. One solution to this problem is public-key cryptography, often known as asymmetric cryptography. This technique requires the sender to create a digital signature on the transaction they want recorded on the blockchain using a private key and then broadcast the signature with a public key. Receiving nodes can use this public key to confirm that the correct user generated the digital signature. Mavroeidis *et al.* (2018) showed that asymmetric cryptography employs prime number factorization or the discrete logarithm problem to generate these key pairs. The key aspect of hash functions is that they cannot be used to extract the original data from the hash output; instead, they take an input of any length and return a string of a defined length.

A quantum computer uses problem-specific quantum algorithms, as indicated before. The security of blockchain technology is at risk from two major quantum algorithms. Fernandez-Carames and Fraga-Lamas (2020) showed that the exponential speedup relative to conventional computers, Shor's approach was proposed in 1992 to tackle prime number factorization. An attacker can crack asymmetric cryptography and the digital signature of the blockchain with a method variant that can also solve the discrete logarithm problem. An adversary armed with a quantum computer running Shor's algorithm may deduce the private key by utilizing data from the publicly disclosed public key that accompanied a transaction. After gaining access to the victim's private key, the malicious actor could use it to publish additional transactions. Cui *et al.* (2020) use the concept of the victim's funds but charging a higher fee to increase the probability that miners would include the attacker's transaction instead of the original one, explores the concept of transaction hijacking in the context of cryptocurrency, where the attacker could broadcast conflicting transactions using the computed private key before the original one was finalized in a block.

The discovery of a collision enables attackers to modify block transactions since the modified content and other block data generate the same hash value yet preserve the blockchain. The implementation of Grover's algorithm provides quantum computer miners with the ability to mine blocks at a much faster rate than conventional computer systems can achieve. One instance that gains control of more than half the network computing power through a 51%-attack would acquire absolute authority to select block data during new block creation. The danger in cryptocurrency applications becomes severe because this attack method enables attackers to exclude their spending operations from blockchain records. Through their control of the computing power, an attacker could form a concealed chain from chosen modified blocks to alter previous transactions. The perpetrator controls most of the network power; thus, his fake chain extends beyond the existing blockchain's length. The system automatically accepts the longest chain as the truth, meaning the forged chain replaces the previous chain of blocks during this process.

Blockchain and Quantum Computing Aid in CPS

Blockchain technology and quantum computing operate differently, but they offer promising enhancements for protecting CPS cybersecurity systems. The fundamental security features of blockchain include decentralized operation and unalterable records that prevent covert attack vectors, which preserve data integrity. An aspect of blockchain technology which increases buyer trust in digital shopping relies on its transparent, distributed consensus systems. The adoption of quantum computing brings benefits and specific drawbacks in its operation. The technology presents an encryption security threat but provides the capability to enable quantum encryption mechanisms like quantum key distribution to establish perfectly secure communication pathways. Computation at the quantum scale helps security operations by accelerating difficult problem solutions in threat detection and analysis. Implementing these technologies in CPS's cybersecurity frameworks requires solving numerous practical and technological obstacles.

Future Directions

The advancement of cybersecurity through Cyber Physical Systems (CPS) will receive major enhancements through top technological innovations. AI integration with blockchain technology alongside QC may develop robust cybersecurity protection against modern cyber threats. The integration seeks to boost AD's security and operational efficiency while solving the current systems' vulnerabilities. Generative models need further research to become more skilled at distinguishing between normal data distributions and attack patterns. This enhancement is essential for augmenting AD systems and bolstering CPS's security framework. The paper underscores that ongoing innovation and adaptation are crucial for keeping up with the changing landscape of cyber threats, highlighting the necessity of creating scalable and intelligent AI-driven solutions capable of responding effectively to emerging difficulties in real-time. The opportunities for the future presented in the paper emphasize the imperative for continuous research and technology progress to strengthen cybersecurity frameworks in a progressively digital environment.

The advancements in AD systems for CPS carry substantial implications, and future research should concentrate on several critical areas to improve the effectiveness and resilience of these systems. Below are some detailed and constructive recommendations.

Integration of AI and Blockchain: Future research should investigate the integration of AI with blockchain technology to strengthen security frameworks. This combination can offer a decentralized and tamper-proof approach to logging anomalies and responses, improving accountability and traceability in CPS environments. Additionally, the exploration of QC should be considered to enhance defences against sophisticated cyber threats.

Generative Models for Anomaly Detection: There is an urgent need for research to improve generative models to better recognize the distinctions between normal data distributions and attack patterns. By enhancing these models, researchers can create more effective anomaly detection systems that can adapt to new threats and lower the rate of false positives, a common challenge in current systems.

Realtime Adaptation Mechanisms: It is vital to develop scalable and intelligent AI-driven solutions to address emerging threats in real-time. Future research should aim to create adaptive algorithms that learn from new data and adjust their detection strategies accordingly. Adaptability will be crucial for keeping anomaly detection systems effective in dynamic settings.

Improving Interpretability of Deep Learning Models: With the rise of Deep Learning-based Anomaly Detection (DLAD) methods, it is essential to enhance their interpretability. Research should develop techniques that help users understand the reasoning behind detection results. This transparency can increase trust in AI systems and lead to more effective decision-making in response to identified anomalies

Addressing Data Quality Challenges: Future studies must explore strategies for improving data quality in CPS environments. This includes creating better labelling techniques and generating high-quality synthetic data to train anomaly detection models. Addressing these challenges can boost detection systems' reliability and effectiveness in identifying threats.

Focus on Collective Anomalies: Research should also aim to identify collective anomalies often neglected by current systems. It's important to develop algorithms that can track behaviour patterns over time instead of just looking at isolated incidents, as this will be key to spotting complex attack scenarios that may not trigger immediate alerts.

Conclusion

This study presents notable advancements in cybersecurity because of artificial intelligence integration in anomaly detection systems targeted at Cyber-Physical Systems (CPS). AI-based anomaly detection systems perform exceptionally in detecting network abnormalities and system breakdowns through accurate identification processes beyond possible human achievement rates. These systems detect zeroday attacks and insider threats through unsupervised learning of real-time data streams without requiring attack signature definitions, demonstrating their ability to confront new cyber threats. This research investigates cybersecurity protocol problems that demand ongoing technological improvements because the systems struggle to process large datasets and extended workload requirements.

Acknowledgment

Thank you to the publisher for their support in the publication of this research article. We are grateful for the resources and platform provided by the publisher, which have enabled us to share our findings with a wider audience. We appreciate the editorial team's efforts in reviewing and editing our work, and we are thankful for the opportunity to contribute to the field of research through this publication.

Funding Information

The authors have no support or funding to report.

Author’s Contributions

All authors equally contributed to this study.

Ethics

This manuscript is an original work. The corresponding author certifies that all co-authors have reviewed and approved the final version of the manuscript. No ethical concerns are associated with this submission.

References

Abadi, M., Agarwal, A., Barham, P., Brevdo, E., Chen, Z., Citro, C., Corrado, G. S., Davis, A., Dean, J., Devin, M., Ghemawat, S., Goodfellow, I., Harp, A., Irving, G., Isard, M., Jia, Y., Jozefowicz, R., Kaiser, Lukasz, Kudlur, M., … Zheng, X. (2016). Tensorflow: Large-Scale Machine Learning on Heterogeneous Distributed Systems. *ArXiv:1603.04467*. https://doi.org/10.48550/arXiv.1603.04467

Anitha, K., Nagaraj, B. K., Paramasivan, P., & Shynu, T. (2023). Enhancing Clustering Performance with the Rough Set C-Means Algorithm. *FMDB Transactions on Sustainable Computing Systems*, *1*(4), 190-203.

Biggio, B., & Roli, F. (2018). Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning. *Pattern Recognition*, *84*, 317-331. https://doi.org/10.1016/j.patcog.2018.07.023

Broadbent, A., & Schaffner, C. (2016). Quantum Cryptography Beyond Quantum Key Distribution. *Designs, Codes and Cryptography*, *78*(1), 351-382. https://doi.org/10.1007/s10623-015-0157-4

Bui, H., Nguyen-Hoang, T.-A., Vo, B., Nguyen, H., & Le, T. (2021). A Sliding Window-Based Approach for Mining Frequent Weighted Patterns Over Data Streams. *IEEE Access*, *9*, 56318-56329. https://doi.org/10.1109/access.2021.3070132

Carlini, N., & Wagner, D. (2017). Towards evaluating the robustness of neural networks. *2017 IEEE Symposium on Security and Privacy (SP)*, 39-57. https://doi.org/10.1109/SP.2017.49

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, *41*(3), 1-58. https://doi.org/https://doi.org/10.1145/1541880.1541882

Chapron, G. (2017). The Environment Needs Cryptogovernance. *Nature*, *545*(7655), 403-405. https://doi.org/10.1038/545403a

Choi, H., Kim, M., Lee, G., & Kim, W. (2019). Unsupervised Learning Approach for Network Intrusion Detection System Using Autoencoders. *The Journal of Supercomputing*, *75*(9), 5597-5621. https://doi.org/10.1007/s11227-019-02805-w

Cui, W., Dou, T., & Yan, S. (2020). Threats and Opportunities: Blockchain meets Quantum Computation. *2020 39th Chinese Control Conference (CCC)*, 5822-5824. https://doi.org/10.23919/ccc50068.2020.9189608

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*, *8*, 21091-21116. https://doi.org/10.1109/access.2020.2968985

Geller, J., Ae Chun, S., & Wali, A. (2014). A Hybrid Approach to Developing a Cyber Security Ontology. *Proceedings of 3rd International Conference on Data Management Technologies and Applications*, 377-384. https://doi.org/10.5220/0005111503770384

Hinton, G. E., Srivastava, N., Krizhevsky, A., Sutskever, Ilya, & Salakhutdinov, R. R. (2012). Improving Neural Networks by Preventing Co-Adaptation of Feature Detectors. *ArXiv:1207.0580*. https://doi.org/10.48550/arXiv.1207.0580

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security-A Survey. *IEEE Internet of Things Journal*, *4*(6), 1802-1831. https://doi.org/10.1109/jiot.2017.2703172

Inoue, Y., Sakuma, J., & Nakao, K. (2017). Deep learning-based anomaly detection on raw TCP/IP packets. *2017 IEEE Symposium on Security and Privacy*, 328-343.

Jain, S., Gera, T., & Gill, R. (2023). A Novel Malware Detection and Classification for Healthcare Apps. *2023 2nd International Conference on Ambient Intelligence in Health Care (ICAIHC)*, 1-6. https://doi.org/10.1109/icaihc59020.2023.10431477

Ji, I. H., Lee, J. H., Kang, M. J., Park, W. J., Jeon, S. H., & Seo, J. T. (2024). Artificial Intelligence-Based Anomaly Detection Technology Over Encrypted Traffic: A Systematic Literature Review. *Sensors*, *24*(3), 898. https://doi.org/10.3390/s24030898

Kaur, J., & Ramkumar, K. . R. (2022). The Recent Trends in Cyber Security: A Review. *Journal of King Saud University - Computer and Information Sciences*, *34*(8), 5766-5781. https://doi.org/10.1016/j.jksuci.2021.01.018

Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., Lvovsky, A. I., & Fedorov, A. K. (2018). Quantum-secured blockchain. *Quantum Science and Technology*, *3*(3), 035004. https://doi.org/10.1088/2058-9565/aabc6b

Kumari, S., & Prabha, C. (2023). A Comprehensive Review on Anomaly Detection in Images: Challenges and Future Research Directions. *2023 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, 1-6. https://doi.org/10.1109/nkcon59507.2023.10396507

Kumari, S., & Prabha, C. (2024). A Comprehensive Review of Deep Anomaly Detection Techniques-An Analysis. *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, 1-6. https://doi.org/10.1109/i2ct61223.2024.10543335

Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., & Kim, K. J. (2019). A Survey of Deep Learning-Based Network Anomaly Detection. *Cluster Computing*, *22*(S1), 949-961. https://doi.org/10.1007/s10586-017-1117-8

Li, S., & Wen, J. (2014). A Model-Based Fault Detection And Diagnostic Methodology Based On Pca Method And Wavelet Transform. *Energy and Buildings*, *68*, 63-71. https://doi.org/10.1016/j.enbuild.2013.08.044

Liu, H., Zhao, B., Guo, J., Zhang, K., & Liu, P. (2024). A Lightweight Unsupervised Adversarial Detector Based on Autoencoder and Isolation Forest. *Pattern Recognition*, *147*, 110127. https://doi.org/10.1016/j.patcog.2023.110127

Mavroeidis, V., Vishi, K., D., M., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications*, *9*(3). https://doi.org/10.14569/ijacsa.2018.090354

Nagaraj, B. K., A, K., R, S. B., S, A., Sachdev, H. K., & N, S. K. (2023). The Emerging Role of Artificial Intelligence in STEM Higher Education: A Critical Review. *International Research Journal of Multidisciplinary Technovation*, *5*(5), 1-19. https://doi.org/10.54392/irjmt2351

Parsamehr, R., Esfahani, A., Mantas, G., Radwan, A., Mumtaz, S., Rodriguez, J., & Martinez-Ortega, J.-F. (2019). A Novel Intrusion Detection and Prevention Scheme for Network Coding-Enabled Mobile Small Cells. *IEEE Transactions on Computational Social Systems*, *6*(6), 1467-1477. https://doi.org/10.1109/tcss.2019.2949153

Peng, X., Liao, Z., Xu, N., Qin, G., Zhou, X., Suter, D., & Du, J. (2008). Quantum Adiabatic Algorithm for Factorization and Its Experimental Implementation. *Physical Review Letters*, *101*(22), 220405. https://doi.org/10.1103/physrevlett.101.220405

Sahay, S., & Sinha, R. K. (2018). Reinforcement learning based adaptive cybersecurity measures: A review. *ACM Computing Surveys*, *51*(4), 1-33.

Shrivastava, P., Pancham, K., & Singh, K. (2021). Classification of Grain s and Quality Analysis u sing Deep Learning. *International Journal of Engineering and Advanced Technology*, *11*(1), 244-250. https://doi.org/10.35940/ijeat.A3213.1011121

Shruti, Rani, S., Shabaz, M., Dutta, A. K., & Ahmed, E. A. (2024). Enhancing Privacy and Security In Iot-Based Smart Grid System Using Encryption-Based Fog Computing. *Alexandria Engineering Journal*, *102*, 66-74. https://doi.org/10.1016/j.aej.2024.05.085

Stewart, I., Ilie, D., Zamyatin, A., Werner, S., Torshizi, M. F., & Knottenbelt, W. J. (2018). Committing To Quantum Resistance: A Slow Defence For Bitcoin Against A Fast Quantum Computing Attack. *Royal Society Open Science*, *5*(6), 180410. https://doi.org/10.1098/rsos.180410

van Ede, T., Bortolameotti, R., Continella, A., Ren, J., Dubois, D. J., Lindorfer, M., Choffnes, D., van Steen, M., & Peter, A. (2020). FlowPrint: Semi-Supervised Mobile-App Fingerprinting on Encrypted Network Traffic. *Proceedings 2020 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium, San Diego, CA. https://doi.org/10.14722/ndss.2020.24412

Vasa, Y. (2024). Ethical Implications and Bias in Generative Ai. *International Journal for Research Publication and Seminar*, *15*(3), 500-511. https://doi.org/10.36676/jrps.v15.i3.1541

Vyas, B. (2022). Integrating Kafka Connect with Machine Learning Platforms for Seamless Data Movement. *International Journal of New Media Studies*, *9*(1), 13-17.

Vyas, B. (2023). Security Challenges and Solutions in Java Application Development. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, *12*(2), 268-275.

Wang, W., Zhu, M., Zeng, X., Ye, X., & Sheng, Y. (2017). Malware Traffic Classification Using Convolutional Neural Network for Representation Learning. *2017 International Conference on Information Networking (ICOIN)*, 712-717. https://doi.org/10.1109/icoin.2017.7899588