Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Intelligent intrusion detection for IoT and cyber-physical systems using machine learning

Maha M. Althobaiti *

Department of Computer Science, College of Computing and Information Technology, Taif University, Taif, Saudi Arabia

ARTICLE INFO

Article history:
Received 10 January 2025
Received in revised form
15 May 2025
Accepted 25 May 2025

Keywords:
Intrusion detection
Cyber-physical systems
Machine learning
IoT security
Classification models

ABSTRACT

Machine learning (ML) plays a key role in intrusion detection systems (IDS) and Internet of Things (IoT) security by improving the ability of cyber-physical systems (CPSs) to resist attacks from malicious users. CPSs combine physical components with networking and communication technologies to ensure safe and efficient operations. However, attackers often try to disrupt or disable the computing resources of these systems. This paper presents a new ML-based IDS framework designed for CPSs. To develop this framework, an open-source dataset containing different types of cyberattacks and related detection features was used. The dataset was labeled and preprocessed to make it clean, balanced, and suitable for training ML models. Preprocessing steps included handling missing values, normalizing features, and balancing the class distribution. Two ML algorithms—Random Forest (RF) and Stochastic Gradient Descent (SGD)—were applied to build and train classification models for intrusion detection. The experimental results showed that the RF model achieved a high accuracy of 99.5%, outperforming the SGD model, which reached 93.6% accuracy. In addition to accuracy, model performance was also measured using precision, recall, and F1 score. The results demonstrate that the proposed IDS is effective in detecting cyberattacks and improving IoT security. It offers a scalable and reliable solution for protecting CPS environments. This research contributes to the development of more secure CPSs by enhancing the trustworthiness, robustness, and flexibility of IoT systems.

1. Introduction

The fusion of Internet-of-Things (IoT) devices with cyberphysical systems (CPSs) has led to a new epoch of innovation (Blasch et al., 2017). This integration facilitates the transfer of data and smooth communication underpinning data analytics across various sectors (Yaacoub et al., 2020). In core sectors, such as manufacturing, healthcare, public transport, and urban development, this convergence has empowered organizations to enhance their operations, boost productivity, and deliver improved services (El-Kady et al., 2023).

As of the year 2023, the size of the global IoT market was approximately 486 billion USD, and it is expected to continue to increase with a compound annual growth rate of 24.7% to 1.6 trillion USD by 2025. Increases in the IoT and corresponding CPS markets clearly indicate a technical evolution that affects various sectors, such as manufacturing, healthcare, smart cities, and transportation. The integration of IoT and CPSs makes real-time interaction and communication between the physical and computational spaces possible.

This integration has boosted operational efficiency, preventive maintenance, and decision-making. For example, the use of the IoT for predictive maintenance in manufacturing can cut equipment breakdown risk by 50% and increase asset lifespans by 20%–40%.

However, the interconnectivity of CPS and IoT also leads to considerable cybersecurity risks, mainly because these systems are susceptible to attacks that can disrupt processes or exploit weaknesses (Djenna et al., 2021; Burg et al., 2017). Because of the interconnectivity of CPSs and IoT, the types of cyberattacks to which they are most susceptible include distributed denial of service (DDoS), data leakage and theft, unauthorized access and exploitation, and device tampering (Tyagi and Sreenath, 2021). Anomaly detection is a specific

* Corresponding Author.
Email Address: maha_m@tu.edu.sa
https://doi.org/10.21833/ijaas.2025.06.009
Corresponding author's ORCID profile:
https://orcid.org/0000-0001-6322-3963

security research field focused on combatting these types of threats. Globally, there are currently approximately 30.9 billion IoT devices, and each is a potential cyber entry point for unknown actors. Cybersecurity Ventures has forecasted that annual cybercrime could cost around 10 trillion USD by the end of 2025, with IoT devices likely to be the main victims of cyberattacks.

Traditional security mechanisms, such as encryption and signature-based methods, play a crucial role in intrusion detection systems (IDSs) and network device firewalls. However, the dynamic and heterogeneous nature of IoT/CPS environments poses unique security challenges that traditional security measures may struggle to address effectively (Burg et al., 2017). These include the vast number and diversity of IoT devices, resource constraints that hinder the widespread implementation of robust security protocols, novel avenues of attack, and the interconnection of physical and digital worlds, adding layers of complexity. In addition, malefactors present at various stages of the production process possess the capability to compromise devices by introducing malware, backdoors, or counterfeit components, thereby jeopardizing the security of the devices in question (Aly et al., 2019). Hence, the development of an intrusion detection system (IDS) tailored to CPS and IoT environments is crucial, as these emerging threats often elude conventional security measures.

New machine learning (ML) models for real-time anomaly detection and for learning new types of attacks are a potential approach to more effectively protect systems and networks. ML-based studies on the contamination practices used to attack IoT/CPS implementations rely on big data analysis to detect patterns that indicate unauthorized operations. Supervised learning, unsupervised learning, and reinforcement learning are some of the methods used to design these complex anomaly detection mechanisms. For instance, supervised learning algorithms can easily be trained on labeled data to distinguish between normal and anomalous behavioral patterns with high accuracy. Clustering and autoencoder models, which are examples of unsupervised learning, are useful in identifying unknown threats because such models can learn the regular behavior of the system and then look for anomalies. Hence, the primary aim of this study was to deploy ML models to accurately predict and identify malware attacks that compromise IoT security within CPSs. The detailed objectives of the study were as follows:

- To investigate the vulnerabilities and principal security challenges inherent in CPSs integrated with the IoT.
- To design and implement ML models that can detect anomalies within the IoT and CPSs
- To monitor and assess the performance of IoT/CPS environments against cyber threats, thereby enhancing their overall availability and reliability

The knowledge derived from this research will benefit the area of cybersecurity, improving our understanding of the topic and enabling approaches to be designed for mitigating the risk and vulnerability of system interconnections and improving the performance of secure and sensitive infrastructures.

The subsequent sections are organized as follows: a review of the literature is provided in Section 2, the research methodology is presented in Section 3, and the results from the experiments and an analysis and discussion of these results comprise Section 4. Finally, the concluding remarks are provided in Section 5.

2. Literature review

The challenges and opportunities for the development and deployment of AI-based attack IDSs for IoT devices and CPSs have been extensively studied in previous work (Zhou et al., 2019). As previously described, because CPSs and IoT devices are often interlinked, it is important to take strict precautions to protect them against potential cyber threats (Ashibani and Mahmoud, 2017), and the potential of ML methods has been demonstrated in this area.

These methods can identify potential security breaches by examining trends and anomalies indicated by previous learning from the vast amount of data available from CPSs and IoT devices. ML techniques, such as clustering, association, and regression, are employed to classify traffic from CPS and IoT networks and detect anomalies (Tyagi and Sreenath, 2021). Despite the many possible advantages provided by ML-based detection and classification of threats and anomalies on CPS and IoT networks, it remains challenging to obtain the correct datasets to train and build effective ML models (Shaukat et al., 2020). This can be attributed mainly to outdated datasets and the lack of reported factual cases of fraud with easily accessible data within this domain (Xin et al., 2018). A broader discourse on the above-mentioned issues is provided in the following sections.

2.1. IoT

The IoT is an advanced concept that outlines how things, objects, and people can connect and communicate with networking technology, both presently and in the future. It is typically implemented as a system of connected devices supplied with sensors, software, and various other technologies that allow both independent and coordinated communication and work. IoT systems increase the ability to monitor, manage, and optimize processes and environments in different domains, such as smart homes, healthcare, manufacturing, and smart cities. However, the continuing developments and exponential growth of the IoT present considerable concerns with respect to security and the identification of intrusions. Mitigating these

challenges is crucial to realizing the full advantages of the IoT while building and maintaining more secure, reliable, and resilient networking environments. This section is devoted to describing the essential research on securing IoT networks with respect to different methods and their efficiency.

Lai et al. (2024) analyzed two datasets (IoTID20 and IoT-23) to determine the details of network traffic from IoT devices, such as smart homes, laptops, and smartphones. The variants of IoTID20 include a binary dataset that is divided into standard and malicious data and a multi-category dataset containing normal, DoS, "man in the middle" address resolution (MITM ARP) spoofing, Mirai, and scan data. The IoT-23 dataset contains data collected from devices such as the Amazon Echo, Philips Hue, and Somfy Door Lock, and features two types of labels: binary and multi-category. The labels were cleaned, and classes of fewer than five instances were removed. Their study considered the ridge regressor, naïve Bayes, multi-layer perceptrons, support vector machines (SVMs), and decision trees using Bayesian optimization methods. The researchers demonstrated that these models were effective in detecting most types of cyberattacks in an IoT setting and recognizing the pervasive features of the network.

Douiba et al. (2023) presented an improved anomaly detection model that combines two ML models: gradient boosting and decision trees. This was enhanced by the CatBoost open-source framework. The developed model was tested on four datasets—NSL-KDD, BoT-IoT, IoT-23, and Edge-IIoT—with a GPU-based performance optimization strategy. Their aim was to enhance the correctness, precision, and processing time of an IDS and achieve an overall accuracy of 99.9% over different metrics. Their model addressed the class imbalance problem, thus increasing the detection rates of minority classes through target statistics and gradient boosting.

The CIDAD dataset was created by Vigoya et al. (2023) to address the scarcity of constrained application protocol (CoAP)-IoT traffic datasets with normal and anomalous cases. Most data were preprocessed to replace missing values, extract features, and balance categories using the synthetic minority oversampling (SMOTE) technique. Fivefold cross-validation was then adopted to measure classifier performance. The following classifiers were considered: Logistic regression, naïve Bayes, random forest (RF), AdaBoost, and SVMs. For these classifiers, the metrics of accuracy, precision, recall, F1 score, and Cohen's kappa statistic were calculated.

The best performance was observed when the RF model was used, and 99% of the labels were correct. The precision (99.9%) and F1 score (100%) recall results, and the estimated Cohen's kappa value (.99), strongly indicated that the multi-layer perceptron was very robust. High predictive power was also shown by the logistic regression and SVM approaches. The CIDAD dataset was shown to produce dependable anomaly detection systems for CoAP-IoT environments.

2.2. Key challenges in IoT

Many companies frequently encounter Internet-related difficulties, making it crucial to ascertain the integrity and reliability of the IoT systems and instruments that they use. Some of the key challenges involved in this area are as follows:

- Multiplicity and diversity. The multiplicity and diversity of IoT devices present serious security risks. IoT ecosystems are often made up of a variety of devices with different features, constructors, and capabilities, making it difficult to implement standardized security protocols throughout an ecosystem (Sfar et al., 2018).
- Constraints on computing resources. The limited storage and processing power capacity of many IoT devices makes it difficult to implement robust security features. Because of these constraints on resources, devices may not optimally perform authentication, encryption, or other security measures, making them vulnerable to attacks (Sha et al., 2018).
- Security communication protocols. IoT systems frequently employ protocols that lack inherent security features for communication over unsecured networks (Omolara et al., 2022). Without adequate authentication and integrity assurances, IoT data can become susceptible to interception, espionage, and manipulation by malevolent entities. IoT devices can be physically damaged, stolen, or vandalized when placed in unmanaged or hostile locations.

The poor availability of recognized safeguards across various IoT platforms and ecosystems, together with interface concerns, makes it difficult to deploy uniform safeguards (Gupta and Quamara, 2020). Overcoming these obstacles calls for an all-encompassing strategy that includes organizational, technical, and legal measures (Sharma et al., 2023). Throughout the entire IoT lifecycle, from product configuration and development to deployment, functioning, and disposal, it is imperative for businesses to prioritize security. This approach enables corporations, industry sectors, and security agencies to establish standard safety measures that facilitate the enforcement of security guidelines, protocols, and policies, thereby endorsing the dependable and secure application of IoT technologies.

2.3. Security of IoT

Conventional IoT security measures comprise an array of methods and mechanisms aimed at safeguarding networks, devices, and data against security threats. A pivotal tactic is network segmentation, which allocates IoT devices to distinct network sections or virtual local area networks

(Kahmann et al., 2023). This compartmentalization mitigates the risk of unauthorized access to critical assets and networks by curtailing security breaches within isolated networks, thereby diminishing repercussions. Encryption is indispensable for IoT security because it secures the confidentiality and integrity of data transmitted between IoT devices and servers or gateways. Protocols such as Transport Layer Security and Datagram Transport Layer Security are employed to encrypt communication channels, thwarting adversaries from intercepting or tampering with data exchange (Baskaran et al., 2019). Verifying the identity of people and devices through IoT systems requires the use of authentication methods and login controls. To ensure that only authorized organizations can access IoT resources, robust security methods, such as digital signatures, login details, and fingerprints, are used (Yang et al., 2021). To reduce the likelihood of unwanted actions, access control methods, such as role-based access control and access lists, aid in restricting users' access rights based on predefined roles or permissions (Malik et al., 2020).

IDSs, intrusion prevention systems (IPSs), and firewalls are integral parts of IoT security architecture. Traffic entering and exiting IoT networks is typically monitored and filtered by firewalls to prevent fraudulent and unauthorized login attempts. Note that IDSs and IPSs are often designed to work in tandem with firewalls (Dorado et al., 2021; Kizza, 2024; Zhou et al., 2019). To reduce IoT vulnerabilities, device-hardening measures must be implemented. Organizations can reduce the scale of attacks and improve security measures for IoT installations by implementing security best practices, such as prohibiting redundant services, changing default passwords, and installing security patches and updates (Pütz et al., 2023).

Physical security measures, especially in open or uncontrolled locations, can also protect IoT equipment from theft, unauthorized access, and physical interference. Examples of such precautions include secure packaging, tamper-evident seals, and access control (Pütz et al., 2023). IoT network visibility can also be implemented via monitoring and recording systems that can help track and document events and activities (Kaur et al., 2022). Educational initiatives can inform users about potential security risks and how to mitigate them, while security policies can provide valid usage rules, incident response protocols, and security best practices (Cram et al., 2017). By putting these traditional IoT security measures in place, businesses can mitigate security risks and protect their IoT facilities from various attacks and vulnerabilities. The rest of this section focuses on research related to ML approaches to improving IoT security.

Altulaihan et al. (2024) presented an IDS to strengthen the security of IoT networks from DoS attacks using ML methods. They used the IoTID20 dataset, which consisted of 59,391 DoS attack instances, 585,710 anomaly instances, and 40,073 normal instances across 386 features. In the preprocessing stage, they performed some computations to remove null values and biased features, and encoding was used to define categorical labels. The database was divided into training and test sets, and feature selection was performed using correlation-based feature selection and a genetic algorithm. They benchmarked classifiers, such as decision trees, RFs, k-nearest neighbors, and SVMs, and identified that the decision tree and RF classifiers using the features selected by the genetic algorithm yielded the highest accuracy. This work discussed the difficulties in designing a lightweight IDS for IoT-constrained environments; nevertheless, the proposed IDS demonstrated a high level of accuracy in detecting DoS attacks, enhancing IoT network security.

Alangari (2024) presented a hybrid optimization approach called AHGFFA to protect mobile ad hoc network-secured IoT sensor networks from blackhole and grayhole attacks. This study modeled various attack scenarios and network topologies using multiple metrics, such as packet delivery ratio, throughput, delay, and energy consumption, based on simulated data gathered from the ns-3 environment.

The dataset contained no missing values and was divided into training and test sets. AHGFFA used a genetic algorithm and the firefly algorithm for routing optimization and achieved a detection rate of 98% for malicious nodes, obtaining considerable improvements in metrics, such as packet delivery ratio and throughput. Although it performed well in simulations, the actual application of this model might face difficulties due to changes in conditions inside an actual network and the need for calculations to be done in real time. This research used hybrid ML with unsupervised techniques for sensor network security in the IoT.

Khan and Alkhathami (2024) discussed how the security of IoT-based healthcare systems could be improved using ML techniques. The authors used the publicly available Canadian Institute for Cybersecurity (CIC) IoT dataset, which contains 33 kinds of IoT attacks categorized into seven main categories. The dataset was preprocessed to balance the class representation using the SMOTE algorithm, ensuring non-biased supervised learning. Classification was made using RF, adaptive boosting, logistic regression, perceptron, and deep neural network methods. The findings revealed that an RF approach performed optimally, with an approximate accuracy of 99.55% for both binary and multiclass classifications.

This research also found that feature reduction had to be done to avoid highly correlated features and hence avoid overfitting and to help improve training time so that good detection would be possible in real time. The method achieved substantial improvements in accuracy, precision, recall, and F1 score, indicating good anomaly detection for IoT-based healthcare applications.

2.4. CPSs in IoT

As previously described, the convergence of CPSs and the IoT has led to new security problems for physical and cyber subsystems (Djenna et al., 2021; Zhou et al., 2019). For example, IoT botnets can compromise smart home gadgets, and ransomware attacks can target enterprise control systems, drawing attention to the potential consequences of privacy breaches in the context of CPS and IoT (Makhdoom et al., 2018). The interconnected elements in CPSs and the IoT can be affected by vulnerabilities in the same area, thereby increasing the potential impact of security incidents (Makhdoom et al., 2018; Lesch et al., 2023). For example, an online attack on a smart grid could lead to a power outage for critical infrastructure, with dire consequences for both the economy and public safety (Kimani et al., 2019). The acquisition of IoT devices and the sharing of sensitive data also raise concerns about privacy and privacy breaches, especially in industries that generate a significant amount of sensitive data, such as healthcare and smart cities (Lesch et al., 2023). The rest of this section focuses on CPS research of relevance to the issues raised in this article.

In a recent study by Rodriguez et al. (2021), an innovative architecture called intelligent architecture for cyber-physical systems (IA-CPS) was proposed to improve CPS management. The IA-CPS architecture is based on two main frameworks: a service-oriented framework and an event-driven framework. They cooperate closely to manage the underlying level of complexity in large-scale and distributed CPS environments. This study presented practical applications using video surveillance and the monitoring of energy consumption. For video surveillance, the IA-CPS can cope with images from 50 cameras simultaneously, performing real-time analysis and generating alerts. In energy management, the system processed data from 1,000 intelligent meters to optimize consumption patterns, reducing energy consumption by 25%. The IA-CPS model also reduced its response time by 30% through the use of real-time processing and an intelligent decision framework. Such enhancements were made possible through the integration of complex event processing and microservices, which offer great flexibility, scalability, and dynamic adaptability to changing conditions.

Djenna et al. (2021) investigated in detail the synergy of CPS and the IoT because of their common characteristics of interoperability, scalability, and the ability to interact in real time. According to the authors, CPSs should be able to perform complex tasks because they integrate computation, networking, and physical processes. For example, an advanced CPS can manage up to 1,000 events in one second, which is important for health applications in which real-time monitoring and response are crucial. In innovative grid applications, energy management via CPS resulted in up to a 30% reduction in energy wastage. Djenna et al. (2021) also mentioned intelligent cities in which the IoT controls infrastructure elements, such as traffic lights. A reduction in average travel time was 20%, and carbon emissions were considerably reduced. These examples reveal how the integration of physical and digital environments through CPS and IoT is transformational in nature.

Tushkanova et al. (2023) reviewed detection techniques that can be used for cyberattacks and anomalies in CPSs, emphasizing early detection to prevent drastic consequences. The authors noted that the effectiveness of an ML model in detecting anomalies depended on the quality and availability of an appropriate dataset. Many researchers have been forced to create synthetic datasets because obtaining real-world CPS data is challenging, as these data are typically private and confidential due to security issues. A problem lies in the completeness and validity of such synthetic datasets. The researchers stated that only one of the three datasets they considered in their study was adequate for intrusion detection tasks because it incorporated both network and sensor data, which was far superior to the standard means of anomaly detection. The researchers also touched on available methods for evaluating ML technique efficiency, suggesting a need for further research in this area.

An advanced anomaly detection technique for CPSs was proposed by Ramachandran et al. (2023), which fused Aquila optimization and ML. Their framework detected abnormal behaviors within CPS environments in what they considered the most efficient way. The framework preprocesses the network data into a compatible format and applies an enhanced Aquila optimization algorithm to select features. In addition, the model integrates an adaptive neuro-fuzzy inference (ANFIS) system and a Chimp optimization algorithm to improve anomaly detection. The chimp optimization algorithm modulates the membership functions underlying the ANFIS method to optimize the overall detection process. The performance of the proposed model was tested using benchmark datasets, achieving an accuracy of 99.37% and outperforming recent models in accuracy and efficiency. This work highlighted the importance of combining optimization algorithms with ML for anomaly detection in CPSs, specifically because of the problems of data complexity and real-time processing.

Hyder et al. (2023) revealed the significance of a realistic and accurate dataset when designing an ML-based anomaly detection system (ADS) for smart grids. Their co-simulation intelligent grid platform performed simulations based on realistic datasets that presented the subject matter of the threat landscape with a rich spectrum of potential cyber-events. A dataset was required, and once this was developed, it was employed to build and evaluate a specific ADS. Although the AI performed well on the specific datasets that were used to train it, it also worked when trained on a random, statistically diverse set of data on which it had not been trained.

This paper helped establish a baseline cyber-resilient middleware architecture for constructing proof-of-concept cybersecurity applications and CPS datasets. The generation of high-fidelity datasets was found to be important in improving the robustness and precision of robust ML-based anomaly detection for CPSs, such as power grids.

Hao et al. (2021) suggested a hybrid statistical ML model to further advance real-time anomaly detection in industry control systems (ICSs). The proposed model integrates a seasonal autoregressive integrated moving average (SARIMA) approach with long short-term memory to obtain high precision and low false omission rates in abnormal traffic pattern detection. ICS network traffic was described, and the model successfully detected various anomaly events, including cyberattacks, malicious behaviors, and network anomalies. Experiments in realistic ICS CPS testbeds have shown that the proposed hybrid model's detection efficiency was over 95%, and it had a lower computational requirement than other models, revealing that the integration of statistical learning methods with algorithmic learning can achieve high performance in real-life anomaly detection in ICS systems.

Yang et al. (2023) proposed an advanced model for industrial CPS traffic outlier detection that has three critical parts: A data preprocessing model, an unsupervised word segmentation model, and an unsupervised classification model based on an autoencoder. The data preprocessing model can efficiently extract those packets that belong to the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) and transform the content of the packets into a series of alphanumeric characters. For word segmentation, the model uses long short-term memory, and the probabilities of the combination of words ensure adequate accuracy among the relationships of words with strong segmentations. This classification model also integrates a one-dimensional convolutional neural network (CNN) with bidirectional encoder representations from transformers (BERT) language model, and it fully utilizes the short- and long-term dependences in the data. In addition, an accuracy of 95% was achieved by the developed model, which demonstrated that it identified cyberphysical attacks. It also met real-time detection criteria.

Elhanashi et al. (2023) thoroughly studied the integration of ML to improve CPS security and to accurately detect network intrusions. The guidelines for anomaly detection presented in their paper included a method of comparative evaluation for multiple attack scenarios from the CSE-CIC-IDS2018 dataset. This method can identify anomalies in network traffic patterns as determined by RF, Gaussian naïve Bayes, and multilayer perceptrons. In this way, they demonstrated the use of such applied techniques to sustain the security and integrity of CPSs. Thus, it is possible to design a method that can perform data preprocessing and correlation-based filtering of complex and imbalanced data to manage computational time and dimensionality reduction, ultimately increasing the speed and accuracy of anomaly detection in CPSs.

2.5. ML-based intrusion detection

One effective way to detect intrusions in IoT/CPS environments is to employ ML techniques, which work by extracting knowledge from data to look for trends and identify anomalies that could be signs of security breaches (Saranya et al., 2020). The growing popularity of ML in intrusion detection can be ascribed to its ability to analyze vast amounts of data and effect mitigation actions in response to newly identified threats. To train ML models on the basic patterns and attributes of security threats, datasets of cases labeled as normal and malicious behavior can be used. With available and reliable datasets, ML techniques, specifically supervised and unsupervised learning techniques, can be easily deployed to train and build models for intrusion detection. Two popular ML approaches for intrusion detection are SVMs and neural networks (Kirubakaran et al., 2024).

ML approaches can also detect anomalies and trends in unclassified or unlabeled datasets without the need for disaggregated data (Selmy et al., 2024). By categorizing data points based on comparisons, unsupervised ML techniques, such as k-means, can identify deviations from typical behaviors that could be signs of security breaches and require further research (Gadal et al., 2022). By establishing a relationship between network environments and the actions occurring in them, IDSs can also learn the best ways to deal with security risks via reinforcement learning (a broad class of methods in ML) (Shaukat et al., 2020; Rodriguez et al., 2021). Reinforcement learning algorithms assimilate feedback from their actions to incrementally enhance their efficacy, such that in dynamic and changing environments, they can continuously adjust and improve IDSs, increasing the effectiveness of defensive barriers (Shaukat et al., 2020; Rodriguez et al., 2021; Nguyen and Reddi, 2021).

Bertoli et al. (2021) provided a general outline of IDSs in CPSs using ML techniques. Their study focused on enhancing the precision of IDSs, and the authors detailed a complete end-to-end system that included data collection, feature extraction, and classification processes. Supervised learning algorithms were trained on labeled datasets to understand the patterns relevant to CPS intrusions. Data preprocessing techniques, data normalization, and feature selection were also considered to improve the performance of the ML models. The performance of this framework in detecting CPS intrusions was found to be robust in different network environments and to significantly improve accuracy compared with traditional frameworks. Finally, the results of real-world implementations in CPS scenarios were also reported, showing the ability of the proposed framework to scale for solving real-world problems. Its F1 score was .96,

indicating that it has the potential for effective intrusion detection and mitigation in CPSs.

Santos et al. (2023) evaluated several ML techniques for intrusion detection in CPSs. Supervised and unsupervised learning methods were compared to determine the one most suitable for CPS security. Different algorithms, such as decision trees, SVMs, and clustering techniques, were described. The evaluation parameters included detection rate, false positive rate, and computational efficiency. Overall, it was found that supervised learning techniques produce better accuracy; however, unsupervised methods can be applied in scenarios in which there is little or few labeled data. The authors reported that a few ML models achieved an accuracy of more than 90% for intrusion detection in CPS. In their concluding remarks, they proposed a hybrid model in which supervised and unsupervised learning are employed to enrich system-wide security.

Nour et al. (2023) explored transfer learning to optimize intrusion detection in industrial CPSs. They proposed a method for leveraging pretrained ML models to improve detection performance in a new environment with very limited labeled data. The idea was to reduce training time and increase the accuracy of IDSs. Their system performed transfer learning on different datasets very well, improving the detection rate and reducing the number of false positives. The authors reported that the fine-tuned models achieved accuracy rates of more than 95%, demonstrating the effectiveness of transfer learning in adapting to the disparate contexts of CPSs. Finally, the authors mentioned the difficulty of domain adaptation and the importance of correctly selecting a pretrained model for transfer learning optimization.

Alqaralleh et al. (2022) presented an optimized ML-based IDS for CPSs. In this work, the main emphasis was on parameter fine-tuning of the algorithms to increase detection accuracy and reduce false positives. Some of the work was on neural networks and ensemble methods that were presented to indicate the importance of parameter optimization in ML model performance. Extensive experiments on their dataset revealed that the proposed optimizations enhanced the detection rate. The accuracy rates were greater than 92%, and the optimized IDS could secure CPS environments. Finally, this study clarified the computational challenges in realizing ML models in real-time CPS applications and offered solutions.

Colelli et al. (2021) designed an anomaly-based IDS to add an enriched security layer to CPS using ML approaches. They considered the problem of discovering abnormal patterns in network traffic and system behavior that might indicate a breach. Their proposed IDS uses an extensive range of unsupervised learning techniques with clustering and anomaly detection algorithms to recognize abnormal behavior. They argued that the system should be adaptive to the dynamic nature of CPS and efficiently detect zero-day attacks. The authors reported that the detection accuracy acquired by the proposed anomaly-based IDS was very high and that its false alarm rate was reduced. They also provided detailed performance metrics and listed the challenges of implementing the IDS in a CPS.

Despite extensive research on intrusion detection in CPS and IoT environments, several challenges remain unaddressed. Most existing IDS models are computationally expensive, making them unsuitable for resource-constrained IoT devices. Furthermore, detecting zero-day attacks remains a critical issue, as traditional models rely on predefined signatures. Anomaly-based IDS approaches also tend to generate high false positive rates, reducing their practical applicability. Additionally, scaling IDS solutions across large IoT networks poses challenges in terms of data processing and resource efficiency. Finally, the integration of blockchain technology for secure IDS logging and decentralized attack mitigation remains unexplored. Addressing these gaps can lead to more effective, efficient, and scalable IDS solutions for CPS and IoT networks.

3. Methodology

The research approach or methodology of this study focused on developing an ML-based IDS for CPSs. The initial phase in creating the proposed framework involved gathering data from online repositories and employing data extraction techniques to isolate critical feature data. Subsequently, ML algorithms (specifically, stochastic gradient descent [SGD] and RF) were used to predict attacks on the CPS. The proposed framework, shown in Fig. 1, is outlined in the following subsections.

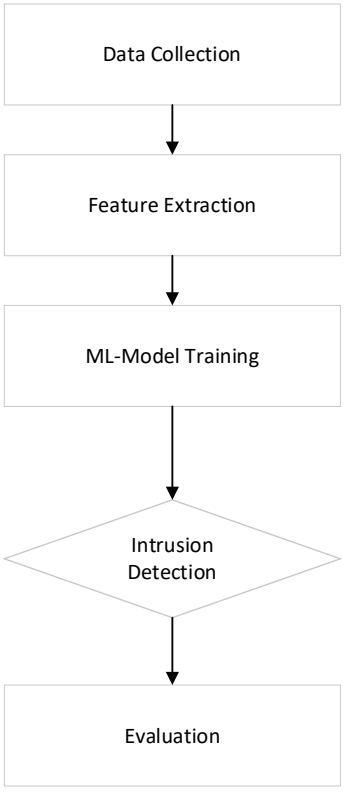

Fig. 1: Proposed framework

3.1. Data collection

This research study employed exploratory data analysis. The primary goal was to collect a substantial volume of numerical network traffic data for ML model development. It was important to ensure completeness in the data to aid in achieving high prediction model accuracy. The initial step involved data collection from Kaggle (www.kaggle.com), which is a large platform that hosts millions of datasets. The selected dataset (CICIDS) consisted of CPS data and comprised 283,743 records and 79 features. The variable types included float (24 bit), object, and int 64. The dataset encoded variables as objects, with labels denoting the classification (normal data traffic or anomalous attack patterns). Various types of network traffic were collected, including user activity, malicious behavior, and attack patterns. The details of the dataset are listed in Table 1. Fig. 2 shows the cyber-physical attacks in the IoT security system dataset. There were 14 types of crucial cybersecurity attacks in the dataset. The DoS Hulk attack was the most common, with 105 instances, and the second-most common was the PortScan attack, with 104.5 instances. The least frequent attacks in the dataset were Heartbleed attacks.

Fig. 3 shows the classification of the cyberattack data: Blue indicates benign activities, and orange signifies cyberattacks. According to the graph, the attack range is 0.50, and the benign range is 2.0. This balance allowed for a good distinction between benign and malicious activities within the dataset. Utilizing the dataset and its categorizations aided in evaluating the performance of the SGD and RF models, subsequently improving cybersecurity measures in IoT environments, as with the investigations carried out in this research.

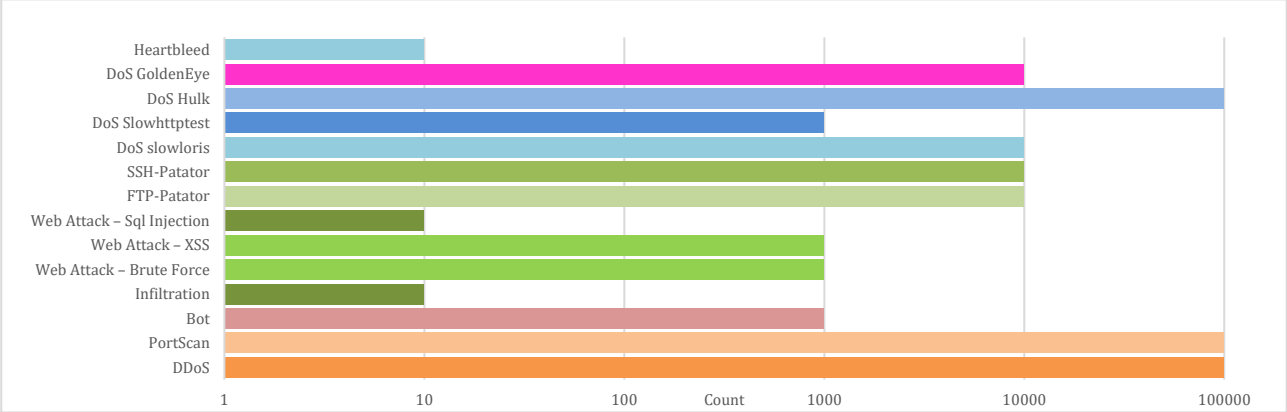

Fig. 2: Distribution of attacks in the dataset

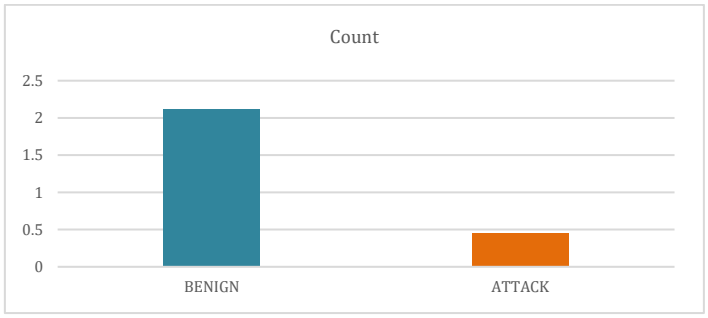

Fig. 3: Classification of the data

Table 1: Dataset details

	a	b	c	d	e	f	g	h	i	j
0	54865	3	2	0	12	0	6	6	6.0	0.0
1	55054	109	1	1	6	6	6	6	6.0	0.0
2	55055	52	1	1	6	6	6	6	6.0	0.0
3	46236	34	1	1	6	6	6	6	6.0	0.0
4	54863	3	2	0	12	0	6	6	6.0	0.0

a: Destination port; b: Flow duration; c: Total Fwd. packets; d: Total backward packets; e: Total length of Fwd. packets; f: Total length of Bwd. packets; g: Fwd. packet length max; h: Fwd. packet length min; i: Fwd. packet length mean; j: Fwd. packet length Std

3.2. Data pre-processing and feature extraction

Effective analysis and operation require high-quality data. Thus, it was necessary to process the collected information and extract the relevant features before it was used for intrusion detection. This phase involved a series of processes designed to clean, develop, and standardize the data, making it ready for further analysis. Preprocessing typically involves processing missing values, normalizing variables, and converting categorical data to numerical values in a mixed dataset that includes both numerical and categorical variables. Addressing the issue of incomplete or missing data is crucial in data preparation, as they can adversely affect the performance of ML algorithms. Employing

techniques such as imputation, in which missing values are filled in using estimates derived from available data, or opting to discard incomplete records based on the severity of data loss, are both viable strategies (Burkov, 2019). The normalization step is particularly vital for numerical attributes to ensure that all variables are on a similar scale. Such normalization enhances the uniformity and effectiveness of the ML model, preventing any single feature from exerting undue influence during the training phase. Techniques such as min-max scaling and z-score standardization, in which values are adjusted by subtracting the mean and dividing by the standard deviation, are commonly used data normalization methods (Sangodoyin et al., 2021).

To ensure high-quality input data for the ML models, multiple preprocessing steps were applied to the dataset:

1. Handling missing values: Any rows with missing values were examined. If a feature had more than 20% missing data, it was removed. For features with minor missing values, missing data were imputed using the mean (for numerical features) or mode (for categorical features).
2. Encoding categorical variables: The dataset included categorical features, such as attack labels. These were converted into numerical values using one-hot encoding for multiclass labels.
3. Feature scaling and normalization: Because the dataset had features with different numerical ranges, min-max scaling was applied to normalize the values between 0 and 1 to prevent any bias toward larger numerical values.
4. Feature selection: The dataset contained redundant and highly correlated features. Using the variance inflation factor (VIF) and Pearson correlation, highly correlated features (>.85) were removed to reduce multicollinearity and improve model performance.
5. Data augmentation: No artificial data augmentation was performed in this study. However, since the dataset had an imbalance between attack and normal traffic, SMOTE was applied to balance the minority attack classes and improve the model generalization.
6. Splitting the dataset: The preprocessed dataset was split into 80% training and 20% testing data using stratified sampling to ensure that both attack and normal traffic instances were proportionally represented in both sets.

The implementation code was as follows:

```
# Step 1: Handle missing values
# Drop columns with more than 20% missing values
df.dropna(thresh=len(df) * 0.8, axis=1, inplace=True)
# Fill remaining missing values with the column mean
df.fillna(df.mean(), inplace=True)

# Step 2: Encode categorical labels
from sklearn.preprocessing import LabelEncoder
df["Label"] = LabelEncoder().fit_transform(df["Label"])

# Step 3: Normalize numerical features
from sklearn.preprocessing import MinMaxScaler
scaler = MinMaxScaler()
numeric_columns = df.select_dtypes(include=['float64', 'int64']).columns
df[numeric_columns] = scaler.fit_transform(df[numeric_columns])

# Step 4: Handle class imbalance using SMOTE
from imblearn.over_sampling import SMOTE
X = df.drop(columns=["Label"])
y = df["Label"]
X_resampled, y_resampled = SMOTE().fit_resample(X, y)

# Step 5: Split the dataset into training and testing sets (80/20 split)
from sklearn.model_selection import train_test_split
X_train, X_test, y_train, y_test = train_test_split(
    X_resampled, y_resampled, test_size=0.2, stratify=y_resampled
)
```

These preprocessing steps ensured that the dataset was cleaned, balanced, and optimized for the ML model training.

3.3. ML model training

The process of training predictive models for intrusion detection spans several stages, from data preparation to evaluating model efficacy. Initially, a dataset is processed to scale the numerical features and divide the dataset into test and training sets. Subsequently, the balance of classes was adjusted to ensure an accurate representation of both benign and malicious instances. In this study, the data were divided into test and training sets using the "train_test_split" function in "sklearn.model_selection." Once this process was completed, the ML models were trained. To optimize performance, the hyperparameters of these classifiers, such as minimum sample leaf and depth range for the RF classifier and loss function and regularization penalty for the SGD classifier, were fine-tuned (Pal and Patel, 2020). After training, the classification models for both methods were evaluated using the test set. Performance metrics, including accuracy, were employed to gauge the ability of the models to classify normal traffic and attack scenarios.

4. Results and discussion

In this section, the results from the experiments carried out by building the ML models for a typical IDS are presented. Specifically, we employed the SGD and RF classification models to categorize cyberattacks in IoT environments. The accuracy, precision, recall, and F1 score metrics of the SDG and RF classifiers are presented to indicate the potential of ML techniques to enhance IoT security by detecting cyberphysical threats. From Table 2, it can be seen that the SGD classifier had an accuracy of 93.6%, a precision of 93.8%, a recall of 92% and an F1 score of 96%, indicating that this model was able to proficiently classify cyberattacks.

Table 2: Performance metrics of SGD and RF classifiers

Classifier	Accuracy	Precision	Recall	F1-score
SGD	0.936	0.938	0.917	0.960
RF	0.995	0.995	0.998	0.992

However, the RF classifier outperformed the SGD classifier. Specifically, the RF classifier had an accuracy of 99.5%, a precision of 99.5%, a recall of 99.8%, and an F1 score of 99.2%. These performance metrics also indicate that the RF classification model was able to proficiently classify cyberattacks.

4.1. Proposed vs. existing IDS approaches

Traditional IDSs for IoT/CPS environments often rely on signature-based or anomaly-based detection mechanisms. Signature-based IDSs, while effective against known attacks, struggle to detect novel threats. Anomaly-based methods, often utilizing statistical or heuristic techniques, can generate a high rate of false positives. Recent advancements have introduced ML-based IDSs, which improve adaptability but often require extensive computational resources.

The proposed approach integrated RF and the SGD classifier, achieving a balance between high detection accuracy and computational efficiency. By leveraging feature extraction and data preprocessing, our IDS minimizes false positives while maintaining high detection rates. This makes it particularly suitable for resource-constrained IoT/CPS environments, where real-time intrusion detection is critical.

4.2. Performance analysis: Why RF outperformed SGD

The RF model achieved 99% accuracy, considerably outperforming the SGD classifier (93%) in detecting intrusions in the IoT/CPS environment. This performance difference can be attributed to the following:

1. Robustness to non-linearity. RF is an ensemble learning method that constructs multiple decision trees, making it more effective in handling non-linear decision boundaries in complex intrusion detection tasks. In contrast, SGD assumes linear separability and performs well when feature relationships are mostly linear but struggles with complex attack patterns.
2. Feature importance and handling of high-dimensional data. RF automatically selects important features, reducing the impact of irrelevant or noisy data, which are common in intrusion datasets. SGD does not perform intrinsic feature selection and is more sensitive to redundant and noisy features, leading to reduced performance.
3. Handling of imbalanced data. RF is more resilient to class imbalance, as it assigns different weights to minority classes, improving the detection of rare cyber threats. SGD is prone to bias toward majority classes, affecting recall and overall detection capability.
4. Stability and generalization. RF's averaging of multiple decision trees prevents overfitting and provides stable predictions, even with noisy data. SGD updates weights iteratively and is highly sensitive to hyperparameters, requiring careful tuning to avoid poor generalization.
5. Practical implications for IDSs. In real-world IDSs, low false-positive rates and robust attack classification are essential. The high accuracy of RF makes it suitable for deployment in resource-constrained IoT environments in which real-time, low-latency detection is required. However, SGD's efficiency and lower computational costs make it a good choice when fast, lightweight detection is prioritized over slightly higher accuracy.

4.3. Why not use deep learning instead?

The computational complexity of deep learning-based IDS models (i.e., artificial neural networks [ANNs]) requires significant processing power, making them impractical for real-time IoT security applications. With regard to data requirements, ANNs need large, labeled datasets for training, whereas RF and SGD perform well even with a few labeled data. RF provides feature importance insights, making it easier for cybersecurity analysts to understand the detection logic, unlike deep learning models, which act as black boxes. RF was chosen because it outperformed SGD in accuracy, handled imbalanced data well, and was interpretable, making it ideal for CPS security. SGD was still valuable for lightweight IDS implementations requiring faster detection with fewer computational resources. Deep-learning models could be explored in future work for IDSs with real-time adaptive learning, but their high resource requirements limit current practical deployment in IoT environments. An overview of the comparisons among these techniques is provided in Table 3.

4.4. Statistical validation of classifier performance

To ensure the reported accuracy improvements were statistically significant, we conducted confidence interval analysis and hypothesis testing to compare the RF and SGD classifiers.

4.4.1. Confidence interval for accuracy

A 95% confidence interval (CI) provides a range within which the true accuracy of the model is expected to lie. The formula for a CI is as follows:

$$\text{CI} = p\hat{} \pm Z\sqrt{p(1-p)/n}$$

where, p^ is the accuracy of the model, Z is 1.96 (for a 95% CI), and n is the number of test samples.

Using this method, the RF accuracy was 99.5%, and its 95% confidence interval was [99.3%, 99.8%]. The SGD accuracy was 93.6%, and its 95% confidence interval was [92.8%, 94.4%]. The non-overlapping confidence intervals indicate that the difference in accuracy was statistically significant, supporting the claim that RF outperformed SGD.

Table 3: Comparison of the described ML models and a deep-learning approach

Model	Advantages	Disadvantages
RF classifier	High accuracy (99%), robust to noise, interpretable, and low tuning effort	Slower training for large datasets and memory intensive
SGD classifier	Fast training, works well with sparse data, and low memory usage	Lower accuracy (93%), sensitive to hyperparameters, and struggles with complex data
Deep learning	Can learn complex patterns, adaptive to dynamic attacks, and effective for large-scale IDSs	Computationally expensive, requires large labeled datasets, and risks overfitting

4.4.2. Hypothesis testing (p-value calculation)

To formally compare the RF and SGD models, we used the hypothesis test for a difference of proportions. The null and alternative hypotheses were as follows:

H0: Accuracy (RF)= Accuracy (SGD)
Ha: Accuracy (RF)> Accuracy (SGD)

Using a z-test to compare the proportions, we computed the p-value to measure the likelihood that the observed difference in accuracy occurred by chance. A p-value ≤.05 would indicate a significant difference (thus, we would reject H0). A p-value >.05 would indicate no significant difference (thus, we would fail to reject H0). The p-value obtained was <.001, confirming that the accuracy of the RF model was significantly higher than the accuracy of the SGD model.

4.5. Real-world challenges and future scalability improvements

4.5.1. Deployment challenges in real-world IDSs

While the proposed IDS achieved high accuracy and strong detection capabilities, deploying it in real-world IoT/CPS environments poses several challenges:

1. Computational constraints: Many IoT devices have limited processing power and memory, making it difficult to run computationally expensive models, such as RF. Edge computing solutions may be required to balance performance and resource efficiency.
2. Many false positives in dynamic environments: While RF offers high accuracy, IDS solutions deployed in dynamic, real-time systems need to minimize false positives, which can lead to unnecessary alerts and system slowdowns. An adaptive threshold tuning mechanism can help refine detection sensitivity.
3. Data imbalance and evolving threats: New cyber threats continuously emerge, requiring IDS models to be adapted and updated in real time. A static ML model might struggle to detect zero-day attacks. Integrating online learning techniques or periodically retraining models can help.
4. Scalability issues in large-scale networks: When deployed across multiple IoT devices and CPS networks, managing data collection and processing the data efficiently becomes a challenge. Implementing a distributed IDS architecture in which models run on edge devices and communicate with a central system can improve scalability.

4.5.2. Future improvements for scalability

To enhance the proposed IDS for large-scale, real-world deployment, the following improvements can be considered:

1. Lightweight model optimization: Deploying compressed versions of RF (e.g., using model pruning or knowledge distillation) can reduce computational overhead. Implementing ensemble learning with simpler models (e.g., decision trees + naïve Bayes) may offer a balance between accuracy and efficiency.
2. Integration with edge computing: Running an IDS on edge nodes rather than centralized cloud servers can reduce latency and allow real-time threat detection. Edge-based feature extraction can reduce the amount of data sent for processing, saving bandwidth and improving response time.
3. Adaptive learning for zero-day attack detection: Implementing semi-supervised learning or reinforcement learning techniques can help an IDS detect evolving attack patterns. A feedback loop from human analysts can continuously fine-tune detection thresholds and improve accuracy.
4. Blockchain-based IDS for trust and security: Using blockchain technology to secure IDS logs and communications can prevent tampering and ensure data integrity. A decentralized approach can enhance the trustworthiness of intrusion reports and attack mitigation strategies.

5. Conclusion

Leveraging accessible open-source data, ML models (i.e., RF and SGD classifiers) were deployed in typical practical scenarios to illustrate the substantial advantages of detecting security infractions in IoT/CPS environments. The methodology adopted involved standard ML

procedures for the handling of missing entries and normalization of the variables during the preprocessing stage, followed by the training of the ML models using the collected data. The SGD classifier was effective, identifying attack scenarios with a 93.6% accuracy rate, and it had high precision, recall, and F1 scores. However, the RF classifier surpassed the SGD model, having better results in terms of precision, recall, and F1 scores, and a higher accuracy rate of 99.5%. This revealed the RF model's exceptional potential in accurately classifying cyberattacks while keeping false positives and negatives to a minimum, while protecting IoT/CPS environments. The performance analysis highlighted that SGD was computationally efficient but struggled with class imbalance and non-linearity, making RF the preferred choice for high-accuracy intrusion detection. Additionally, statistical validation using confidence interval analysis and hypothesis testing ($p<.001$) confirmed the statistical significance of the RF model's higher accuracy. The comparative analysis further highlighted the RF model's superiority in terms of its reliability and effectiveness in detecting breaches within IoT/CPS security frameworks. To further enhance security robustness in IoT/CPS environments, additional experimentation and assessments may be necessary to investigate other essential factors that affect model performance and to refine the proposed intrusion detection architecture presented in this work.

Acknowledgment

The authors would like to acknowledge the Deanship of Graduate Studies and Scientific Research, Taif University, for funding this work.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Alangari S (2024). An unsupervised machine learning algorithm for attack and anomaly detection in IoT sensors. Wireless Personal Communications. https://doi.org/10.1007/s11277-023-10811-8

Alqaralleh BA, Aldhaban F, AlQarallehs EA, and Al-Omari AH (2022). Optimal machine learning enabled intrusion detection in cyber-physical system environment. Computers, Materials and Continua, 72(3): 4691-4707. https://doi.org/10.32604/cmc.2022.026556

Altulaihan E, Almaiah MA, and Aljughaiman A (2024). Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms. Sensors, 24(2): 713. https://doi.org/10.3390/s24020713 **PMid:38276404 PMCid:PMC10820271**

Aly M, Khomh F, Haoues M, Quintero A, and Yacout S (2019). Enforcing security in Internet of Things frameworks: A systematic literature review. Internet of Things, 6: 100050. https://doi.org/10.1016/j.iot.2019.100050

Ashibani Y and Mahmoud QH (2017). Cyber physical systems security: Analysis, challenges and solutions. Computers and Security, 68: 81-97. https://doi.org/10.1016/j.cose.2017.04.005

Baskaran SBM, Arumugam S, and Prasad AR (2019). Internet of things security. Journal of ICT Standardization, 7(1): 21-42. https://doi.org/10.13052/jicts2245-800X.712

Bertoli GDC, Júnior LAP, Saotome O, Dos Santos AL, Verri FAN, Marcondes CAC, Barbieri S, Rodrigues MS, and De Oliveira JMP (2021). An end-to-end framework for machine learning-based network intrusion detection system. IEEE Access, 9: 106790-106805. https://doi.org/10.1109/ACCESS.2021.3101188

Blasch E, Kadar I, Grewe LL, Brooks R, Yu W, Kwasinski A, Thomopoulos S, Salerno J, and Qi H (2017). Panel summary of cyber-physical systems (CPS) and internet of things (IoT) opportunities with information fusion. In the Signal Processing, Sensor/Information Fusion, and Target Recognition XXVI, SPIE, Anaheim, USA, 1020000: 171-188. https://doi.org/10.1117/12.2264683

Burg A, Chattopadhyay A, and Lam KY (2017). Wireless communication and security issues for cyber–physical systems and the Internet-of-Things. Proceedings of the IEEE, 106(1): 38-60. https://doi.org/10.1109/JPROC.2017.2780172

Burkov A (2019). The hundred-page machine learning book. Volume 1, Andriy Burkov, Quebec City, Canada.

Colelli R, Magri F, Panzieri S, and Pascucci F (2021). Anomaly-based intrusion detection system for cyber-physical system security. In the 29th Mediterranean Conference on Control and Automation (MED), IEEE, PUGLIA, Italy: 428-434. https://doi.org/10.1109/MED51440.2021.9480182

Cram WA, Proudfoot JG, and D'arcy J (2017). Organizational information security policies: A review and research framework. European Journal of Information Systems, 26(6): 605-641. https://doi.org/10.1057/s41303-017-0059-9

Djenna A, Harous S, and Saidouni DE (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10): 4580. https://doi.org/10.3390/app11104580

Dorado G, Gálvez S, and del Pilar Dorado M (2021). Computer firewalls: Security and privacy protection for Mac: Review. Big Data and Information Analytics, 6: 1-11. https://doi.org/10.3934/bdia.2021001

Douiba M, Benkirane S, Guezzaz A, and Azrour M (2023). An improved anomaly detection model for IoT security using decision tree and gradient boosting. The Journal of Supercomputing, 79(3): 3392-3411. https://doi.org/10.1007/s11227-022-04783-y

Elhanashi A, Gasmi K, Begni A, Dini P, Zheng Q, and Saponara S (2023). Machine learning techniques for anomaly-based detection system on CSE-CIC-IDS2018 dataset. In: Berta R and De Gloria A (Eds.), Applications in electronics pervading industry, environment and society: 131-140. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-031-30333-3_17

El-Kady AH, Halim S, El-Halwagi MM, and Khan F (2023). Analysis of safety and security challenges and opportunities related to cyber-physical systems. Process Safety and Environmental Protection, 173: 384-413. https://doi.org/10.1016/j.psep.2023.03.012

Gadal S, Mokhtar R, Abdelhaq M, Alsaqour R, Ali ES, and Saeed R (2022). Machine learning-based anomaly detection using K-mean array and sequential minimal optimization. Electronics, 11(14): 2158. https://doi.org/10.3390/electronics11142158

Gupta BB and Quamara M (2020). An overview of Internet of things (IoT): Architectural aspects, challenges, and protocols. Concurrency and Computation: Practice and Experience, 32(21): e4946. https://doi.org/10.1002/cpe.4946

Hao W, Yang T, and Yang Q (2021). Hybrid statistical-machine learning for real-time anomaly detection in industrial cyber–physical systems. IEEE Transactions on Automation Science and Engineering, 20(1): 32-46. https://doi.org/10.1109/TASE.2021.3073396

Hyder B, Ahmed A, Mana P, Edgar T, and Niddodi S (2023). Leveraging high-fidelity datasets for machine learning-based anomaly detection in smart grids. In the 11th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems, IEEE, San Antonio, USA: 1-6. https://doi.org/10.1109/MSCPES58582.2023.10123428

Kahmann F, Dreyer J, and Toenjes R (2023). Dynamic VLAN-tagging approach for IoT Network Segmentation and ad-hoc Connectivity. In the 27th ITG-Symposium: Mobile Communication-Technologies and Applications, VDE, Osnabrück, Germany: 55-60.

Kaur A, Singh G, Kukreja V, Sharma S, Singh S, and Yoon B (2022). Adaptation of IoT with blockchain in food supply chain management: An analysis-based review in development, benefits and potential applications. Sensors, 22(21): 8174. https://doi.org/10.3390/s22218174 **PMid:36365871 PMCid:PMC9655358**

Khan MM and Alkhathami M (2024). Anomaly detection in IoT-based healthcare: Machine learning for enhanced security. Scientific Reports, 14: 5872. https://doi.org/10.1038/s41598-024-56126-x **PMid:38467709 PMCid:PMC10928137**

Kimani K, Oduol V, and Langat K (2019). Cyber security challenges for IoT-based smart grid networks. International Journal of Critical Infrastructure Protection, 25: 36-49. https://doi.org/10.1016/j.ijcip.2019.01.001

Kirubakaran S, Maheswari K, Bhavani M, Syamsundar C, Rani BS, and Raju KS (2024). A significant and enhanced machine learning algorithm by using feature selection network intrusion identification and detection. In the 5th International Conference on Data Intelligence and Cognitive Informatics, IEEE, Tirunelveli, India: 593-597. https://doi.org/10.1109/ICDICI62993.2024.10810806

Kizza JM (2024). System intrusion detection and prevention. In: Kizza JM (Ed.), Guide to computer network security: 295-323. Springer International Publishing, Cham, Switzerland. https://doi.org/10.1007/978-3-031-47549-8_13

Lai T, Farid F, Bello A, and Sabrina F (2024). Ensemble learning based anomaly detection for IoT cybersecurity via Bayesian hyperparameters sensitivity analysis. Cybersecurity, 7: 44. https://doi.org/10.1186/s42400-024-00238-4

Lesch V, Züfle M, Bauer A, Iffländer L, Krupitzer C, and Kounev S (2023). A literature review of IoT and CPS—What they are, and what they are not. Journal of Systems and Software, 200: 111631. https://doi.org/10.1016/j.jss.2023.111631

Makhdoom I, Abolhasan M, Lipman J, Liu RP, and Ni W (2018). Anatomy of threats to the Internet of Things. IEEE Communications Surveys and Tutorials, 21(2): 1636-1675. https://doi.org/10.1109/COMST.2018.2874978

Malik AK, Emmanuel N, Zafar S, Khattak HA, Raza B, Khan S, Al-Bayatti AH, Alassafi MO, Alfakeeh AS, and Alqarni MA (2020). From conventional to state-of-the-art IoT access control models. Electronics, 9(10): 1693. https://doi.org/10.3390/electronics9101693

Nguyen TT and Reddi VJ (2021). Deep reinforcement learning for cyber security. IEEE Transactions on Neural Networks and Learning Systems, 34(8): 3779-3795. https://doi.org/10.1109/TNNLS.2021.3121870 **PMid:34723814**

Nour AA, Mehbodniya A, Webber JL, Bostani A, Shah B, and Ergashevich BZ (2023). Optimizing intrusion detection in industrial cyber-physical systems through transfer learning approaches. Computers and Electrical Engineering, 111: 108929. https://doi.org/10.1016/j.compeleceng.2023.108929

Omolara AE, Alabdulatif A, Abiodun OI, Alawida M, Alabdulatif A, Alshoura WH, and Arshad H (2022). The internet of things security: A survey encompassing unexplored areas and new insights. Computers and Security, 112: 102494. https://doi.org/10.1016/j.cose.2021.102494

Pal K and Patel BV (2020). Emotion classification with reduced feature set sgdclassifier, random forest and performance tuning. In: Chaubey N, Parikh S, and Amin K (Eds.), Computing science, communication and security: 95-108. Springer, Singapore, Singapore. https://doi.org/10.1007/978-981-15-6648-6_8

Pütz P, Mitev R, Miettinen M, and Sadeghi AR (2023). Unleashing iot security: Assessing the effectiveness of best practices in protecting against threats. In the 39th Annual Computer Security Applications Conference, Association for Computing Machinery, Austin, USA: 190-204. https://doi.org/10.1145/3627106.3627133

Ramachandran A, Gayathri K, Alkhayyat A, and Malik RQ (2023). Aquila optimization with machine learning-based anomaly detection technique in cyber-physical systems. Computer Systems Science and Engineering, 46(2): 2177–2194. https://doi.org/10.32604/csse.2023.034438

Rodriguez E, Otero B, Gutierrez N, and Canal R (2021). A survey of deep learning techniques for cybersecurity in mobile networks. IEEE Communications Surveys and Tutorials, 23(3): 1920-1955. https://doi.org/10.1109/COMST.2021.3086296

Sangodoyin AO, Akinsolu MO, Pillai P, and Grout V (2021). Detection and classification of DDoS flooding attacks on software-defined networks: A case study for the application of machine learning. IEEE Access, 9: 122495-122508. https://doi.org/10.1109/ACCESS.2021.3109490

Santos VF, Albuquerque C, Passos D, Quincozes SE, and Mossé D (2023). Assessing machine learning techniques for intrusion detection in cyber-physical systems. Energies, 16(16): 6058. https://doi.org/10.3390/en16166058

Saranya T, Sridevi S, Deisy C, Chung TD, and Khan MA (2020). Performance analysis of machine learning algorithms in intrusion detection system: A review. Procedia Computer Science, 171: 1251-1260. https://doi.org/10.1016/j.procs.2020.04.133

Selmy HA, Mohamed HK, and Medhat W (2024). Big data analytics deep learning techniques and applications: A survey. Information Systems, 120: 102318. https://doi.org/10.1016/j.is.2023.102318

Sfar AR, Natalizio E, Challal Y, and Chtourou Z (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2): 118-137. https://doi.org/10.1016/j.dcan.2017.04.003

Sha K, Wei W, Yang TA, Wang Z, and Shi W (2018). On security challenges and open issues in Internet of Things. Future Generation Computer Systems, 83: 326-337. https://doi.org/10.1016/j.future.2018.01.059

Sharma S, Tyagi R, and Bhardwaj R (2023). Sustainable smart society development based on geo sensitive equality using Vedic structure, artificial intelligence, blockchain and IoT. In the 1st International Conference on Circuits, Power and Intelligent Systems, IEEE, Bhubaneswar, India: 1-6. https://doi.org/10.1109/CCPIS59145.2023.10291593

Shaukat K, Luo S, Varadharajan V, Hameed IA, Chen S, Liu D, and Li J (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, 13(10): 2509. https://doi.org/10.3390/en13102509

Tushkanova O, Levshun D, Branitskiy A, Fedorchenko E, Novikova E, and Kotenko I (2023). Detection of cyberattacks and anomalies in cyber-physical systems: Approaches, data sources, evaluation. Algorithms, 16: 85. https://doi.org/10.3390/a16020085

Tyagi AK and Sreenath N (2021). Cyber physical systems: Analyses, challenges and possible solutions. Internet of Things

and Cyber-Physical Systems, 1: 22-33. https://doi.org/10.1016/j.iotcps.2021.12.002

Vigoya L, Pardal A, Fernandez D, and Carneiro V (2023). Application of machine learning algorithms for the validation of a new CoAP-IoT anomaly detection dataset. Applied Sciences, 13(7): 4482. https://doi.org/10.3390/app13074482

Xin Y, Kong L, Liu Z, Chen Y, Li Y, Zhu H, Gao M, Hou H, and Wang C (2018). Machine learning and deep learning methods for cybersecurity. IEEE Access, 6: 35365-35381. https://doi.org/10.1109/ACCESS.2018.2836950

Yaacoub JPA, Salman O, Noura HN, Kaaniche N, Chehab A, and Malli M (2020). Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and Microsystems, 77: 103201. https://doi.org/10.1016/j.micpro.2020.103201 **PMid:32834204 PMCid:PMC7340599**

Yang T, Jiang Z, Liu P, Yang Q, and Wang W (2023). A traffic anomaly detection approach based on unsupervised learning for industrial cyber–physical system. Knowledge-Based Systems, 279: 110949. https://doi.org/10.1016/j.knosys.2023.110949

Yang W, Wang S, Sahri NM, Karie NM, Ahmed M, and Valli C (2021). Biometrics for Internet-of-Things security: A review. Sensors, 21(18): 6163. https://doi.org/10.3390/s21186163 **PMid:34577370 PMCid:PMC8472874**

Zhou Y, Yu FR, Chen J, and Kuo Y (2019). Cyber-physical-social systems: A state-of-the-art survey, challenges and opportunities. IEEE Communications Surveys and Tutorials, 22(1): 389-425. https://doi.org/10.1109/COMST.2019.2959013