AJEMA GLOBAL RESEARCH NETWORK

AMERICAN Journal of Engineering, Mechanics and Architecture
Volume 2, Issue 10, 2024 ISSN (E): 2993-2637

Network Security for Cyber-Physical Systems Using Deep Neural Network-Based Anomaly Detection

Maytham Mohammed Tuaama
Imam Al-Kadhum College (IKC), Department of Computer Technical Engineering

Abstract: In recent years, Cyber-Physical Systems (CPS) have seen explosive growth in popularity thanks to their many practical uses. Network security and user privacy are key concerns while deploying CPS networks because of the high number of internet-connected devices in such an ecosystem, which makes them more susceptible to cyber-attacks. An effective and efficient Intrusion Detection System (IDS) might be a feasible way to defend CPS networks from different threats. This study proposes a new intrusion detection system (IDS) for Cyber-Physical Systems networks that uses deep learning to detect anomalies. In particular, we have introduced a Deep Neural Network (DNN) model for filter-based feature selection that drops features with strong correlations.

In addition, several parameters and hyperparameters are used to fine-tune the model. The UNSW-NB15 dataset, which includes four types of attacks, is used for this. To address class imbalance concerns in the dataset, the suggested model was trained using Generative Adversarial Networks (GANs). It then generated synthetic data of minority assaults and attained a 98% accuracy rate with the balanced class dataset.

Keywords: CPS; DNN; DL; ML; Cyber-Physical Systems; Deep Neural Network.

1. INTRODUCTION

Cyber-Physical Systems (CPS) play an important role in smart grids, healthcare, and various industry applications[1]. However, there are several challenges, including the vulnerability of protocols and service frameworks used in CPS. Wireless networks with characteristics such as low cost, fast deployment, mobility, flexible connection, and service compared to wired networks are widely used [2]. However, they are still a popular target for attacks because they have weaknesses such as open environments, lack of centralized management, widely available attack tools, and not all security mechanisms functioning. Attacks that exploit the vulnerabilities of wireless networks can lead to information leakage, connection interference, denial of service, and control signal manipulations[3]. Therefore, various studies are being conducted to enhance the level of security of wireless networks. However, all existing methods have vulnerabilities, and new methods are required for unknown attacks [4].

Deep learning-based intrusion detection that shares learning data through accuracy improvement with fewer features shows the potential of being a good classifier while ensuring higher accuracy[5]. However, prior work using DNN for anomaly-based intrusion detection includes various hand-crafted algorithms for preprocessing the raw input data. Given this purpose, we propose a deep learning-based anomaly detection scheme. Specifically, we utilize an autoencoder-based neural network structure to extract higher abstract features prior to the

training process. The training process is conducted through the extracted features to achieve better performance than those obtained from conventional hand-crafted preprocessing [6]. It is worth noting that the higher abstract features lead to better classification results if the feature space is well clustered. The proposed method, as well as the baseline approaches, is evaluated using a simulation. Our process ensures higher accuracy in simulated scenarios compared to the baseline schemes.

1.1. Overview of Cyber-Physical Systems (CPS)

Cyber-physical systems (CPS) are systems that tightly integrate cyber capabilities with physical components in smart motion systems and smart control systems[7]. While the first layer of the smart motion system includes the mechanical components such as steps, joints, links, etc., the second layer includes the physical controllers for motion control, which are the analog and digital electronic devices and the actuators, and the third layer comprises the sensory monitoring devices in the form of smart sensors and image sensors [8]. The first layer in the smart control system has the power management components, including the energy harvesting modules and the power storage devices; the second layer houses the physical controllers for stability analysis and networked/adaptive control and the sensor signal conditioning, followed by the third layer that includes ultrasonic, video, and lightwave communication devices for nearest neighbor and end-to-end communication [9].

There are significant design challenges for preserving the integrity, security, and safety of networked cyber-physical layered structures in smart motion systems or control systems [10]. Cybersecurity is an increase in complexity and requires that a new layer consisting of security monitors and anomaly detectors be added to the physical layer control system, which leads to a new concept of cyber-physical security monitoring[11].

1.2. Importance of Network Security in CPS

Cyber-Physical Systems (CPS) are crucially important to the public in the form of transportation, communication, energy, and manufacturing. As a result, cyber and physical elements are increasingly merging, and an infrastructure that integrates network and systems management and security technologies is enabling CPS[1], [12]. In addition, however, the integration of CPS makes it easier to interfere with psychological or physical systems by attacking digital systems over the network. The act of taking over control decisions inappropriately and altering the actual states of physical systems is called network intrusion or attack [13]. A number of network intrusions have already occurred that have succeeded in affecting physical systems. As concern grows worldwide over the security of CPS, a plethora of research is underway to resolve security problems related to CPS [14]. Many of these studies are designed to solve security problems by specifically integrating the operating systems or communication technologies that serve as components in CPS [15]. The primary method to defend CPS is to prevent cyber-attacks on CPS components such as firewalls, intrusion detection systems, and intrusion prevention systems. However, since general security technologies cannot completely guarantee the security of CPS, a new security method tailored to CPS, called deep learning-based anomaly detection, is needed.

2. DEEP LEARNING AND NEURAL NETWORKS

A kind of machine learning known as "deep learning" trains models to learn representations of data and one of its cornerstones, neural networks. In general, deep learning uses multiple layers to learn higher-level representations that make sense of the data. These methods specialize in one kind of representation learning and can be seen as methods of compressing data into multiple layers of learned intermediate features[16] [17].

Deep learning models consist of neural networks: A core concept of deep learning is neural networks. In a numerical representation of a biological brain, numerous artificial neurons are connected with each other to mimic the learning process as human neurons do. The input layer

receives signals and the output signals diverge into output units where pairs of activation and weight form. Activation refers to responders and weight refers to a channel of information [18].

In deep learning, neural networks consist of many layers. These layers include an input layer, hidden layers, and an output layer, as shown in Figure 1. The layers are used to compute the input feature into the next layers. Each layer includes intermediate activations that are generally used for computation[19].

In a linear system, the output of a layer can be represented mathematically as a linear combination of the input. From primitive layer models to advanced layer models, all layer models use the same kind of equation [20]. However, the equation is different among uncomplicated versus viable systems.

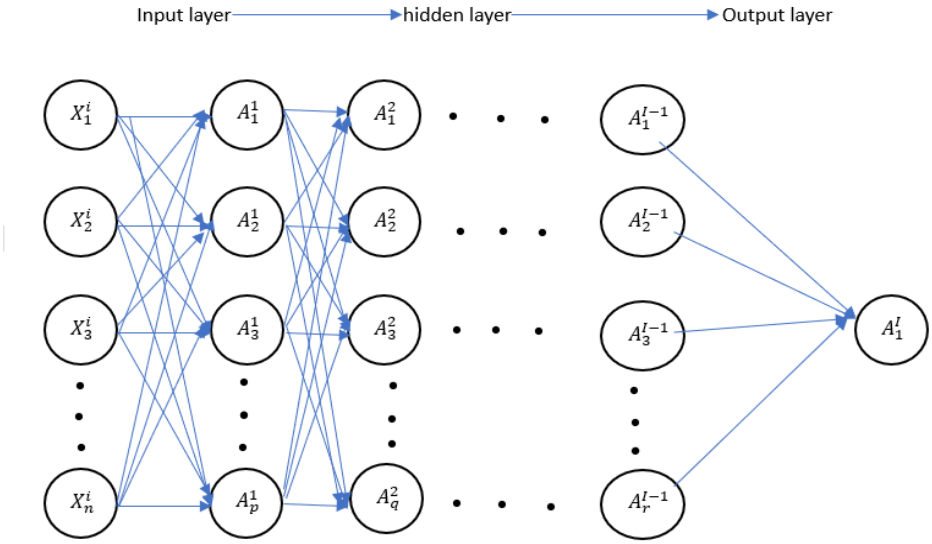

Fig .1 DNN Architecture

2.1. Introduction to Deep Learning

As the depth of architectures for neural networks becomes deeper, their abilities also improve. Particularly, learning ability and discrimination ability are dramatically enhanced[21]. The potential of deep architectures is a subject of much revived interest. Noticeably, deep learning reveals its state-of-the-art performance in many complex image problems[16], [22]. Furthermore, deep architectures are applied in practical use for search engines and speech recognition. If the concepts regarding deep learning are well understood, correctly implementing deep learning algorithms is a significant issue. The training duration of deep architectures takes a considerable amount of time on conventional resources[23] . An obstacle to attaining state-of-the-art performance using deep models is the time-consuming restrictions of the training process. With the rapid increase in the architecture size of deep models, deep learning models are designed with millions of weights and billions of neurons [24]. Although high performance is achieved using large models, the impetus behind this issue stems from both human understanding and modern computer technologies[25] . The learning capability becomes remarkable, without demonstrating deep human knowledge. Until now, many shallow networks shared parameters or only one layer had been adopted[26]. However, the concept of state-of-the-art deep learning is merely a good idea. Based on a simple scaling model, the large size of the network contributes to high performance as well as a single parameter effect. Proper scaling makes the weights of deep architectures converge to reasonable ranges[27] [24]. Even though a large model is properly based, the power of deep learning is driven by the computations that an extensive computer system requires. The research cannot utilize deep learning to significant effects in other systems that do not have resources for recent capabilities. Inexpensive deep learning becomes impractical in real life[28]. Thanks to recent massively parallel computation power, enormous energy and

time are consumed on extremely expensive cloud computation services. Neural network models with their training data require an inordinate amount of resources and time. With the growth of devices, the learning capability using their private data is proven with a considerable amount. Only large organized companies possess their external computing power outside the computer power needed for deep learning. In their own way, abilities for deep learning are reserved [29].

2.2. Types of Neural Networks

There are various types of DNNs that can be utilized to conduct ADE for CPS network security. The most commonly used types either consist of feedforward neural networks with fully connected layers, while others are derived from this structure by applying different types of constraints on the trainable parameters, such as convolutions, recurrent connections, or sparsity [30]. FFNNs consist of a stack of layers that are interconnected with each other. Each of the interconnected layers is trained to output the true class label that each input image instance belongs to, or to determine the discrete values of a given input data set[31], [32] .

In order to accomplish this, the first layer of the FFNN receives the sensors' raw measurements as input. The output of each layer is then computed by applying continuous transformations on the input data followed by the use of a fixed nonlinear function. After passing through a number of layers, the predictions are made by the final layer [33]. In CNNs, rather than using fully connected layers, consecutive layers are partially connected with banks of learnable convolutional kernels, which are usually used to identify the presence of specific types of features in the input data [34]. RNNs utilize cyclic connections across layers that allow for the propagation of previous hidden states, which makes them particularly effective in capturing temporal dependencies inherent in naturally occurring sequential data sets such as audio, text, or time series[35] .

3. ANOMALY DETECTION IN CPS

Anomaly detection plays a critical role in protecting network security in cyber-physical systems (CPS), especially for detecting unknown or hidden security threats that are difficult to model[36] . However, anomaly detection in CPS is challenging due to the high-dimensional time series and spatial-temporal data characteristics. Traditional anomaly detection focuses on feature extraction, feature selection, and classifier design, generally using shallow-structured classifiers [37]. This paper provides an alternative CPS network security solution using deep learning.

Cyber-physical systems (CPS) provide the foundational technology for smart cities, smart grids, linked automobiles, and industrial control systems[38]. Security incidents have been on the rise in recent years, indicating that CPS security is growing in importance. Typically, security measures begin with anomaly detection[39]. However, ensuring the security of CPS poses significant challenges.

Firstly, CPS is more intricate than older forms of computer systems. Because of its cyber and physical components, anomaly detection is considerably more difficult[40].

Secondly, compared to more conventional computer systems, the typical scenario in CPS might be trickier. Numerous physical variables, including as temperature, velocity, and location, are now connected with the conventional network packets and computational operations[41].

Thirdly, cyberattacks on CPS can have an impact on both the physical process and the computer system[42].

Lastly, the physical process's intricacy and the necessity for real-time prediction necessitate the employment of basic machine learning models[43].

In this paper, we take a close look at the latest and greatest studies that have successfully integrated machine learning with cybersecurity. Specifically, we focus on studies that have shown promising results in protecting cyber physical systems (CPS) on a large scale. To ensure that our review is thorough and up-to-date, we have excluded studies that do not pertain to

computer science and require unfettered data access, such as those involving Common Off-The-Shelf (COTS) firmware or the creation of non-generalized trust boundaries. The broad applicability of our results and insights to many cyber physical systems is crucial, as it will aid in the development of CPS security. There are several kinds of anomalies in CPS, as shown in Figure (2).

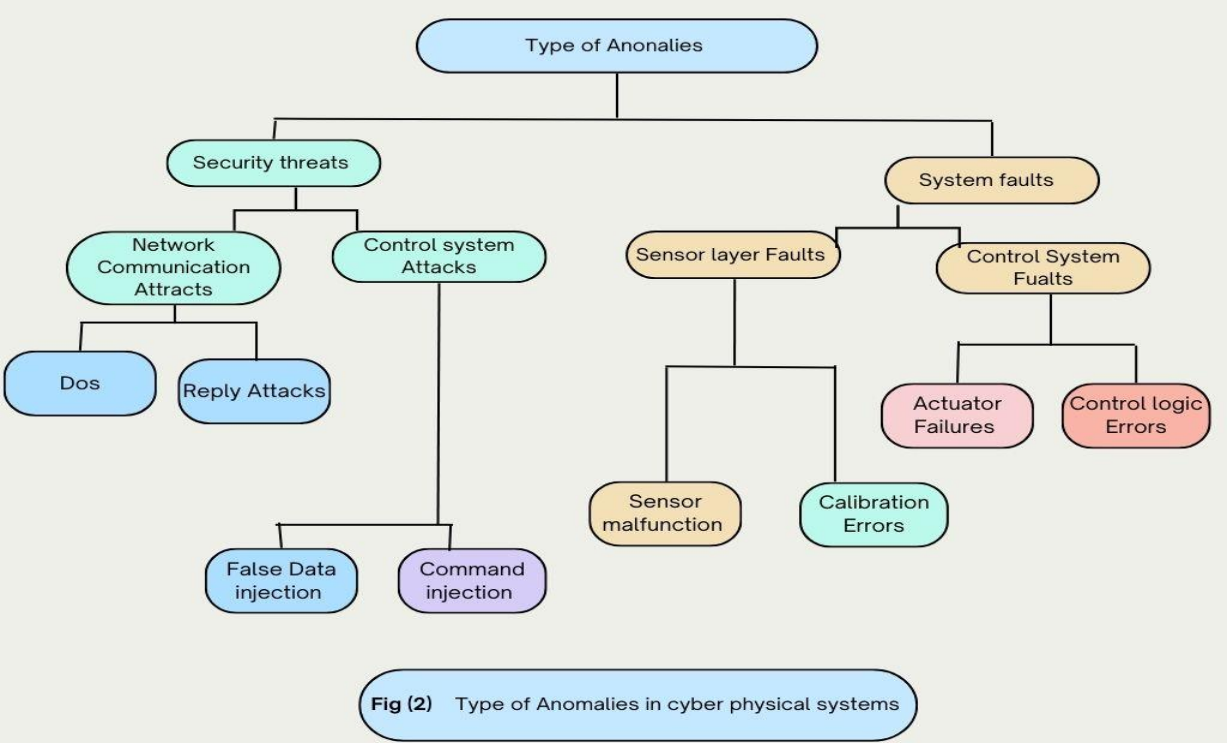

Fig (2) Type of Anomalies in cyber physical systems

3.1. Traditional Methods vs. Machine Learning Approaches

3.1.1 Traditional Methods

Traditional methods have mainly focused on detecting attacks and defending systems against them. A common methodology used in many security mechanisms is digital signatures. Intrusion detection systems, such as a network intrusion detection system or intrusion protection system, can monitor all incoming or outgoing traffic, find any known attack signals, and generate an alert to reduce system damage [50][51]. Digital signatures have provided an efficient filtering and detection methodology because they cover many characteristics of network communication and are easy to compare and interpret [52][53]. However, a security problem occurs when the network system cannot receive any existing signatures, or the large increase in signatures is still inefficient and can miss many newly implemented attacks [54]. Moreover, most traditional security solutions are based on theories of heuristic triggers, rules, or digital signatures, and so the security product has a high false-positive rate of application invocation [55].

3.1.2. Machine Learning Techniques

Anomaly detection has advanced to a new level with the advent of fast technology development and an explosion in training data volume, thanks to machine learning (ML) and, in particular, deep learning (DL). Processing high-dimensional sensor data requires the capacity to abstract complicated structures, which is another factor contributing to the heightened interest [44]. Unsupervised learning, in which training models does not need any labeled normal or abnormal data, is a typical feature of ML-based AD. After all of the training is complete, the model ought to be able to distinguish between typical and out-of-the-ordinary samples. Assuming the AD model is effective, this feature has the potential to automate model training with minimal human intervention[45].

The data set is divided into K predetermined clusters using K-means based methods, such as K-means and Fuzzy C-Means. Many ML strategies for AD are based on clustering algorithms. A

data set's manifold is learned using an auto-encoder based technique during the model training phase [46]. Despite its successful unsupervised training, the AD algorithm still requires a lot of human intervention. Some semi-supervised learning methods have been tested for AD to alleviate the annotation load. These models include sequence-to-sequence auto-encoders, convolutional neural network (CNN)-based encoders and decoders, and long-short term memory (LSTM) based recurrent neural networks [47]. It is not necessary to pre-train the deep neural networks for the unsupervised AD. The purpose of supervised AD is to learn to distinguish between normal and abnormal data, as opposed to the unavailability of labels in unsupervised AD. An intermediate step is semi-supervised AD, in which the labelled data set contains just a subset of the total[48]. In order to create a multi-resolution spatio-temporal correlation, it is recommended to use hybrid ML-based approaches that combine symbolic query and model-based learning, as well as LSTM with convolutional networks. This will allow for a more accurate modeling of the relationship among a number of sensors for sequential data[49]. Random neural network (RNN) networks encode input with a latent distribution as its output. Researchers have also looked at a new way to employ the variational autoencoder (VAE) where the input data is assumed to have a Gaussian distribution and the latent variables' conditional probability distribution[50]. An irregularity may have been detected if the distribution characteristics changed suddenly. A plethora of alternative approaches have been put forth, including graph-based unsupervised anomaly detection and semi-supervised classification using neural networks, deep unsupervised learning for unsupervised anomaly detection using directed compounds, feature importance guided data association, and a combination of support vector machines and directed compounds.

4. LITERATURE REVIEW

One of the most common methods for detecting CPSoS anomalies is the Intrusion Detection System (IDS)[51]. Electronic commerce and telecommunications are only two of the many systems that make extensive use of it. A comprehensive review of IDS was conducted by Granville and Oliveira (2005)[52], [53]. Each server runs its own application and host intrusion detection systems (HIDS). Data collection is dependent on their regular execution of the whole set of system (or application) actions. Listening to all kernel calls triggered allows one to compile this list of system or application uses [54]. The only difference between the HIDS and the External IDS (HIDS) is that the latter listens to kernel calls made via the network. When something out of the ordinary happens, such as a sensor failing to transmit an alert, a message indicating an attack, or unauthorised access resulting in a change to the user list, the HIDS/external IDS will activate[55], [56]. A radio telescope technique is used by BaseStation, a system for monitoring wireless networks, to listen to the whole band by receiving packets from the entire network. We send each addressed packet to the MIPS accelerator for observation, and then we compare the side-channel observations to the assumptions based on the models. While the remaining packets are reshuffled to go on to the next simulation stage, those packages identified as outliers are punished and sent to the central server[57].

The requirement for static knowledge rather than learning is the primary issue with the IDS[58]. In contrast to intrusion detection systems (IDS), which change their signatures in response to specific events, IPS systems require frequent file downloads and updates. The next step is to deploy the signature on the servers or routers, which might interfere with the CPSoS functionality [59]. The utilization of an anomaly can also be traced by the activity of the IDS. A CPSoS adaption model update, however, will occur in real time when the model is being executed, regardless of whether an anomaly exists[60]. In addition, the information gathered by the IDS is technology-specific, and the CPSoS components may use vastly different technologies [61].

Amiri et al (2023). An extensive amount of information on the concepts and applications of machine learning (ML) techniques in healthcare is provided by this study. it addresses a broad variety of common health issues. It carefully considers potential outcomes, including in all the

essential steps that must be organized for the future [62] . Several clear challenges exist, however, when using ML to personal healthcare. Importantly, supervised learning algorithms are trained using diagnostic labels. However, because mental disorders are so varied, these classifications may not be accurate enough to train AI systems to be very sensitive and particular. Instead of making diagnosis, ML algorithms might be used to predict certain symptoms or outcomes. More than that, DNN may be used autonomously to find new biomarkers for identifying certain illnesses. Despite the need of transparency and repeatability, protecting proprietary information is a major roadblock to ML algorithm implementations. Big data requires a lot of prep work before it can be used, and it's also essentially unstructured. Furthermore, it is not usual practice to include details about the data's quality and any biases in the results of ML algorithms.

Malika et al. (2023). Using deep reinforcement learning as its foundation, this work introduces Anomaly-NIDS. This approach to data gathering and preparation might prove useful in a variety of network topologies. This method of reinforcement learning gives you a bunch of choices. The model's capacity to accurately identify incoming network traffic is enhanced in the Learning mode by continuous learning and updating, while processing speed is optimized in the detection mode. The author successfully tested the method on 100 million Palo Alto network logs as part of the campus networking environment. In order to evaluate the suggested DRL, three machine-learning techniques were employed. Proven in experiments, the suggested approach efficiently updates models in real time while simultaneously achieving maximum detection accuracy and processing speed [63]. However, pre-processing data is lacking[64] .

Mahdi et al. (2024). The suggested method tracks and updates the estimation of each packet using sequential packet labeling in order to get the attack probability score for each flow. The CICIDS2017 and CSE-CIC-IDS2018 datasets are used to assess the framework using CNN-based and LSTM-based deep models. By doing comprehensive experiments and assessments, the researcher proves that the proposed distributed system successfully handles traffic concept drift. Our results show that convolutional neural network (CNN) models can adjust to traffic idea drift, and with just 128 more frames, they achieve identification rates above 95%. On the other hand, online intrusion detection systems that use LSTM-based models to classify packets sequentially are exceptional at identifying intrusions within 15 packets [65].

Singh et al. (2024). Sophisticated Intrusion Prevention System A new method for intrusion detection called AID-DRL has just been created, and it uses Deep Reinforcement Learning. The proposed system uses deep neural networks and reinforcement learning to build an adaptive intrusion detection system (IDS) that can safeguard against evolving cyber threats. Consideration of scalability, adaptability, and interaction with cybersecurity infrastructure was given during the design and construction of AID-DRL. The experimental results show that the AID-DRL system detected and mitigated threats better in real-time than baseline models. Learning algorithms should be made more adversary resilient, dynamic policy modification should be a priority of future research, as should the integration of threat intelligence, scalability, deployment, and privacy preservation. These domains aim to address the dynamic nature of cybersecurity while also enhancing intrusion detection systems [66].

Jeffrey et al. (2024). supply a method for CPS anomaly detection based on "unsupervised learning models" that employ one-class classification algorithms. Because the normally utilized studies have an incredibly small quantity of aberrant data, this will assist in making up for it. Although it helps with some of the accuracy challenges resulting from data classes that are not balanced, this strategy is not highly portable to CPS settings and concentrates on the distinctions between supervised and unsupervised learning using a narrow range of classification methods [67].

Afrifa et al. (2023). start with the idea that criminals frequently take over huge numbers of “IoT devices”, transforming them into botnets to carry out their nefarious schemes, posing a threat to global trade. A single compromised Internet of Things (IoT) device probably wouldn't cause

much trouble on its own, but a botnet of hundreds—or perhaps millions—could cause havoc. By identifying individual nodes inside a botnet, we offer a novel way to detect botnets and prevent incursions in real-time using Ensemble Learning. This innovative approach uses Ensemble Learning to identify botnet hosts, as opposed to the conventional approach of deciding whether an action against a particular host is harmful or benign [68].

Yazdinejad et al. (2023). provide an ensemble deep learning-based anomaly detection approach for IIoT settings; this model uses AE architecture and LTSM to review time series data in order to spot unusual action. In IIoT/CPS anomaly detection scenarios, imbalanced datasets are common and affect the prediction power of several ML algorithms. This study applies pattern recognition to time series data collected from "IIoT environment" monitoring in order to determine if the activity is normal or abnormal. The premise is that IIoT environments are dispersed and filled with diverse sensors and actuators. The goal is to tackle the issue as a big data challenge [69].

Nicholas et al(2024). For CPS anomaly detection, this study suggests a hybrid technique that combines “signature-based detection” for IT networks, “threshold-based detection “for OT networks, and behavioral-based Ensemble Learning (EL) for improved accuracy.

Several publicly available research datasets are used to validate the hybrid technique. Minimizing a measure of behavioural-based data for "ML model" training, it employs a "divide-and-conquer strategy" to outsource cyber threat detection to methods that rely on signatures and thresholds yet are computationally cheap. This leads to improved accuracy in less time. The experiment findings demonstrated an improvement in anomaly detection accuracy of 4-7% across many datasets. This is of utmost importance for CPS operators due to the significant financial implications and safety costs associated with system outages [70].

Vincent et al (2024). The effectiveness, security, and cost-effectiveness of hyperphysical systems have been enhanced by the integration of communication and information technology with large-scale power grids.

Despite its broad and open communication environment, the smart grid is susceptible to cyber-attacks.

A major threat to grid operations comes from data integrity attacks that circumvent conventional security measures. The existing smart grid detection algorithms aren't flexible enough to deal with non-Euclidean data sources or characteristics that are constantly changing and diverse. To detect data integrity breaches in cyber-physical systems, the author introduces a novel Deep-Q-Network method based on a graph convolutional network (GCN) architecture. When compared to earlier benchmark approaches, the simulation results show that the framework is more accurate and scalable [71].

JIMSHA K et. al (2024). This study provides a comprehensive methodology for intrusion detection in WSNs and addresses the vulnerabilities that are inherent to WSNs. A hybrid of regularization and PSO feature extraction with CNN-Bi-LSTM classification is proposed as a feasible solution. The system starts with meticulous data preparation, which involves normalizing the raw data acquired from the WSN. It is critical to standardize feature scales in order to guarantee data consistency and enhance interpretability. Then, pertinent features are identified and feature selection is optimized using the PSO algorithm. Reduced duplication and improved feature set discrimination are two ways in which PSO improves intrusion detection. With these features in hand, the CNN-Bi-LSTM model integrates the spatial feature extraction of CNN with the temporal modeling of Bi-LSTM.

Bi-LSTM is better at finding temporal correlations in sequential sensor data than CNN is at focusing on spatial representations. This cooperation allows the framework to detect intricate infiltration patterns with high accuracy. Using tagged datasets for performance evaluation, the integrated system beats prior intrusion detection methods. In order to improve the security of

these critical networks, the results of the tests show that the framework may enhance intrusion detection in WSNs [72].

Afrah et al (2024). In response to this, the authors have created an intrusion detection system (IDS) model that uses a combination of convolutional neural network (CNN) and long short-term memory (LSTM) DL methods.

By combining the pattern recognition capabilities of convolutional neural networks (CNNs) with those of long short-term memories (LSTMs), this fusion makes it easier and more accurate to detect and categorize benign and malicious IoT data. After training the model using the recently released CICIoT2023 dataset, the authors ran final tests to see how well it performed, and finally, they utilized the CICIDS2017 dataset to confirm that their model had worked.

A low loss of 0.0275 and an accuracy rate of 98.42% were achieved by the authors using the suggested model. Another crucially important factor is the false positive rate (FPR), which is 9.17% when the F1-score is 98.57%. Cyber threat mitigation in IoT systems is facilitated by the proposed CNN-LSTM IDS paradigm [73].

Roya et al. (2024). This paper presents a state-of-the-art solution for an Internet of Things (IoT) intrusion detection network using deep learning techniques and clean data. The author trains and tests their intrusion detection models using the open-source CICIDS2017 dataset, which contains information on botnet activity, port scans, and distributed denial of service attacks. The goal is to provide a method that is more effective than previous ones. The suggested deep learning model captures spatial and temporal data interactions using LSTM architecture and thick transition layers. When assessing the efficacy of the model, the writers relied on stringent measures including accuracy and sparse categorical cross-entropy loss. On test data, this method achieved an accuracy of 0.997, demonstrating its excellent yield. You can trust this model's intrusion detection capabilities since its loss and accuracy scores are consistent. You can see how effective this strategy is by comparing it to other machine learning techniques. Additionally, test how well the model holds up under challenging conditions by seeing how well it handles Gaussian noise. Additionally, it provides performance metrics for several attack types, demonstrating the model's utility in different threat situations[74].

Ju Hyeon et al. (2023). This research introduces a method for detecting cyber threats in solar plants' central system, the Programmable Logic Controller (PLC) of the inverter, using network packets. The cyber hazards were discovered during an investigation of cyberattacks and vulnerabilities in solar power facilities. To disrupt solar plant operations, inverters are the most common target of denial-of-service and malicious code injection assaults, according to the research. Before training machine learning-based classification models, the authors developed an anomaly detection method by preprocessing PLC network packet data using correlation analysis and normalization. An accuracy of 97.36% was achieved using the Random Forest model, which was the most effective. Solar plant security might be enhanced, anomalies in network packets could be detected, and cyber threats could be identified using the proposed technique [75].

M.Tuaama (2024). In a smart healthcare context, this work proposes a deep learning architecture (DLA) for managing anomaly detection. The DLA constructs the intelligent control procedure with the aid of perceptive, algorithmic self-learning that may automate and signal. Preprocessing and the incorporation of IoT gadgets from smart medical start the acquisition of huge volumes of data. To ensure the safety, security, and reliability of control methods and management service decisions, the next stage is to coordinate intelligence frameworks with DLA. To determine if a system state is normal or pathological, deep architectures build a mathematical model using training methods. These models build a composite analytic link by integrating data patterns with system variables; this connection aids in detecting both typical and unusual system behaviour[76].

Despite the excellent detection accuracies attained thus far, there is still room for improvement, according to our literature analysis. Accuracy levels and the amount of data manipulation are two

examples of these issues. There has been very little development in the area thus far. We have described the selected IDSs and compared their basic attributes in a table (1). The majority of the researchers concentrated on intrusion prevention, while some touched on intrusion detection in various ways. but just a small fraction made use of deep learning for intrusion detection. Thus, we are of the opinion that the methods and research presented in this paper may produce reliable outcomes while simultaneously cutting costs and saving time through the optimization of detection accuracy and the reduction of false alarms.

Table 1

NO	Author&year	Method	Datset	Objectives	Advantage	drawbacks
	Malik et al.(2023)	ANID	Palo Alto System Network Logs	Process data more quickly.	Processing at a superior speed	Limited to specific regions of the network
	Roger et al.(2023)	RL-Based ID	8TB Real Network Traffic Data	Reduced quantity of computing resources	Accuracy and High Reliability	utilized a single dataset, which makes it challenging to transfer to another dataset
	Afrifa et al.(2023)	ML techniques	public dataset	recognize and avert botnet assaults on interconnected personal computers, particularly those involving internet of things devices.	For the purpose of detecting botnet attacks, the method employs real-time behavioral analysis driven by AI. For prompt prevention, this might be vital.	The use of an ensemble approach including multiple ML models may increase the complexity of the implementation, calling for more computational resources and expertise.
	Ju Hyeon et al. (2023)	ML	PLC Network Packet Data	The goal is to develop a method for detecting anomalies in solar plant PLC data that can protect inverters from cyber assaults.	The Random Forest model's ability to detect cyber threats was shown by its remarkable 97.36% accuracy rate.	The model's ability to detect some types of attacks is contingent upon the variety and quality of the data retrieved from the network packets, but it can still capture some of them.
	Amiri et al 2023	ML(CNN,RNN,DNN,MLP)	Micromed	virtual environment	Extreme precision Extensive reliability	Inadequate evaluation of the approaches
	Sang et al. 2024	DRL	Simulation with Real scenatio	A Realistic Improvement in CPS Models	effectiveness enhancement	Given their reliance on similarity, they may fail to adequately portray the intricacy of real cyberthreats.
	Soltani et al.(2024)	multi-Agent NIDS	CICID2017&CSE-CIC-IDS2018	The objective is to enable a distributed IDS architecture that improves detection accuracy and tackles big data challenges by utilizing observations from several sensors.	Its distributed detection function allows it to scale for networks with high throughput.	The use of multi-agent systems allows for a more complex implementation.

	Singh et al.(2024)	DRL	NSL-KDD	The system penalizes false positives in an effort to improve accuracy.	The system has the potential to adjust to upcoming dangers.	It could be more difficult to execute the technique.
	jeffrey et al.(2024)	Hybrid ID	Edge-IIoTest2023 & CICIoT2023	the cyber physical system's identification accuracy optimization	Precision improvement	Limited possibilities for knowledge sharing
	Vincent et al.(2024)	DQN & GCN		identify and thwart any dangers to the integrity of smart grid data,	The detection accuracy is exceptionally high.	It could be more difficult to execute the technique.
	JIMSHA K et. al (2024)	PSO & CNN-Bi-LSTM	Enumerated Datasets	Using regularization, PSO, CNN, and Bi-LSTM, we can improve the efficiency and accuracy of WSN intrusion detection.	When it comes time to feature selection, PSO increases detection performance by removing irrelevant features and concentrating on the main ones.	Using many sophisticated algorithms (CNN, Bi-LSTM, PSO) increases the model's complexity, which may increase the time and resources needed for training.
	Afrah et al (2024)	cnn & LSTM	CICIoT2023 & CICIDS2017	Developing a hybrid intrusion detection system The model that effectively and accurately uses CNN and LSTM to detect fake IoT traffic..	Identifies incursions with an accuracy of 98.42%.	Since the performance is assessed on specific datasets, its applicability to different IoT scenarios or datasets can be restricted.
	Roya et al. (2024)	LSTM	CICIDS2017	Develop a cutting-edge IoT intrusion detection solution that surpasses state-of-the-art methods by leveraging deep learning	The model's remarkable ability to detect intrusions was on full display when it obtained an astounding 0.997 accuracy on test data.	It may be difficult to generalize results from studies conducted on the CICIDS2017 dataset to other datasets or real-world Internet of Things environments.
	M.Tuaama (2024)	DNN	SDN-IoT	The importance of using deep neural networks (DNN) to detect network attacks, classify anomalies, and enhance the protection of IoT devices in healthcare environments.	**Enhanced Diagnostics**: IoT enables the collection of a wide range of health-related metrics, providing a comprehensive view of patient health.	**Complexity in Model Selection**: The success of deep learning models relies heavily on selecting the right architecture, making it challenging to ensure consistent reliability across different scenarios.

To evaluate the proposed strategy in relation to comparable approaches found in the literature, Table 1 summarizes the main points. These features are linked to three things: (1) the security

implementation method; (2) the dataset used with this algorithm; and (3) the model's advantages and shortcomings.

5. METHODOLOGY

Here, we provide a DNN-based architecture for cyber-physical systems network vulnerability and threat detection. We begin by discussing the framework's main workflow and then examine the evaluation of each step and its important contributions.

5.1. The suggested framework's workflow

It consists of five primary steps: Extracting useful data via preprocessing, maintaining class equilibrium through augmented data, and discovering optimal characteristics through feature selection. Step one is to prepare the features for encoding and dataset segmentation. Step two is to train and evaluate the DNN model. Figure 1 shows the proposed system's procedure flow. Each of these procedures will have its operational basics explained in great depth.

Preprocessing Data: We begin by collecting raw network data with the networking analysis tool. After that, we extract attributes from the packets. After discarding unnecessary packets from the dataset, we gather samples of classes inside it.

Using the encoding method, we converted the symbolic data to integers, and then we used min-max standardization to ensure that all of the numerical values in the dataset were consistent.

- **Symbolic Encoding:**

Features that fall within the category of: $X_{encoded} = encode(X_{categorical})$……(1)

- **Normalization using Min-Max:**

With regard to continuous features**:** $X^{!} = \frac{X - X_{min}}{X_{max} - X_{min}}$ ……..(2)

Data Augmentation: Imbalanced data occurs when the sample sizes of each class are not evenly distributed, resulting in data skewness that biases the model towards a class with a more significant amounts of samples.

Resampling the training data before classification helps to reduce class imbalance. Oversampling requires increasing the number of samples from minority classes, whereas undersampling involves decreasing the number of samples from majority classes.

Researchers are using the oversampling approach; nevertheless, it leads to the problem of overfitting owing to the redundancy of the data obtained from oversampling [22]. The Synthetic Minority Oversampling Technique (SMOTE) generates new samples by picking instances from the minority class, but it also produces noise and class overlap.

Recent advancements in generative adversarial networks (GANs) utilize neural networks to produce synthetic data that closely resembles original datasets [23].

Because GANs permit model adjustment, which aids in developing an accurate model, and because they avoid overfitting, and class overlap, as well as noise problems, they are superior to other traditional approaches like SMOTE [24].

To ensure that the dataset is balanced, we extract fresh samples from it. With GANs, we are able to raise the packet count for the minority attack classes. The dataset becomes more balanced when the synthetic data is generated. Goodfellow et al. [26] introduced GANs, which are comprised of a pair of neural networks that collaborate to produce synthetic data and identify both real and synthetic data. Generative networks take an input dataset and use it to create artificial data; The produced data is separated from the real data in the input set using a discriminator network.

- **Handling Class Imbalance:**

Data oversampling using SMOTE or GAN: $X_{augmented} = GAN(X_{minority})$

Where GAN generates synthetic samples of the minority class.

To a balanced dataset:

$|X_{class1}| \approx |X_{class2}|$

- **Feature Selection:** selecting features decreases computational costs and increases storage efficiency [77]. The following methods are used for feature selection:
- A filter method is one that uses the correlation scores of characteristics to determine how related they are. We choose features according to the scores and threshold value of statistical methods, which are used for feature selection. Methods like the Chi-Square test, information gain, and correlation are the most popular.
- **Wrapper Methods:** A machine learning (ML) model is trained on an subset of features using wrapper methods. The subset's characteristics are either added to or removed from depending on the model's accuracy. Two of the most prevalent examples of this kind of approach are forward selection and backward elimination.
- **Embedded Methods:** Combining the best features extraction with computational cost preservation, this strategy is an improvement over both the filter and wrapper approaches. Two of the most prevalent variants of this approach are Random Forest [78] and LASSO regularization [79].
- Dataset partitioning:

$$X_{train}, X_{val}, X_{test} = splt(X, train\_size, val\_size, test\_size$$

Where the data is partitioned into sets for testing, validation, and training.

We conduct our studies using the Filter Method since it is significantly quicker and uses less compute than the other two approaches.

- **Feature preprocessing:** Following feature extraction, feature reduction, and feature encoding, we partitioned the data we had processed into three sets: training, validation, and testing. Each set included the labels for normal and attack-type classes.
- **Training &Testing Dataset:** The DNN model is taught to use the training set's processed data during the training phase. After training, the model is put to the test using the testing set data, which it uses to distinguish between normal and attack kinds.

6. RESULT ANALYSIS

To achieve better accuracy, we construct multiple DNN designs using varied dense hidden layers and neuronal densities in each layer. The DNN model, which uses three dense hidden layers—each with 64 neurons—to get the greatest results. The amount of neurons and thick hidden layers determines the model's complexity. When the value is tiny, it indicates that the model is underfitting; conversely, when the value is big, it indicates that the model is overfitting. Through the use of Adam optimiser, we experimented with various learning rates and discovered that the default value of 0.001 yields superior accuracy.

Using metrics, we evaluate the suggested DNN Algorithm with different attacks in the dataset. This includes the F1 score, precision, accuracy, and recall. Furthermore, provides categorization confusion matrices. The model's performance is assessed using evaluation metrics when two classes, C1 and C2, are provided.

Model of DNN Algorithm for Training.

The model parameters are updated using gradient descent. For each epoch, weights W are updated:

$$W_{t+1} = W_t - \eta . \nabla L(W_t)$$

Where η is the learning rate and L(W) is the loss function (e.g., cross-entropy loss):

$$L = -\frac{1}{N} \sum_{i=1}^{N} [y_i \log(\hat{y_i}) + (1 - y_i) \log(1 - \hat{y_i})]$$

Efficiency learning and performance assessment both seek to estimate a model's accuracy on future data and metrics, so that researchers may analyse the efficacy of the suggested approach and compare it to other models. This will help them decide which methodology is most suited for this activity. As a result of its predictive capabilities, the confusion matrix sheds insight on categorisation problems. The classifier's accuracy (Equation 1), sensitivity (also known as a true positive rate [TPR] or recall) (Equation 2), false-positive rate (FPR) (Equation 3), precision (Equation 4), specificity (Equation 5), F1-score (Equation 6) and the types of errors (TP, FP, FN, and TN) are all provided. The ROC curve illustrates the classifier's accuracy and the connection between the true positive and false positive rates in various threshold circumstances.

Evaluation Metrics:

$$Accuracy = (TP + TN)/(TP + TN + FP + FN) \quad \text{.....(1)}$$

$$Sensitivity = TP/(TP + FN) \quad \text{.....(2)}$$

$$\boldsymbol{FPR} = FP/(TN + FP) \quad \text{.....(3)}$$

$$Precision = TP/(TN + FP) \quad \text{.....(4)}$$

$$Specificity = TN/(TN + FP) \quad \text{.....(5)}$$

$$F1 - Score = 2 * TP/(2 * TP + FP + FN) \quad \text{.....(6)}$$

To identify malicious actions, several academics have created sophisticated ML-based models that compete with one another.

Table 2. Different ML classifiers' accuracy

Classical classification methods	Accuracy
RF	98.01
SVM	97.39
SGD	97.65
Logistic Regression	97.01
Linear Discriminant Analysis	97.94
Gaussian NB	89.14
our Proposal	98.37

Table 2 lists the accuracy of the classic ML approach; it is evident that DNN models outperform it when it comes to detecting invasive behaviours.

This article presents a variety of Network-CPS suggested models that investigate literature on threat detection. Along with other models like decision trees, naïve Bayesian, and random forests, Ham et. al[80] presented the linear SVM algorithm for use on a synthetic data set. This model would perform multiclassification and be evaluated using metrics like TPR, FPR, precision, accuracy, and F-measure. As demonstrated in Table 3, SVM has achieved an accuracy of 99.7 percent and an F1-score of 95.4 percent, whereas our suggested model has an accuracy of 98.37 percent and an F1-score of 98.0 percent. Due to the synthetic nature of the data, the F1-

score, which includes both false-negative and false-positive cases, will be given greater weight than accuracy.

Table 3. A comparison of the proposed model's accuracy to that of other models

Author	Dataset	Model Accuracy		our proposal
13	Synthetic	SVM	99.7	98.37
		Bayes net	94.3	
		RF	91.5	
		Naïve Bayes	70.4	

7. CONCLUSION AND FUTURE WORK

Studies on privacy and network security have been conducted in recent years regarding cyberphysical systems (CPS). Several proposals for IDS designs based on ML and DL have been made. The Internet of Things (IoT) makes extensive use of deep learning for intrusion detection.

We addressed the imbalance of the problem class in the dataset. We demonstrated the effectiveness of our proposed framework in CPS networks by increasing the delivery of DNN-based packets belonging to minority assault classes, feature selection, and GANs. With GANs, the classifier achieves 98% accuracy in multi-class classification, whereas with traditional methods, it reports an accuracy of 97% in predictions. The findings have important implications for cyber-security. Selected features and an increase in the amount of DoS attack packets allow for accurately classifying attacks as either regular or malicious. Nevertheless, we ran into a number of problems. To create traffic for the dataset's minority assaults, the suggested model may be used with GANs, and The method may be used with different datasets that have unequal classification labels. The feature selection method has cut down on the model's feature count, which in turn has lowered the model's cost.

To decrease the feature count prior to classification, one might apply a variety of feature extraction and selection methods. This study focused on five distinct kinds of traffic while doing multi-class categorization. It is possible to develop a new DNN-based classifier with improved accuracy and reduced loss in FN terms and FP predictions, and future dataset updates should include more minority attack categories. Another potential future goal of this research is to develop a DNN-based intrusion detection model for Cyber-Physical Systems networks that can operate in real-time.

BIBLIOGRAPHY

1. M. K. Hasan, A. K. M. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, “Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations,” *Journal of network and computer applications*, vol. 209, p. 103540, 2023.
2. N. S. Madasamy, K. J. Eldho, T. Senthilnathan, and J. Deny, “A Novel Back-Propagation Neural Network for Intelligent Cyber-Physical Systems for Wireless Communications,” *IETE J Res*, vol. 70, no. 2, pp. 1361–1373, 2024.
3. Y. Jiang, S. Wu, R. Ma, M. Liu, H. Luo, and O. Kaynak, “Monitoring and defense of industrial cyber-physical systems under typical attacks: From a systems and control perspective,” *IEEE Transactions on Industrial Cyber-Physical Systems*, 2023.
4. L. Rybalchenko, A. Kosychenko, and I. Klinytskyi, “Ensuring economic security of enterprises taking into account the peculiarities of information security,” 2022.
5. M. Sajid *et al.*, “Enhancing intrusion detection: a hybrid machine and deep learning approach,” *Journal of Cloud Computing*, vol. 13, no. 1, p. 123, 2024.

6. V.-H. Le and H. Zhang, “Log-based anomaly detection with deep learning: How far are we?,” in *Proceedings of the 44th international conference on software engineering*, 2022, pp. 1356–1367.
7. M. Hamzah *et al.*, “Distributed Control of Cyber Physical System on Various Domains: A Critical Review,” *Systems*, vol. 11, no. 4, p. 208, 2023.
8. G. Y. Dayankl, S. Sinha, D. Muniraj, R. M. Gerdes, M. Farhood, and M. Mina, “{Physical-Layer} attacks against pulse width {Modulation-Controlled} actuators,” in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 953–970.
9. Y. Wu, H.-N. Dai, H. Wang, Z. Xiong, and S. Guo, “A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1175–1211, 2022.
10. A. Pundir, S. Singh, M. Kumar, A. Bafila, and G. J. Saxena, “Cyber-physical systems enabled transport networks in smart cities: Challenges and enabling technologies of the new mobility era,” *IEEE Access*, vol. 10, pp. 16350–16364, 2022.
11. A. Yaseen, “The role of machine learning in network anomaly detection for cybersecurity,” *Sage Science Review of Applied Machine Learning*, vol. 6, no. 8, pp. 16–34, 2023.
12. S. Kim, K.-J. Park, and C. Lu, “A survey on network security for cyber–physical systems: From threats to resilient design,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1534–1573, 2022.
13. F. J. Egloff and M. Smeets, “Publicly attributing cyber attacks: a framework,” *Journal of Strategic Studies*, vol. 46, no. 3, pp. 502–533, 2023.
14. W. Duo, M. Zhou, and A. Abusorrah, “A survey of cyber attacks on cyber physical systems: Recent advances and challenges,” *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 5, pp. 784–800, 2022.
15. M. K. Habib, C. Chimsom, and others, “CPS: Role, characteristics, architectures and future potentials,” *Procedia Comput Sci*, vol. 200, pp. 1347–1358, 2022.
16. S. F. Ahmed *et al.*, “Deep learning modelling techniques: current progress, applications, advantages, and challenges,” *Artif Intell Rev*, vol. 56, no. 11, pp. 13521–13617, 2023.
17. A. Goyal and Y. Bengio, “Inductive biases for deep learning of higher-level cognition,” *Proceedings of the Royal Society A*, vol. 478, no. 2266, p. 20210068, 2022.
18. A. E. Cil, K. Yildiz, and A. Buldu, “Detection of DDoS attacks with feed forward based deep neural network model,” *Expert Syst Appl*, vol. 169, p. 114520, 2021.
19. M. Adil, R. Ullah, S. Noor, and N. Gohar, “Effect of number of neurons and layers in an artificial neural network for generalized concrete mix design,” *Neural Comput Appl*, vol. 34, no. 11, pp. 8355–8363, 2022.
20. H. M. D. Kabir *et al.*, “Spinalnet: Deep neural network with gradual input,” *IEEE Transactions on Artificial Intelligence*, vol. 4, no. 5, pp. 1165–1177, 2022.
21. M. M. Taye, “Theoretical understanding of convolutional neural network: Concepts, architectures, applications, future directions,” *Computation*, vol. 11, no. 3, p. 52, 2023.
22. M. Makarkin and D. Bratashov, “State-of-the-art approaches for image deconvolution problems, including modern deep learning architectures,” *Micromachines (Basel)*, vol. 12, no. 12, p. 1558, 2021.

23. A. P. Kaur, A. Singh, R. Sachdeva, and V. Kukreja, “Automatic speech recognition systems: A survey of discriminative techniques,” *Multimed Tools Appl*, vol. 82, no. 9, pp. 13307–13339, 2023.

24. G. Menghani, “Efficient deep learning: A survey on making deep learning models smaller, faster, and better,” *ACM Comput Surv*, vol. 55, no. 12, pp. 1–37, 2023.

25. S. S. Gill *et al.*, “Ai for next generation computing: Emerging trends and future directions. Internet Things 19: 100514,” 2022.

26. T. Sun, S. Ding, and L. Guo, “Low-degree term first in ResNet, its variants and the whole neural network family,” *Neural Networks*, vol. 148, pp. 155–165, 2022.

27. Y. Liu, P. Sun, N. Wergeles, and Y. Shang, “A survey and performance evaluation of deep learning methods for small object detection,” *Expert Syst Appl*, vol. 172, p. 114602, 2021.

28. Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Yao, “Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities,” *ACM Computing Surveys (CSUR)*, vol. 54, no. 5, pp. 1–36, 2021.

29. M. Shahin, F. F. Chen, H. Bouzary, and A. Hosseinzadeh, “Deploying convolutional neural network to reduce waste in production system,” *Manuf Lett*, vol. 35, pp. 1187–1195, 2023.

30. V. Chaudhary, “Securing Future Generation Virtual Wireless Networks for Cyber Physical Systems,” Howard University, 2023.

31. R. Novickis, D. J. Justs, K. Ozols, and M. Greitāns, “An approach of feed-forward neural network throughput-optimized implementation in FPGA,” *Electronics (Basel)*, vol. 9, no. 12, p. 2193, 2020.

32. P. Singh, S. K. Borgohain, A. K. Sarkar, J. Kumar, and L. D. Sharma, “Feed-Forward Deep Neural Network (FFDNN)-Based Deep Features for Static Malware Detection,” *International Journal of Intelligent Systems*, vol. 2023, no. 1, p. 9544481, 2023.

33. P. Suawa, T. Meisel, M. Jongmanns, M. Huebner, and M. Reichenbach, “Modeling and fault detection of brushless direct current motor by deep learning sensor data fusion,” *Sensors*, vol. 22, no. 9, p. 3516, 2022.

34. J. Raitoharju, “Convolutional neural networks,” in *Deep learning for robot perception and cognition*, Elsevier, 2022, pp. 35–69.

35. J. P. Bharadiya, “Exploring the use of recurrent neural networks for time series forecasting,” *Int J Innov Sci Res Technol*, vol. 8, no. 5, pp. 2023–2027, 2023.

36. M. N. Al-Mhiqani, T. Alsboui, T. Al-Shehari, K. hameed Abdulkareem, R. Ahmad, and M. A. Mohammed, “Insider threat detection in cyber-physical systems: a systematic literature review,” *Computers and Electrical Engineering*, vol. 119, p. 109489, 2024.

37. X. Yang, E. Howley, and M. Schukat, “ADT: Time series anomaly detection for cyber-physical systems via deep reinforcement learning,” *Comput Secur*, vol. 141, p. 103825, 2024.

38. A. Pundir, S. Singh, M. Kumar, A. Bafila, and G. J. Saxena, “Cyber-physical systems enabled transport networks in smart cities: Challenges and enabling technologies of the new mobility era,” *IEEE Access*, vol. 10, pp. 16350–16364, 2022.

39. S. M. Nagarajan, G. G. Deverajan, A. K. Bashir, R. P. Mahapatra, and M. S. Al-Numay, “IADF-CPS: Intelligent anomaly detection framework towards cyber physical systems,” *Comput Commun*, vol. 188, pp. 81–89, 2022.

40. N. Jeffrey, Q. Tan, and J. R. Villar, “A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems,” *Electronics (Basel)*, vol. 12, no. 15, p. 3283, 2023.

41. M. K. Habib, C. Chimsom, and others, “CPS: Role, characteristics, architectures and future potentials,” *Procedia Comput Sci*, vol. 200, pp. 1347–1358, 2022.

42. W. Duo, M. Zhou, and A. Abusorrah, “A survey of cyber attacks on cyber physical systems: Recent advances and challenges,” *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 5, pp. 784–800, 2022.

43. C. Lv *et al.*, “Machine learning: an advanced platform for materials development and state prediction in lithium-ion batteries,” *Advanced Materials*, vol. 34, no. 25, p. 2101474, 2022.

44. M. Bahri, F. Salutari, A. Putina, and M. Sozio, “AutoML: state of the art with a focus on anomaly detection, challenges, and research directions,” *Int J Data Sci Anal*, vol. 14, no. 2, pp. 113–126, 2022.

45. S. Zehra *et al.*, “Machine learning-based anomaly detection in NFV: A comprehensive survey,” *Sensors*, vol. 23, no. 11, p. 5340, 2023.

46. Z. Huang, H. Zheng, C. Li, and C. Che, “Application of machine learning-based k-means clustering for financial fraud detection,” *Academic Journal of Science and Technology*, vol. 10, no. 1, pp. 33–39, 2024.

47. P. S. Muhuri, P. Chatterjee, X. Yuan, K. Roy, and A. Esterline, “Using a long short-term memory recurrent neural network (LSTM-RNN) to classify network attacks,” *Information*, vol. 11, no. 5, p. 243, 2020.

48. L. Heckler, R. König, and P. Bergmann, “Exploring the importance of pretrained feature extractors for unsupervised anomaly detection and localization,” in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2023, pp. 2917–2926.

49. S. C. K. Tekouabou, E. B. Diop, R. Azmi, R. Jaligot, and J. Chenal, “Reviewing the application of machine learning methods to model urban form indicators in planning decision support systems: Potential, issues and challenges,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 5943–5967, 2022.

50. N. Nguyen and B. Quanz, “Temporal latent auto-encoder: A method for probabilistic multivariate time series forecasting,” in *Proceedings of the AAAI conference on artificial intelligence*, 2021, pp. 9117–9125.

51. M. N. Al-Mhiqani, T. Alsboui, T. Al-Shehari, K. hameed Abdulkareem, R. Ahmad, and M. A. Mohammed, “Insider threat detection in cyber-physical systems: a systematic literature review,” *Computers and Electrical Engineering*, vol. 119, p. 109489, 2024.

52. P. Shukla, C. R. Krishna, and N. V. Patil, “Iot traffic-based DDoS attacks detection mechanisms: A comprehensive review,” *J Supercomput*, vol. 80, no. 7, pp. 9986–10043, 2024.

53. S. Nicolazzo, A. Nocera, and W. Pedrycz, “Service Level Agreements and Security SLA: A Comprehensive Survey,” *arXiv preprint arXiv:2405.00009*, 2024.

54. R. Mitev, A. Pazii, M. Miettinen, W. Enck, and A.-R. Sadeghi, “Leakypick: Iot audio spy detector,” in *Proceedings of the 36th Annual Computer Security Applications Conference*, 2020, pp. 694–705.

55. J. M. Kizza, “System intrusion detection and prevention,” in *Guide to computer network security*, Springer, 2024, pp. 295–323.

56. Y. Shen, “Machine Learning and Knowledge-Based Integrated Intrusion Detection Schemes,” Université d’Ottawa/University of Ottawa, 2022.

57. S. Chakraborty, G. Hellbourg, M. Careem, D. Saha, and A. Dutta, “Collaboration with Cellular Networks for RFI Cancellation at Radio Telescope,” *IEEE Trans Cogn Commun Netw*, vol. 9, no. 3, pp. 765–778, 2023.

58. A. Thakkar and R. Lohiya, “A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions,” *Artif Intell Rev*, vol. 55, no. 1, pp. 453–563, 2022.

59. T. Sommestad, H. Holm, and D. Steinvall, “Variables influencing the effectiveness of signature-based network intrusion detection systems,” *Information security journal: a global perspective*, vol. 31, no. 6, pp. 711–728, 2022.

60. R. Pinto, G. Gonçalves, J. Delsing, and E. Tovar, “Enabling data-driven anomaly detection by design in cyber-physical production systems,” *Cybersecurity*, vol. 5, no. 1, p. 9, 2022.

61. S. N. M. Garc\’\ia, A. Sánchez-Cabrera, E. Schiavone, and A. Skarmeta, “Integrating the manufacturer usage description standard in the modelling of cyber–physical systems,” *Comput Stand Interfaces*, vol. 87, p. 103777, 2024.

62. Z. Amiri *et al.*, “The personal health applications of machine learning techniques in the internet of behaviors,” *Sustainability*, vol. 15, no. 16, p. 12406, 2023.

63. M. Malik and K. S. Saini, “Network Intrusion Detection System using Reinforcement learning,” in *2023 4th International Conference for Emerging Technology (INCET)*, 2023, pp. 1–4.

64. M. Sarhan, S. Layeghy, M. Gallagher, and M. Portmann, “From Zero-Shot Machine Learning to Zero-Day Attack Detection. arXiv 2021,” *arXiv preprint arXiv:2109.14868*.

65. M. Soltani, K. Khajavi, M. Jafari Siavoshani, and A. H. Jahangir, “A multi-agent adaptive deep learning framework for online intrusion detection,” *Cybersecurity*, vol. 7, no. 1, p. 9, 2024.

66. D. N. Singh, S. Jaiswar, P. Jha, V. K. Tiwari, and P. K. Saket, “Adaptive Intrusion Detection Using Deep Reinforcement Learning: A Novel Approach,” *International Journal of all Research Educvation & Scientific Methods*, vol. 12, no. 05.

67. N. Jeffrey, Q. Tan, and J. R. Villar, “A hybrid methodology for anomaly detection in Cyber–Physical Systems,” *Neurocomputing*, vol. 568, p. 127068, 2024.

68. S. Afrifa, V. Varadarajan, P. Appiahene, T. Zhang, and E. A. Domfeh, “Ensemble machine learning techniques for accurate and efficient detection of botnet attacks in connected computers,” *Eng*, vol. 4, no. 1, pp. 650–664, 2023.

69. A. Yazdinejad, M. Kazemi, R. M. Parizi, A. Dehghantanha, and H. Karimipour, “An ensemble deep learning model for cyber threat hunting in industrial internet of things,” *Digital Communications and Networks*, vol. 9, no. 1, pp. 101–110, 2023.

70. N. Jeffrey, Q. Tan, and J. R. Villar, “Using Ensemble Learning for Anomaly Detection in Cyber–Physical Systems,” *Electronics (Basel)*, vol. 13, no. 7, p. 1391, 2024.

71. E. Vincent, M. Korki, M. Seyedmahmoudian, A. Stojcevski, and S. Mekhilef, “Reinforcement learning-empowered graph convolutional network framework for data integrity attack detection in cyber-physical systems,” *CSEE Journal of Power and Energy Systems*, 2024.

72. S. ARUMUGASAMY, “AN INTRUSION DETECTION APPROACH IN WIRELESS SENSOR NETWORK SECURITY THROUGH CNN-BI-LSTM MODEL,” *J Theor Appl Inf Technol*, vol. 102, no. 2, 2024.

73. A. Gueriani, H. Kheddar, and A. C. Mazari, “Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems,” in *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, 2024, pp. 1–7.

74. R. Morshedi, S. M. Matinkhah, and M. T. Sadeghi, “Intrusion Detection for IoT Network Security with Deep learning,” *Journal of AI and Data Mining*, vol. 12, no. 1, pp. 37–55, 2024.

75. J. H. Lee, J. Shin, and J. T. Seo, “Solar Power Plant Network Packet-Based Anomaly Detection System for Cybersecurity,” *Computers, Materials & Continua*, vol. 77, no. 1, 2023.

76. M. M. Tuaama, “Anomaly Detection-Based Intrusion Detection System Using Deep Neural Networks in Healthcare Internet of Things,” *Innovative: International Multidisciplinary Journal of Applied Technology (2995-486X)*, vol. 2, no. 7, pp. 40–56, 2024.

77. B. Sharma, L. Sharma, and C. Lal, “Feature selection and deep learning technique for intrusion detection system in IoT,” in *Proceedings of International Conference on Computational Intelligence: ICCI 2020*, 2022, pp. 253–261.

78. A. K. Al Hwaitat *et al.*, “Improved security particle swarm optimization (PSO) algorithm to detect radio jamming attacks in mobile networks,” *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 4, 2020.

79. M. N. Khan *et al.*, “Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks,” *Ieee Access*, vol. 8, pp. 176495–176520, 2020.

80. H.-S. Ham, H.-H. Kim, M.-S. Kim, and M.-J. Choi, “Linear SVM-based android malware detection for reliable IoT services,” *J Appl Math*, vol. 2014, no. 1, p. 594501, 2014.