ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 10, No. 3, June 2022, pp.261-275

Using machine learning algorithm for detection of cyber-attacks in cyber physical systems

Rasha Almajed[1], Amer Ibrahim[2], Abedallah Zaid Abualkishik[3], Nahia Mourad[4], Faris A Almansour[5]
[1,2, 3,4,5] College of Computer Information Technology; American University in Emirates, Dubai, UAE

ABSTRACT

Network integration is common in cyber-physical systems (CPS) to allow for remote access, surveillance, and analysis. They have been exposed to cyberattacks because of their integration with an insecure network. In the event of a violation in internet security, an attacker was able to interfere with the system's functions, which might result in catastrophic consequences. As a result, detecting breaches into mission-critical CPS is a top priority. Detecting assaults on CPSs, which are increasingly being targeted by cyber criminals and cyber threats, is becoming increasingly difficult. It is potential that (AI) Artificial Intelligence as well as (ML) Machine Learning will make this the worst of times, but it also has the potential to be the best of times. There are a variety of ways in which AI technology can aid in the growth and profitability of a variety of industries. Such data can be parsed using ML and AI approaches in designed to check attacks on CPSs. We present the new framework for the detection of cyberattacks, which makes use of AI and ML. We begin a process to cleaning up the data in the CPS database by applying normalization to eliminate errors and duplication. The features are obtained by using a technique known as Linear Discriminant Analysis (LDA). We have suggested the SFL-HMM together with HMS-ACO process as a method used for detection of the cyber-attacks. A MATLAB simulation used to evaluate the new strategy, and the metrics obtained from that simulation are compared to those obtained from the older methods. According to the findings of several studies, the framework is significantly more effective than conventional methods in maintaining high levels of privacy. In addition, the framework outperforms conventional detection algorithms in words of detection rate, the rate of the false positive, and calculation time, respectively.

Keywords: Cyber-physical systems (CPS), cyberattacks, Artificial Intelligence (AI), Machine Learning (ML), Linear Discriminant Analysis (LDA), Self-tuned Fuzzy Logic based Hidden Markov Model (SFL-HMM), Heuristic Multi-Swarm Optimization (HMS-ACO)

Corresponding Author:

Rasha Almajed
College of Computer Information Technology
American University in Emirates
Dubai, UAE
E-mail: Rasha.almajed@aue.ae

1. Introduction

As a result of the internet's inception, numerous innovations and technologies that seem to have a profound impact on human life, interpersonal interactions, and the environment were born. Interaction, teamwork, and access to data were made easier by the capacity to connect computers around the world electronically [1]. Complex, sophisticated, intelligent, and self-aware CPSs have emerged in the last several years. These include smart grids in the power industry, industry 4.0 in the manufacturing sector, transportation systems, hospital and medical fields, and robots. [2] It is tough to anticipate the activity of CPSs because of the complex interplay between various cyber and physical aspects, as well as the fact that they are vulnerable to significant disturbances owing to both unintentional and deliberate occurrences. In the meantime, since the frequency of cyber-attacks has risen and their activity has become much more advanced, popularly known as zero-day vulnerabilities, investigators in industry and university are noticing to cyber defense for CPS. [6] CPS's. Fig 1. illustrates the entire building.

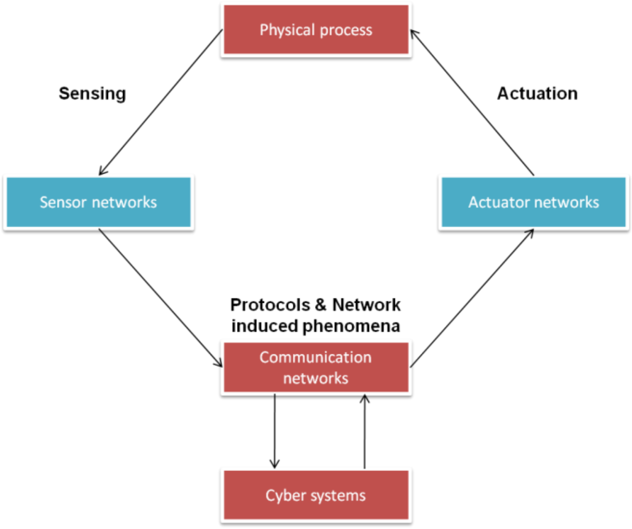

Figure 1. illustrates the entire building of the CPS

In view of CPSs, a variety of psychosocial purposes were carried out. There are a wide range of applications in transport systems, grids, medicine, and water/gas distributors, among others. Another group that falls under the umbrella of CPS is networked control mechanisms, wireless sensing networks, including wireless industrialized sensor systems. Using the Internet, CPS can operate as expert machines that manage operations that had previously been largely reliant on human endeavor. According to various writers, they are referred to as physical and engineering systems where a central computer or communication core is responsible for coordinating, controlling, and integrating every one of the processes.

Standard cyber security measures such as intrusion detection and prevention systems (IDS/IPS) and access control cannot detect, prevent, or block zero-day attacks since the characteristics of these attacks are not kept in the databases of the security systems. CPSs are protected against zero-day attacks thanks to cyber security solutions based on artificial intelligence [5]. Cyber security uses ML technology [3] to manage a significant amount of heterogeneous data from different sources in order to fast build separate attack patents and properly anticipate the future misconduct of hackers. This allows for a more accurate prediction of the hackers' future behavior.

Along with security experts' involvement, the prevention of zero-day assaults necessitates cooperation between different AI and ML technologies [4]. The goal of human-machine engagement seems to be to limit the frequency of wrongful convictions, so human decision-making really improves detection mechanism.

Communication and control signals are exchanged between CPS components using ad hoc networks or possibly the Internet. As a result, the system is vulnerable to assaults that originate from the network domain. Attacks on CPS have the potential to be devastating. This attack isn't limited to cyberspace; it can also take place in the real world. All components of the CPS are vulnerable to attack.

Cyber-attacks on CPS can result in structural malfunctions and interfere with the normal operation of physical processes, which is why conventional machine learning approaches are used to discover them. When networks are complicated there is just not enough information about the object under investigation, definitive assessment of cyber-attacks against CPS becomes a difficulty. There are strategies and solutions in artificial intelligence that greatly enhance neural networks' capabilities and efficacy. With so many layers, the neural network may start with simple characteristics and work its way up to more complicated ones.

Despite numerous effective implementations for the detection of cyber-attack-related equipment problems, methodologies based on extensive training have shown that the same design may not always be reliable. The technique's constraints are influenced by the diversity of the physical process. Our goal is to find a way around this restriction and create the SFL-HMM method. High detection efficiency of cyber-attacks and negative relation of mistakes between models would be ensured by this method.

2. Related work

A technology called Deep Fed, which is a unique distributed machine learning method, was presented in [8]. Its purpose is to detect cyber risks to commercial CPSs. They create a ground-breaking deep researching analytical model for commercial CPSs by combining a gated recurrent unit with a deep neural network. Deep convolutional neural networks, often known as CNNs, are brought into play in [9] in order to build a model for a system that can identify distributed denial-of-service, or DDoS, attacks that are associated with a botmaster who supervises problematic systems. In [10], new DL techniques for detecting cyber risks in a CPS setting are introduced. For the purpose of utilizing DL strategies in order to discover cyber breaches on CPS systems, a methodology that is driven by DL and consists of six steps has been presented for examining and evaluating the researched literature.

The objective of the study [11] was to assist researchers and practitioners in the process of developing and deploying surveillance systems that incorporate enormous amounts of data derived from system logs, network traffic, and other organization sources. This was accomplished by providing assistance to researchers and practitioners in the process of developing and deploying such systems. In [12], which is an example from the reference, an explanation of how to recognize unexpected input from sensors in cyber-physical systems was provided using a water distribution system as an illustration. This strategy makes use of both machine learning and the modeling of technological systems to accomplish its goals. [13] The plan for the study includes conducting an inquiry into any instances of fraud. Because it was constructed on mobile robots, a cyber physical system was able to make the identification of cyber vulnerabilities such as overflow attacks. These vulnerabilities include: (DoS, DDoS, RDoS).

[14] suggests that the creation of a low-coupling system that is centered on edge computing could be a solution to the problems that are linked with coupling. The edge software platform, which also serves the function of a middleware platform, is the one that is responsible for providing the feature of scheduling. The authors of [15] outline a variety of distinct machine learning algorithms that can be used for identifying IoT dangers in cyber-physical space systems. These approaches can be applied in a variety of different ways. A substantial amount of data is necessary in order to implement machine learning for the purpose of ensuring the cyber security of the internet of things (IoT), despite the fact that this data is uncommon. In [16], the reader will find a discussion of various techniques for Deep Learning-based Anomaly Detection (DLAD) in Computer Protected Systems.

They propose a taxonomy of anomaly kinds, methodologies, implementation, and assessment measures so that they can gain a better understanding of the essential components that make up existing methods. This will allow them to gain a better understanding of the essential components that make up existing methods. The acronym FID-GAN, which stands for "fog-based, unsupervised intrusion detection system with Generative Adversarial Network," was given to this innovative unsupervised method of detecting cyber-attacks in CPSs by the researchers that came up with it. This approach was utilized all throughout the course of this investigation [20]. A combination of discrimination and reconstruction losses is required in order for the mapping of samples to the latent space to be carried out properly. This is because discrimination losses are used to eliminate redundant information. Because of this, it is deployed most successfully in situations in which there is only a constrained amount of time available for a reaction. As a result of this, it can be utilized to its fullest potential in situations. In this study [21], techniques using machine learning and deep learning are examined with regard to critical path scheduling and safety analysis. We now have a better grasp of CPS and the implications that it has for security as a result of the work that has been done.

The current level of internet and telecommunications penetration has fostered technology innovations like as the Internet of Things and the Connected Personal System in [22]. In the context of cybersecurity, artificial intelligence and machine learning have been extensively investigated, along with the possible risks and benefits. A study was carried out in [23] in order to acquire the most recent information possible regarding the manner in which CPSs recognize cyber assaults. The most recent twenty papers are compiled and evaluated as part of this research project, which is structured according to a DL-driven process that consists of six steps. It is anticipated that more progress will be made with regard to this topic. [24] provides a structure for healthcare systems that can be used to secure and safeguard the information of patients.

This paper addresses concerns about the safety of cyber-physical systems, as well as research barriers in ensuring the integration of cyber-physical systems. In the paper [25], a novel structure was offered for identifying and differentiating DoS and fidelity cyber assaults in CPSs using 1-dimensional CNNs. This new structure is superior to the methods that are currently in use. When it comes to examining systems that are able to identify circumstances of this nature, this research is rather unique. Utilizing a federated learning-based strategy, as described in [26], is one way to cut down on the amount of data that is lost from VCPS, which stands for "Vehicular Cyber-Physical System." We have developed a fresh method of updating random sub-gossip in order to protect the pupils' privacy while they are working on their schoolwork. An explanation of the conceptual underpinnings of AI-CPS can be found in [27].

In accordance with the tenets of this methodology, you will need to construct a number of classifiers and train each one separately. This research investigates a wide variety of network system attacks and threats, as well as the most common solutions that may be used to mitigate these issues. More investigation is required in order to determine the total amount of damage that has been incurred as a result of these hits. Using ML techniques, anomalies and attacks can be identified in their early stages, allowing for the implementation of countermeasures. In [28], the authors advise using a parallel relaxation-based technique in order to reliably and quickly identify cyberattacks. For the purpose of doing additional research into the anomaly, relevant data obtained from the outcomes of this procedure could be sent to other devices. After that, more investigation into this particular anomaly can be carried out. They describe a Generic-Specialized autoencoder design in [29]. In this design, the generic autoencoder trains just domain-specific characteristics, while the specialized autoencoder gets universal features. It is important to avoid incorrect classification at all costs.

To determine whether or not the strategy is successful, it is necessary to apply it to multiple datasets. There have already been presentations in [30] of brief abstracts of the most recent breakthroughs in the detection of cyber-physical system attacks. According to the amount of information they have about the entire network, the controllers of the various CPSs can be categorized as centralized or dispersed controllers. The most widely analyzed procedures include LTI systems' classic attack detection tactics, sensor and actuator attack detection methods, nonlinear structures, and noise-prone structures. In the paper [31], the authors developed a two-stage ensemble deep learning-based assault detection and attribution approach for unbalanced ICS data. This method was based on deep learning. The changes included the addition of a cyber-threat hunting feature to assist in the finding of abnormalities that were not seen by the detection component. This might be done, for example, by constructing a typical profile of the entire network, which would include the resources.

They suggested a novel technique that is based on intelligent variable structure management [32] in order to estimate and adjust for assaults in the forward connection of nonlinear CPSs. This technique can be found here. Both non-linear control and artificial neural networks are put to use in the implementation of the method that has been suggested. Identifying Cyber Physical assaults in CMS uses physical data machine learning methods, as described in [33]. Investigation is required to determine the cyber-physical dangers posed by CMS configurations. They intend to continue researching 3D printing and CNC machining in an effort to find other production methods and identify fraudulent vulnerabilities in systems. Along with the creation of safety standards and goods, the development of a CMS security model is a component of this process.

[34] is working on developing methods for detecting cyber-physical risks on intelligent water distribution systems. In order to identify strange patterns in sensor readings, the method makes use of a number of different anomaly detection strategies. On the other hand, it has a propensity to place the system in what is known as a "false attack state" for a period of time after the actual risk has occurred. During the course of this research project for CPS, [35] conceived and built a malware detection technique for mobile-IoT applications. They employed semi-supervised learning in addition to deep learning strategies. Despite the fact that the framework that was proposed was successful, there is still opportunity for growth and development within it. The authors of [36] constructed a cyberattack within the AI industry using BBN as a framework in order to gain a better understanding of the vulnerabilities of CSC as well as the consequences of uncertainty.

In the paper [37], the authors presented a method that makes use of deep learning to design an effective and promising NIDS by combining ICs and ICS. NIDS, which is based on CNN, was selected. In the long run, network intrusion detection systems (NIDS) will be developed using deep learning. Based on the results of a power audit, a DL-based Internet of Things (IoT) safety solution is built in [38]. Both cyber and physical anomalous activity can be tracked through the utilization of an anomaly detection system that is predicated on forecasting mistakes. The suggested paradigm has the potential to improve both the monitoring and protection of IoT networks. According to [39], the authors conducted research on the application of GAN for anomaly identification in multivariate environments using data from the CPS. Their objective is to include MAD-GAN into an increased number of anomaly detection systems for usage in both smart buildings and machines. This research in [40] developed an IoT-CPS that was safe, and it did it by using AI to the process of diagnosing illnesses in patients. Due to the vast amounts of data that companies save, dishonest customers, such as scammers and hackers, as well as other dishonest consumers, are drawn to them. Anyone who has access to this information puts themselves at danger of having it utilized in a way that is detrimental to them. To put it another way, the protection of IoT-CPS approaches offered by AI is considered to be an estimate.

3. Problem statement

An individual, a group of individuals, or an organization could be the perpetrator of a cyberattack, and the attack could be a part of either interstate cyberwarfare or cyberterrorism. In the modern era, cyberattacks have been used by a variety of parties, including independent states, persons, companies, the public, communities, as well as gangs; furthermore, these attacks be able to make from anyone. Getting unauthorized access to a secure network makes it possible to steal, modify, or even destroy a particular target. There is a wide range of potential objectives that can be pursued in the course of a cyberattack, from the planting of malware on a personal computer to the attempt to cripple an entire nation's infrastructure. It is the intention of those who specialize in legal matters to limit the use of the term "hacking" to instances in which the physical structure of a building or an item of equipment sustains damage, and to distinguish this type of intrusion from more minor data breaches. Concerns about control are exacerbated by the fact that CPS is susceptible to a large number of cyber-attacks without giving any indication that the system is failing, which further compounds the problem. Attacks made against the physical system may result in the system becoming unstable. Repeated cyberattacks on CPS that show no sign of being successful pose a threat to the agency. If the dynamics of the program are not protected by hardware or software safeguards, the hacker has complete freedom to cause any form of disruption they choose. Controlling systems that have been compromised by cyberattacks presents a significant challenge, particularly in the context of power systems. Attacks, both digital and physical, could be launched against CPS. Direct disruption of dynamic response is caused by physical attacks, whereas disruption of cyber-physical connections is caused by cyber-attacks and undermines CPS. A physical attack can take many forms, such as an assault on the framework or the physical condition, or it can take the form of measures that have been tampered with.

3.1 The goal of the study

Cyber-Physical Systems, sometimes known as CPS for short, are systems that incorporate aspects from both the digital and physical realms in order to improve functionality. Cyber threats and attacks are occurring at an exponentially higher pace, and more reports of them are being made as a result. This is largely attributable to the growing use of cyber-physical systems (CPS) to deliver cutting-edge technology. The exponential proliferation of cyber-physical systems has given rise to new worries regarding their level of safety (CPS). For the subsequent generation of CPS, brand-new dangers, hazards, assaults, and countermeasures have been integrated. Despite this, there has not yet been a comprehensive investigation of the CPS security issues. It has been challenging to investigate this subject using a solitary generalized model due to the broad range of CPS components and the wide variety of CPS systems. Those two factors combined make it tough. Because CPS security has evolved into a problem on a worldwide scale, it is imperative that an appropriate framework be developed for CPS.

3.2 The scope of the study

The process of research has evolved to become an essential component of the independent study of cyber-physical systems. This has resulted in advances to surveillance and security that were made possible by the research's use of ML and AI approaches. Aspect-based training was utilized in the pattern of CPS in addition to sensors, electronics, control engineering, software engineering, and error management in order to differentiate between problems that cut across many domains. As a result of this research, we have proposed using the Heuristic Multi-Swarm Optimization (HMS) algorithm in conjunction with the Self-tuned Fuzzy Logical HMM (SFL-HMM) for the purpose of identifying cyberattacks.

4. Methodology

We start by pulling data from the CPS database, then we normalize the data to get rid of errors and entries that are duplicated. The features are obtained by using a technique known as (LDA). Together with (HMS-ACO) process are utilized to optimize the system (SFL-HMM). The effectiveness of the proposed technique is illustrated in Figure 2.

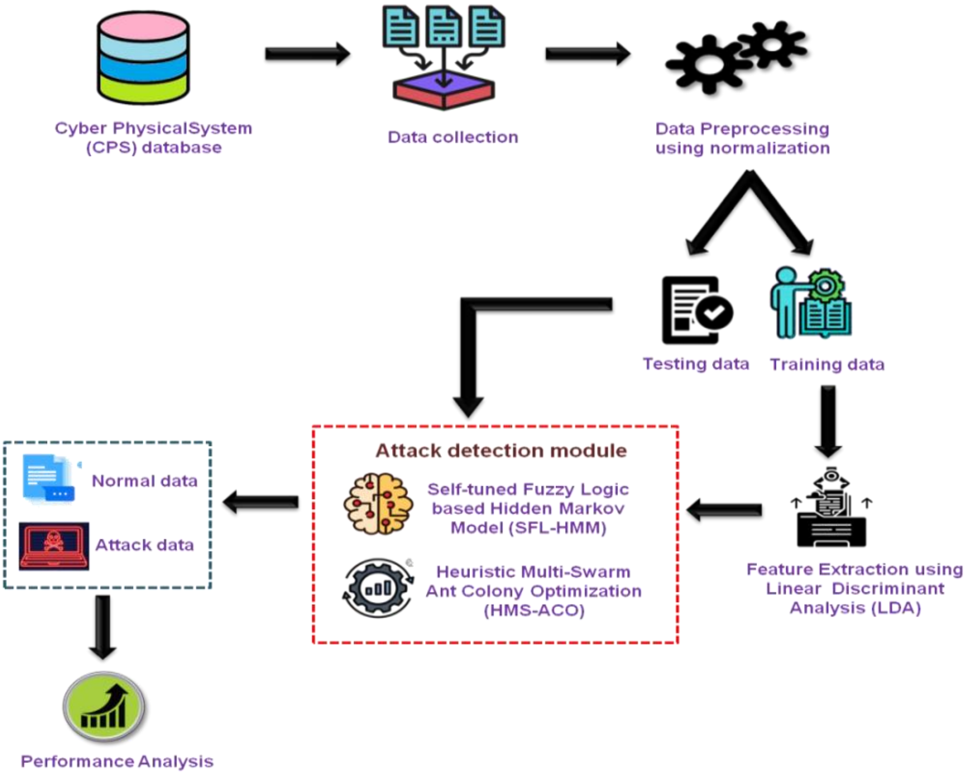
Cyber PhysicalSystem (CPS) database
Data collection
Data Preprocessing using normalization
Testing data
Training data
Feature Extraction using Linear Discriminant Analysis (LDA)
Attack detection module
Self-tuned Fuzzy Logic based Hidden Markov Model (SFL-HMM)
Heuristic Multi-Swarm Ant Colony Optimization (HMS-ACO)
Normal data
Attack data
Performance Analysis

Figure 2. The proposed methodology is depicted in the diagram

In the KDD99 dataset, there are a total of 41 features that collectively indicate 22 distinct kinds of attacks. It is not obvious whether the attacker was trying to completely break into the system or whether he or she was simply trying to log in for a limited amount of time [7]. The suggested dataset is laid out and discussed in Table 1.

Table 1. The Explanation of The Dataset

No.	The Name of a Features	The type of The Data	Symbols
1.	Duration	continuous	-
2.	protocol_type	symbolic	tcp, udp, icmp
3.	service	symbolic	http, smtp, domain_u
4.	flag	symbolic	SF, S0, REJ, etc.
5.	src_bytes	continuous	-
6.	dst_bytes	continuous	-
7.	land	symbolic	0, 1
8.	wrong_fragment	continuous	-
9.	urgent	continuous	-
10.	hot	continuous	-
11.	num_failed_logins	continuous	-
12.	logged_in	symbolic	0, 1
13.	num_compromised	continuous	-
14.	root_shell	continuous	-
15.	su_attempted	continuous	-
16.	num_root	continuous	-
17.	num_file_creations	continuous	-
18.	num_shells	continuous	-
19.	num_access_files	continuous	-
20.	num_outbound_cmds	continuous	-
21.	is_host_login	symbolic	0, 1

No.	The Name of a Features	The type of The Data	Symbols
22.	is_guest_login	symbolic	0, 1
23.	count	continuous	-
24.	srv_count	Continuous	-
25.	serror_rate	Continuous	-
26.	srv_serror_rate	Continuous	-
27.	rerror_rate	Continuous	-
28.	srv_rerror_rate	Continuous	-
29.	same_srv_rate	Continuous	-
30.	diff_srv_rate	Continuous	-
31.	srv_diff_host_rate	Continuous	-
32.	dst_host_count	Continuous	-
33.	dst_host_srv_count	Continuous	-
34.	dst_host_same_srv_rate	Continuous	-
35.	dst_host_diff_srv_rate	Continuous	-
36.	dst_host_same_src_port_rate	Continuous	-
37.	dst_host_srv_diff_host_rate	Continuous	-
38.	dst_host_serror_rate	Continuous	-
39.	dst_host_srv_serror_rate	Continuous	-
40.	dst_host_rerror_rate	Continuous	-
41.	dst_host_srv_rerror_rate	continuous	-

4.1 The processing of the data while it was being normalization

Transforming data into a predetermined range, such as from -1 to 1, is what this procedure entails. When the limits of multiple qualities are dramatically divergent, normalization is required. When there are no outliers in the data set, this scaling method is the best choice. This clearly demonstrates the theoretical foundations of normalization. Don't cast the data in the range of 0 to 1 if you don't have to do so.

$$\frac{valueAfterNomalization-0}{1-0}=\frac{valueBeforeNormalization-min}{max-min} \quad (1)$$

$$\frac{valueAfterNomalization}{1}=\frac{valueBeforeNormalization-min}{max-min} \quad (2)$$

$$valueAfterNomalization=\frac{valueBeforeNomalization-min}{max-min} \quad (3)$$

4.2 The extraction feature by using (LDA)

Suppose there are c pattern classes, $n_j$signifies the extent of data in the j^th class, and b = x j=1 indicates the number of samples in the j^th class $\sum_{j=1}^{s} x$. The samples were collected in total is bj, and the i th sample of the j^th class is m in the column vector. Finding a projection vector that decreases the distance between samples of the same class while simultaneously widening the range of samples within each class is the purpose of utilizing LDA. The projection vector needs to be found. The Fisher criteria are utilized by LDA in order to construct this projection vector. LDA employs the Fisher criteria described below.

$$m = arg\max_{m}\frac{m^{S}T_{n}m}{m^{S}T_{z}m} \quad (4)$$

Tn and Tz are the scatter matrices for within- and between-class comparisons, respectively. The formulas for computing Tn and Tz are as follows:

$$T_n = \frac{1}{b}\sum_{j=1}^{x} b_j\left(v_j - v\right)\left(v_j - v\right)^{S} \quad (5)$$

$$T_z = \frac{1}{b}\sum_{j=1}^{x}\sum_{i=1}^{b_j}\left(c_i^j - v_j\right)\left(c_i^j - v_j\right)^{S} \quad (6)$$

$$m = arg\max_{m^{S}m=1} m^{S}\left(T_z - \leftthreetimes T_n\right)m \quad (7)$$

where is a positive constant of a modest magnitude,

After working through Eq. 7, it becomes clear that a good prediction vector, m, is the eigen vector that has a lowest eigen value for the expression Tzm = Tnm. The vast majority of the time, a solitary projection vector is insufficient for distinguishing between several groups. Real-world applications frequently make use of a collection of projection vectors that fulfill the optimum requirements of the Fisher criterion in order to perform multi-class classification. M= arg min Sr(Ms (tz-tn)M). It is possible to construct the projection matrix M by using the first k lowest eigenvectors of the matrix TzM = tnM. To put it another way, the set of the k selected eigenvectors is denoted by the symbol M = [d1,...,dk] Rm*k, and the discriminative feature vectors for each sample are denoted by the symbols yji Rd and yji= MSCjibe.

4.3 The module of attack detection

1. SFL-HMM

Fuzzy Logic-based Hidden Markov Model (SFL-HMM) is a theoretical approach for model uncertainty that employs various logics to achieve its goal. This could also be used to perform a classification task. All classes do not have to be statistically represented. It is possible to represent suggestions in a broad range of true (one) to false (zero) frequencies using a fuzzy set-based Boolean logic method known as SFL-HMM.

The cyber-attack can have been described by 4 factors b1, b2, b3, as well as b4 as

$$\mu_{example(y)} = \begin{cases} 0, & y - b_1 \\ (y-b_1)/(b_2-b_1), & b_1 \leq y < b_2 \\ 1, & b_2 \leq y < b_3 \\ (b_4-y)/(b_4-b_3), & b_3 \leq y < b_4 \\ 0, & y \leq b_4. \end{cases} \tag{8}$$

The b1, b2, b3, as well as b4 cases basically represent four different threshold values for the variable that is being supplied. The connection between two random processes is depicted in Figure 3. One of the processes has a collection of states that cannot be seen or detected, whereas the other process has states that can be seen or detected. A is equal to A1, A2, and so on up to AN, where N represents the number of hidden states that may not be present immediately calculated. Some other dynamical system is denoted by a collection of M variable symbols denoted by S= S1,S2,...SM. Expectation maximization (EM) and maximum probability estimation (MPE), both of which have being common methods for calculating SFL-HMM variable quantity and, respectively, the highly possible hidden states, can have being utilized to conclude the hidden state sequence from the noticeable state classification. This is accomplished by comparing the two sequences and finding the difference between them. In addition, the SFL-HMM technique is illustrated in figure 4.

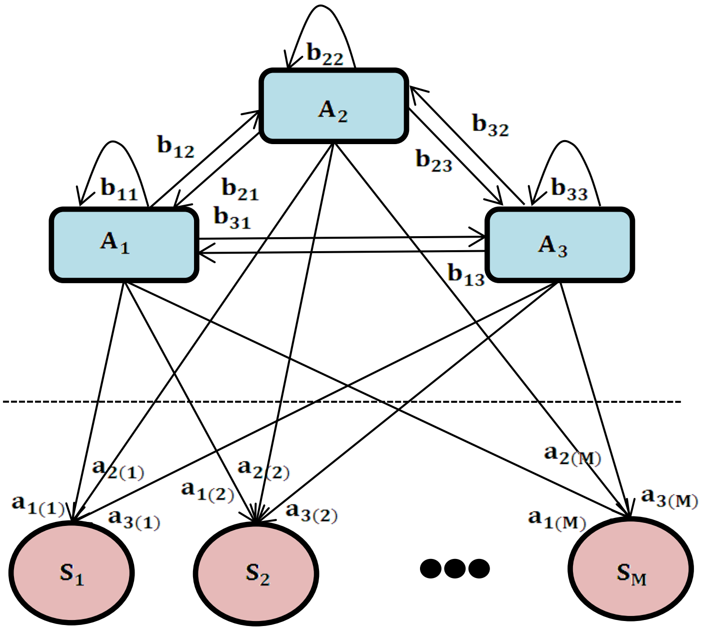

Figure 3. Map of the SFL-HMM

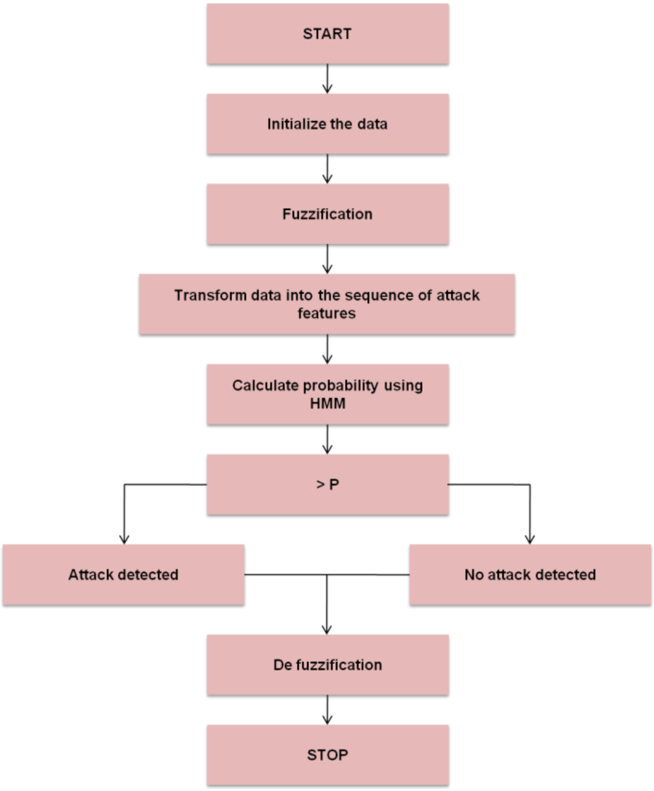

Figure 4. Process of the SFL-HMM

2. HMS-ACO

The HMS-ACO is utilized most frequently for the purpose of resolving challenges related to combinative optimization, where V connotes a set of nodes, then E denotes the collection of sides. Although the Zants circumnavigate the net nodes on their way to the collection of alternate, the amount of trail T 0 along each of the graph edges is the same. Equation 9 provides the early concept transition rule. After that, a sequence of processes is repeated over and over again until a stop condition is satisfied. This process includes a number of different steps, including the evaluation of new alternatives, the upgrading of trails, the evaluation of new solutions, and the remembering of the best answer.

$$\mathrm{n}M_{xy}^{l}(s)=\frac{\left[\tau_{xy}\right]^{\alpha}\left[\eta_{xy}\right]^{\beta}}{\sum_{k\in R_{j}^{l}}\left[\tau_{xy}\right]^{\alpha}\left[\eta_{xy}\right]^{\beta}}\,if i\in I_{l}(j) \qquad (9)$$

Whereas the heuristic swarm ant colony the optimization factor influences levels have been found to be specified via and, separately. A path that is found on surfaces i and j is referred to as Sij. is yl, the list of unvisited links maintained by Ant k. Different algorithms that are part of the ACO group make use of a variety of selection and updating strategies in order to choose the following node in the trail and improve it as they search for new solutions. In this work, we address the problem of Cloud Service Composition by utilizing HMS-ACO as our solution. The HMS-ACO is denoted by the first algorithm.

Algorithm 1: Heuristic MultiSwarm Ant colony Optimization

Input: *Graph, Parameters*

```
Output: $BDT_{best}$
$BDT_{best\ ts} \leftarrow CreateHeuristicsolution(Graph);$
$Pheromone \leftarrow InitializePheromone(Parameters.\tau_o);$
$BDT_{best} \leftarrow Cost(T_g);$
While (-Stop Condition)
For(x=1 To Parameters.W)
$Ti_{best} \leftarrow ConstructSolution(pheromone, Graph, Parameters);$
    $If\ (Ti_{best} \leq BDT_{best})$
                                        $BDT_{best} \leftarrow Ti_{best};$
End
```

```
Local Update and Decay Pheromone (Pheromone,$Ti_{best}$,Parameters);
    End
Global Update and Decay Pheromone (Pheromone $BDT_{best}$,Parameters);
End
Return ($BDT_{best}$)
```

5. The results and the discussion of the results

At this part of the article, we calculate the performing of the suggested system depended on the variety of the cyber-attacking factors, and we contrast the model with other methods that are already in use. Isolation forest [17], Kullback–Leibler distance [18], and Blockchain [19] are all components of the conventional model. In this research, we have suggested an approach for the detection of cyberattacks that is based on (SFL-HMM) combined with (HMS-ACO) process. Accuracy, the recognition threshold, RTP rate of true positive, and RFP rate of false positive are some of a parameter.

5.1 Histogram

Histograms are bar graphs that show a set of data along the x-axis, with each bar representing a possible outcome. The numerical score or ratio of instances in the statistics for every column is represented by the y-axis, which could be used to see how the data is distributed. Figure 5 depicts the histogram plot of this research.

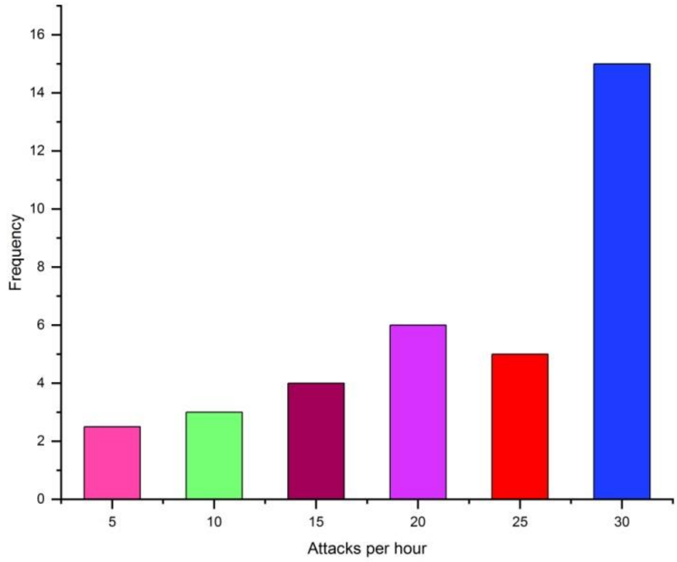

Figure 5. Histogram plot

5.2 The accuracy

The ability of a test to differentiate between normal data and malicious data is a major factor in determining how accurate it is. For the purpose of determining how reliable a test is, it is necessary to be aware of the proportion of instances in which the outcomes were definitively either positive or negative. It can be shows mathematically such as:

$Accuracy = TP + TN / TP + TN + FP + FN$(10)
“TP = True positive; TN= True negative; FP= False positive; FN= False negative”

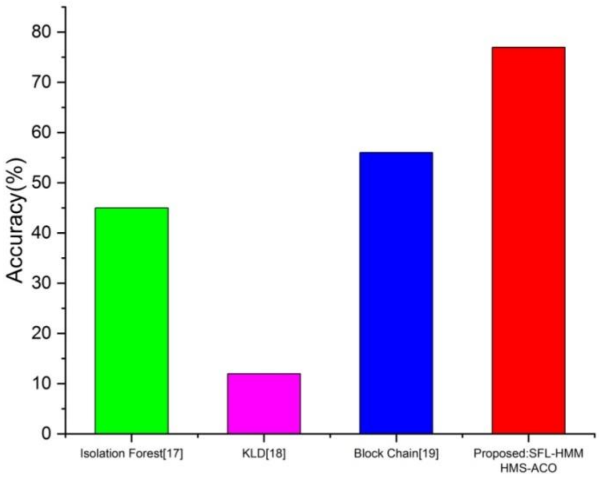

Figure 6. Existing and proposed techniques are compared in terms of accuracy

Fig. 6 presents a contrast between the suggested methods and those that are currently in use. It is clear to us that the approach that we have advocated for will be more successful in bringing us closer to accomplishing our objective.

5.3 The rate of the true positive

The Rate of the True Positive (RTP) is the ratio of true estimates in positive class values.
$RTP = TP/(TP + FN)$(11)
“RTP= rate of the true positive; TP= True positive; FN= False negative”

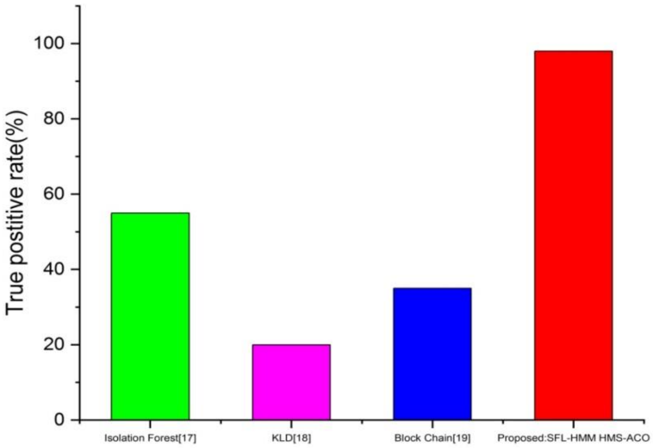

Figure 7. Existing and proposed techniques are compared in words of their rate of the true positive

The RTP of the currently used method and the proposed method are compared in Figure 7. The work that was suggested has a higher true positive rate than the work that already exists.

5.4 The rate of the false positive

When doing a classification task, the percentage of false positives in that task relative to the overall number of positive predictions is indicated to like the RFP in the CPS.

$$RFP = FP/(FP + TN) \quad (12)$$

“RFP=the rate of the false positive; FP= False positive; TN= True negative”

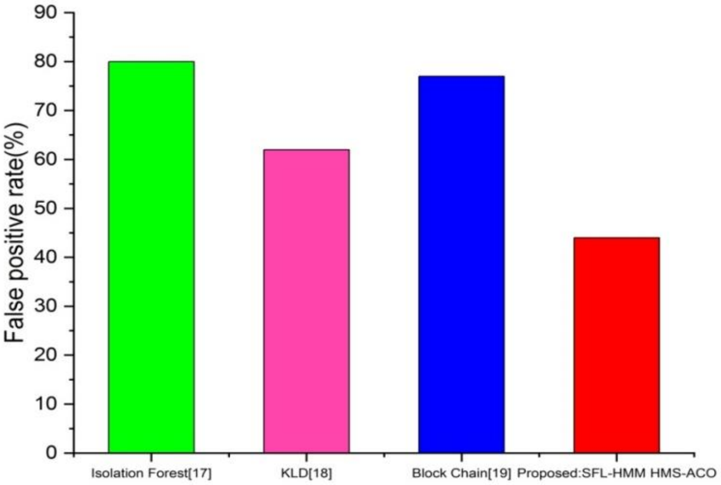

Figure 8. Compare between the existing rate of false combined with proposed method

Fig. 8 compares the false positive rate of existing and new methods. As can be seen in the graph, FPR plummets precipitously. Therefore, if the threshold is placed too small, the algorithm is going to be proactive in detection attacks, which will take the lead to a small RFP. There is no effect on the RFP from the size of the attack or the number of attacks.

5.5 The threshold of the detection

The detection threshold is a measure of the rate at which cyber-attacks are detected. For existing and proposed methods, a comparison of detection thresholds is shown in Figure 9.

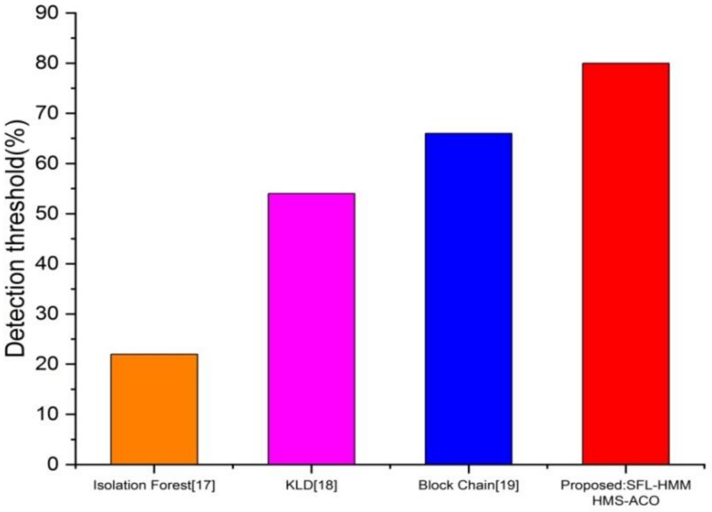

Figure 9. Comparison of current and proposed detection thresholds

The detection thresholds for a single assault (SA) as well as numerous attacks (MA) on state variables are investigated. The original name had to be changed after DT was implemented. As can be observed from the chart, RFP decreases significantly if the discovery threshold is increased to a higher level. If a threshold is placed too small, the algorithm is going to be overly attacker in its detection of the attacks, which will result in the higher discovery the threshold. This can be avoided by setting the threshold higher.

5.6 ROC

It is a graph of FPR versus detection rate for changing values of the predefined threshold, which is known as a ROC curve. Figure 10 depicts the ROC plot with presented and existing approaches.

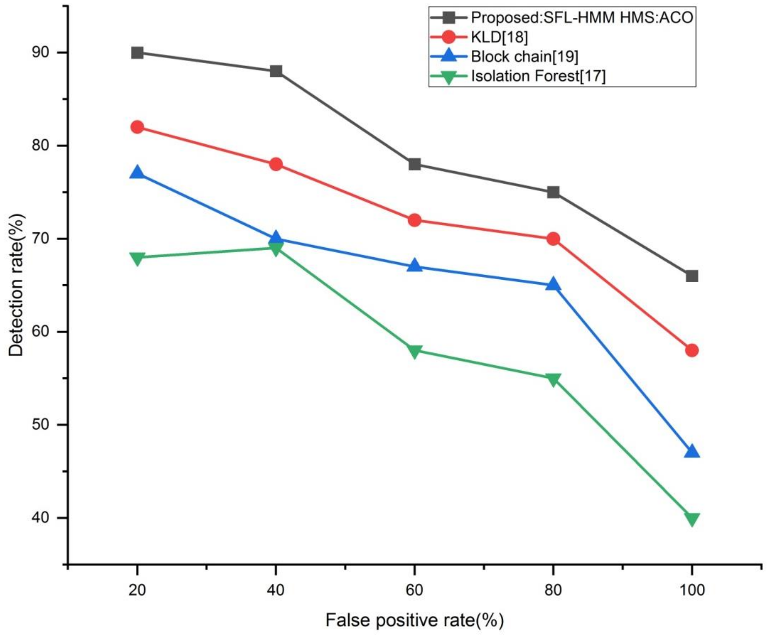

Figure 10. ROC plot

6. Discussion

The KDD99 attack datasets are being utilized in this investigation due to the fact that these datasets contain material that is either redundant or unnecessary. During the pre-processing step, a normalizing strategy should be utilized in order to achieve standardization or achieve balance. After the data have been normalized, they are then separated into two sets: one set is used for training, while the other set is used for testing. LDA is utilized to transmit the training set as well as recover crucial attack characteristics. The SFL-HMM technique is used to identify assaults, and it does so by combining the training dataset with the testing dataset. Within the scope of this investigation, we will be looking into a variety of different measures. The histogram, accuracy, ROC, FPR, and TPR, as well as the detection threshold, are all components of this. The findings that were given above show that the strategy that we propose is the most effective one when compared to all of the criteria. However, there are a few problems with the approaches that are currently being used, which will be discussed further below. Standard methods of detection are completely ineffective in Isolation Forest [17] when it comes to finding recently committed crimes. Nevertheless, these detection methods have been hampered by performance limits due to enormous computer processes. In addition to reducing the number of false negatives, this issue needs to be resolved. KLD [18] evaluations are less accurate for investors who are concerned about a firm's eco-efficiency when the scale of the company has been taken into account, which shows that KLD ratings should be used with caution. According to Blockchain [19], cyberattacks are growing increasingly complicated and difficult to distinguish as time goes on. It becomes increasingly complicated for a single or unique (IDS) connection to recognize every threats. As a consequence of this, we have designed a cyber-attack detection system that utilizes self-tuning fuzzy logic in conjunction with heuristic multi-swarm optimization (HMS-ACO).

7. Conclusion

The primary objective of this work was to employ AI and ML techniques for the purpose of performing early detection of the cyber-attack going on the physical system. We studied and examined a variety of alternative approaches of launching a cyberattack. In recent years, techniques for launching cyberattacks have undergone a remarkable transformation. Because those who commit cybercrime are always finding new ways to get around security measures, there is a continuing need for new kinds of detection systems. Because of the vast amount of information that needed to be acquired from a variety of different sources, the identification of cyber attackers necessitated the adoption of techniques from both AI and ML. We present a Fuzzy Logic Hidden Markov Model (SFL-HMM) that is based on Heuristic Multiple Swarm Optimization for the purpose of identifying malicious cyber activity (HMS-ACO).

Future work

The methodologies outlined in this study will be applied by the sensors that make up the technical system in order to obtain new data. After that, it will be compared with several approaches to the genesis of novel concepts. After a solid prediction model has been developed, the next step for the researchers will be to design action for staying safe in potentially dangerous situations.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

References

[1] 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, May 2022.

[2] C. Kwon and I. Hwang, “Reachability Analysis for Safety Assurance of Cyber-Physical Systems Against Cyber Attacks,” IEEE Transactions on Automatic Control, vol. 63, no. 7, pp. 2272–2279, Jul. 2018.

[3] H. Yang, K. Zhan, M. Kadoch, Y. Liang, and M. Cheriet, “BLCS: Brain-Like Distributed Control Security in Cyber Physical Systems,” IEEE Network, vol. 34, no. 3, pp. 8–15, May 2020.

[4] R. Prasad and V. Rohokale, “Artificial Intelligence and Machine Learning in Cyber Security,” Cyber Security: The Lifeline of Information and Communication Technology, pp. 231–247, Oct. 2019.

[5] M. Yildirim, “Artificial Intelligence-Based Solutions for Cyber Security Problems,” Artificial Intelligence Paradigms for Smart Cyber-Physical Systems, pp. 68–86, 2021.

[6] S. Tepjit, I. Horváth, and Z. Rusák, “The state of framework development for implementing reasoning mechanisms in smart cyber-physical systems: A literature review,” Journal of Computational Design and Engineering, vol. 6, no. 4, pp. 527–541, Apr. 2019.

[7] T. Merino, M. Stillwell, M. Steele, M. Coplan, J. Patton, A. Stoyanov, and L. Deng, “Expansion of Cyber Attack Data from Unbalanced Datasets Using Generative Adversarial Networks,” Studies in Computational Intelligence, pp. 131–145, Jul. 2019.

[8] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, “DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber–Physical Systems,” IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5615–5624, Aug. 2021.

[9] B. Hussain, Q. Du, B. Sun, and Z. Han, “Deep Learning-Based DDoS-Attack Detection for Cyber–Physical System Over 5G Network,” IEEE Transactions on Industrial Informatics, vol. 17, no. 2, pp. 860–870, Feb. 2021.

[10] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, “Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey,” IEEE/CAA Journal of Automatica Sinica, vol. 9, no. 3, pp. 377–391, Mar. 2022.

[11] F. Skopik, M. Landauer, M. Wurzenberger, G. Vormayr, J. Milosevic, J. Fabini, W. Prüggler, O. Kruschitz, B. Widmann, K. Truckenthanner, S. Rass, M. Simmer, and C. Zauner, “synERGY: Cross-correlation of operational and contextual data to timely detect and mitigate attacks to cyber-physical systems,” Journal of Information Security and Applications, vol. 54, p. 102544, Oct. 2020.

[12] A. V. Meleshko, V. A. Desnitsky, and I. V. Kotenko, “Machine learning based approach to detection of anomalous data from sensors in cyber-physical water supply systems,” IOP Conference Series: Materials Science and Engineering, vol. 709, no. 3, p. 033034, Jan. 2020.

[13] A. S. Rajawat, R. Rawat, R. N. Shaw, and A. Ghosh, “Cyber Physical System Fraud Analysis by Mobile Robot,” Studies in Computational Intelligence, pp. 47–61, 2021.

[14] T. Wang, Y. Liang, Y. Yang, G. Xu, H. Peng, A. Liu, and W. Jia, “An Intelligent Edge-Computing-Based Method to Counter Coupling Problems in Cyber-Physical Systems,” IEEE Network, vol. 34, no. 3, pp. 16–22, May 2020.

[15] Y. Maleh, “Machine Learning Techniques for IoT Intrusions Detection in Aerospace Cyber-Physical Systems,” Machine Learning and Data Mining in Aerospace Technology, pp. 205–232, Jul. 2019.

[16] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. (Daphne) Yao, “Deep Learning-based Anomaly Detection in Cyber-physical Systems,” ACM Computing Surveys, vol. 54, no. 5, pp. 1–36, Jun. 2022.

[17] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. (Daphne) Yao, “Deep Learning-based Anomaly Detection in Cyber-physical Systems,” ACM Computing Surveys, vol. 54, no. 5, pp. 1–36, Jun. 2022.

[18] B. Bouyeddou, F. Harrou, B. Kadri, and Y. Sun, “Detecting network cyber-attacks using an integrated statistical approach,” Cluster Computing, vol. 24, no. 2, pp. 1435–1453, Nov. 2020.

[19] O. Ajayi, M. Cherian, and T. Saadawi, "Secured Cyber-Attack Signatures Distribution using Blockchain Technology," 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Aug. 2019.

[20] P. Freitas de Araujo-Filho, G. Kaddoum, D. R. Campelo, A. Gondim Santos, D. Macedo, and C. Zanchettin, "Intrusion Detection for Cyber–Physical Systems Using Generative Adversarial Networks in Fog Environment," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6247–6256, Apr. 2021.

[21] S. Rashid, A. Ahmed, I. Al Barazanchi, A. Mhana, and H. Rasheed, "Lung cancer classification using data mining and supervised learning algorithms on multi-dimensional data set," Period. Eng. Nat. Sci., vol. 7, no. 2, pp. 438–447, 2019.

[22] F. O. Olowononi, D. B. Rawat, and C. Liu, "Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS," IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 524–552, 2021.

[23] C. Li, "Case Study: Online Cyber-Attack Detection in Smart Grid," Reinforcement Learning for Cyber-Physical Systems, pp. 169–188, Feb. 2019.

[24] A. A. AlZubi, M. Al-Maitah, and A. Alarifi, "Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques," Soft Computing, vol. 25, no. 18, pp. 12319–12332, Jun. 2021.

[25] C. M. Paredes, D. Martínez-Castro, V. Ibarra-Junquera, and A. González-Potes, "Detection and Isolation of DoS and Integrity Cyber Attacks in Cyber-Physical Systems with a Neural Network-Based Architecture," Electronics, vol. 10, no. 18, p. 2238, Sep. 2021.

[26] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Federated Learning for Data Privacy Preservation in Vehicular Cyber-Physical Systems," IEEE Network, vol. 34, no. 3, pp. 50–56, May 2020.

[27] B. Wan, C. Xu, R. P. Mahapatra, and P. Selvaraj, "Understanding the Cyber-Physical System in International Stadiums for Security in the Network from Cyber-Attacks and Adversaries using AI," Wireless Personal Communications, May 2021.

[28] H. Karimipour and H. Leung, "Relaxation-based anomaly detection in cyber-physical systems using ensemble kalman filter," IET Cyber-Physical Systems: Theory & Applications, vol. 5, no. 1, pp. 49–58, Oct. 2019.

[29] S. Thakur, A. Chakraborty, R. De, N. Kumar, and R. Sarkar, "Intrusion detection in cyber-physical systems using a generic and domain specific deep autoencoder model," Computers & Electrical Engineering, vol. 91, p. 107044, May 2021.

[30] S. Tan, J. M. Guerrero, P. Xie, R. Han, and J. C. Vasquez, "Brief Survey on Attack Detection Methods for Cyber-Physical Systems," IEEE Systems Journal, vol. 14, no. 4, pp. 5329–5339, Dec. 2020.

[31] I. Al-Barazanchi, S. A. Shawkat, M. H. Hameed, and K. S. L. Al-Badri, "Modified RSA-based algorithm: A double secure approach," Telkomnika (Telecommunication Comput. Electron. Control., vol. 17, no. 6, pp. 2818–2825, 2019, doi: 10.12928/TELKOMNIKA.v17i6.13201.

[32] F. Farivar, M. S. Haghighi, A. Jolfaei, and M. Alazab, "Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT," IEEE Transactions on Industrial Informatics, vol. 16, no. 4, pp. 2716–2725, Apr. 2020.

[33] M. Wu, Z. Song, and Y. B. Moon, "Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods," Journal of Intelligent Manufacturing, vol. 30, no. 3, pp. 1111–1123, Feb. 2017.

[34] A. A. Abokifa, K. Haddad, C. Lo, and P. Biswas, "Real-Time Identification of Cyber-Physical Attacks on Water Distribution Systems via Machine Learning–Based Anomaly Detection Techniques," Journal of Water Resources Planning and Management, vol. 145, no. 1, p. 04018089, Jan. 2019.

[35] S. Sharmeen, S. Huda, and J. Abawajy, "Identifying Malware on Cyber Physical Systems by incorporating Semi-Supervised Approach and Deep Learning," IOP Conference Series: Earth and Environmental Science, vol. 322, no. 1, p. 012012, Aug. 2019.

[36] A. Yeboah-Ofori, S. Islam, and A. Brimicombe, "Detecting Cyber Supply Chain Attacks on Cyber Physical Systems Using Bayesian Belief Network," 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), May 2019.

[37] "Intrusion Detection, Prevention, and Response System (IDPRS) for Cyber- Physical Systems (CPSs)," Securing Cyber-Physical Systems, pp. 390–411, Oct. 2015.

[38] F. Li, Y. Shi, A. Shinde, J. Ye, and W. Song, "Enhanced Cyber-Physical Security in Internet of Things Through Energy Auditing," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5224–5231, Jun. 2019.

[39] D. Li, D. Chen, B. Jin, L. Shi, J. Goh, and S.-K. Ng, "MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks," Lecture Notes in Computer Science, pp. 703–716, 2019.

[40] L. K. Ramasamy, F. Khan, M. Shah, B. V. V. S. Prasad, C. Iwendi, and C. Biamba, "Secure Smart Wearable Computing through Artificial Intelligence-Enabled Internet of Things and Cyber-Physical Systems for Health Monitoring," Sensors, vol. 22, no. 3, p. 1076, Jan. 2022.