ARTICLE

JOURNAL OF UNIVERSITY OF BABYLON

For ENGINEERING SCIENCES (JUBES)

Vol.31, No.3.| 2023

مجلـة جـامعة بـابل للعلـوم الهندسية

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

Detection and Identification of Cyberattacks in CPS by Applying Machine Learning Algorithms

Zina A.Saleh

Department of Studies and Planning, Presidency of the University of Babylon, Iraq

zina.badi@uobabylon.edu.iq

Received:	**22/2/2023**	**Accepted:**	**11/4/2023**	**Published:**	**9/5/2023**

Abstract

In general, cyber-physical systems (also known as CPS) consist of networked components that allow for remote access, monitoring, and examination. Because they were integrated into an unsecured network, they have been the target of multiple cyberattacks. In the event that there was a breach in internet security, an adversary would be able to damage the system, which may have devastating effects. Thus, it is extremely important to maintain the credibility of the CPS. It is becoming increasingly difficult to identify assaults on computerised policing systems (CPSs) as these systems become more of a target for hackers and cyberthreats. It is feasible that Machine Learning (ML) as well as Artificial Intelligence (AI), may also make it the finest of times. Both of these outcomes are plausible. Technology based on artificial intelligence (AI) can play a role in the growth and success of a wide range of different types of enterprises in a variety of different ways. The goal of this type of data analysis is to avoid CPS assaults using machine learning and artificial intelligence techniques. A new framework was offered for the detection of cyberattacks, which makes use of machine learning and artificial intelligence (ML). the process of cleaning up the data in the CPS database is starting by performing normalisation in order to get rid of errors and duplicates. This is done so that the data is consistent throughout. Linear Discriminant Analysis is the method that is used to get the features, and it is known as that (LDA). As a mechanism for the identification of cyberattacks, The suggested used process was the SFL-HMM process in conjunction with the HMS-ACO procedure. The new strategy is evaluated using a MATLAB simulation, and the metrics obtained from that simulation are compared to the metrics received from the earlier methods. The framework is shown to be substantially more effective than traditional techniques in the upkeep of high degrees of privacy, as demonstrated by the outcomes of a number of separate investigations. In addition, in terms of detection rate, false positive rate, and computation time, respectively, the framework beats traditional detection methods.

Keywords: AI, CPS, cyber-attacks, ML, LDA, SFL-HMM, HMS-ACO.

مـجلـة جـــامعة بـــابـل للعلـــوم الهندسية مـجلـة جـــامعة بـــابـل للعلـــوم الهندسية مـجلـة جـــامعة بـــابـل للعلـــوم الهندسية

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

1. INTRODUCTION

Recent developments in technology have led to the introduction of cyber-physical systems. These systems have improved computational and communicational capabilities, and they integrate both physical and cyber-components. As a result, many dynamic applications have seen significant advancements as a result of these systems. Yet, this advancement comes at the expense of increased susceptibility to cyberattacks [1,2,3]. Logical components and embedded computers make up cyber-physical systems, and these systems communicate with one another through various communication routes, including the Internet of Things (IoT). To be more exact, these systems consist of digital or cyber components, analogue components, physical devices, and humans that are meant to interact between the physical and cyber aspects of the system. To put it another way, a cyber-physical system is any system that consists of both cyber and physical components, as well as humans, and possesses the capability to trade between the physical and cyber elements [4,5].

Because cyber-physical systems also include physical components, the security of these hybrid systems is of much greater significance than it was in the case of cyber-only systems [6,7]. It is possible for malicious actors to attack physical components, such as sensors, which are tasked with gathering information from their immediate surroundings and feeding it into the system. The presence of a large number of sensors in the environment, which collect such a large amount of data, with such a wide variety of data, and at such a high speed, is one of the most important challenges that a cyber-physical system faces in its physical component. This challenge is specifically related to the physical part of the system. Another one of the most important tasks will be establishing a connection between the sensors, doing the required calculations, and analysing the data that has been gathered.

Thus, the ability to communicate amongst these sensors, calculate, and operate the system is one of the most significant elements of a cyber-physical system. The detection of cyberattacks through the use of cyber-physical systems is an essential issue that must be addressed in these systems [8]. It is important to keep in mind that cyber-attacks take place in unpredictable ways, and it is not possible to explain these assaults in a method that is both regular and sequential [9]. In general, cyber attacks in cyber-physical systems are divided into two main types: denial of service(Dos) and deception attacks [10]. In denial of service, the attacker prevents communication between network nodes and communication channels.

Nevertheless, deception attacks are those that inject false data into the system. These attacks are carried out by misusing system components such as sensors or controllers, and they have the potential to corrupt data or enter incorrect information into the system, both of which can result in the system behaving inappropriately [11]. The monitoring of the system within the system is able to detect these kinds of attacks. However, if the attacker is able to organise a high-level attack to keep himself from being detected, these attacks are referred to as stealthy deception attacks, and other standard techniques of counteracting such attacks will not work [12,13]. As a result, it is essential to maintain a level of awareness regarding the attacks that take place in order to provide a quick response to those who launch attacks. To put it another way, the security system needs to be aware of the attack in order for it to be able to respond appropriately and locate the attack and take control of it. The use of security analytics to look for hidden trends and figure out how to trick someone is one way to strengthen a cyber defence system. This study's primary objective is to analyse the functionality of deception attacks from the

مـجلـة جـامعة بـابـل للعلـــوم الهندسية مـجلـة جـامعة بـابـل للعلـــوم الهندسية مـجلـة جـامعة بـابـل للعلـــوم الهندسية
info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

perspective of the system, with the goals of identifying and controlling those attacks [14]. Deception attacks can be carried out in one of two ways: either the data that is generated in the system is attacked, or the data that is applied to the system is fake, but it is similar to the data that is sought, and the system accepts it as valid [15]. Hence, in order to ensure the system's safety, it will be necessary to conduct an analysis of the data that is transferred between the nodes. The application of approaches based on machine learning is made more compelling as a result of this motivation. Figure 1. shows the architecture of cybersecurity attacks.

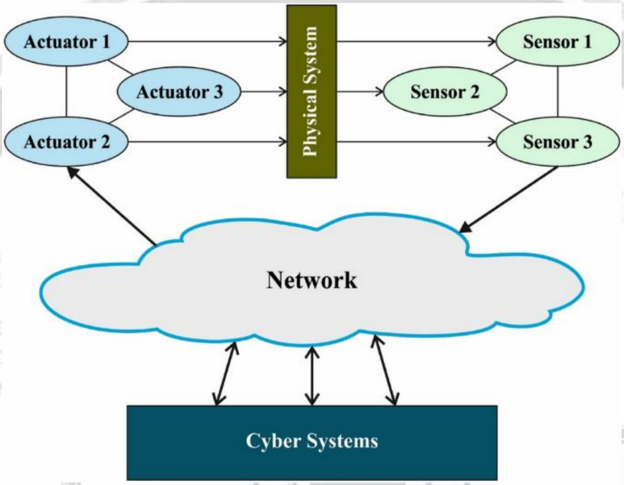

Figure 1. The architecture of cybersecurity attacks.

2. LITERATURES REVIEW

The literature on cyberattack detection techniques is dissected in this section. Smart grids' measures were classified as secure or exploited using machine learning methods [16]. In order to overcome constraints imposed by sparse composition in machine learning, this approach was created for capitalising on existing system knowledge. In this instance, we modelled the attack detection problem using well-known batch and online learning methods, as well as decision and feature level fusion. The statistical learning approaches used to analyse the connections between the statistical and geometric aspects of attack vectors in attack scenarios allowed for the detection of previously unseen attacks.

For the purpose of assessing dangers posed by IoT devices, an intrusion detection system based on artificial neural networks (ANNs) was proposed [17]. The primary objective of this system was to identify DDoS/DoS attacks on an IoT network by differentiating between normal and abnormal traffic patterns. As part of this setup, a multi-level perceptron was trained with data taken from actual Internet traffic. The trained model was then tested to see how well it could prevent DDoS attacks. Also, the ANN's overall performance was evaluated in comparison to an IoT network simulation.

CPSs anomaly detection by recurrent neural network was proposed [18]. (RNN). The primary motivation for this system was to introduce a brand-new approach to behaviorally-based intrusion detection in CPSs. To represent the typical data features of CPSs, a long short-term memory (LSTM)-RNN was used in this system. Following that, anomalies in a water management facility were detected using the cumulative sum technique. To identify and categorise CPS attacks, an anomaly-based detection method was presented [19]. As a first step in establishing what constitutes a normal system, anomaly detection relied on the calculation of outlier scores. The model was then used to spot discrepancies between the new data and the old. Moreover, a Bayes classifier was used to train the supervised assaults model. The attack model was then used to categorise the anomaly, and the confidence levels in the predictions made by the trained classes were assessed.

In order to detect distributed denial of service (DDoS) assaults in smart grids, a detection system [20] was presented, in which the characteristics were extracted from input data using a discrete wavelet transform. Further, the extracted features were used to train a convolutional neural network (CNN), and the network was put through its paces in an experiment designed to determine whether or not it could successfully detect anomalous features in the data given a given threshold value. The unsupervised machine learning approach was presented for use in anomaly detection in a water management system [21]. This approach takes time series data from a CPS and modifies it for use with a deep neural network (DNN) and a one-class support vector machine (SVM). The testbed for safe water treatment (SWaT) data was used to compare the effectiveness of the various approaches. Both sets of detectors were first trained using a log produced by SWaT while it was in operation under varying attack conditions. Additionally, the SWaT's dynamic behaviour was predicted using an LSTM framework.

Based on a deep neural network (DNN) algorithm, a novel approach to detecting sensor attacks [22] was proposed for a car's central processing unit (CPU). The primary goal of this method was to identify deception assaults without any prior knowledge. This technique was used to examine the behaviour of an autonomous vehicle equipped with an inertial measurement unit (IMU) and wheel encoder sensors in the presence of uncertainty and nonlinearity. At first, we determined the many ways in which the sensors could be compromised and settled on a design model accordingly.

Furthermore, performance was also trained and validated using real-world measurement data collected by unmanned ground vehicles. There was a proposal for a new data analytical method [23] to protect smart grids from attacks involving fraudulent data injection. In this method, a data-centric paradigm with a margin setting algorithm was used to detect attacks of bogus data injection (MSA). MSA was educated on the collected data to recognise the threat patterns and accomplish anomaly detection in CPS with great precision. Also, both theoretical and practical methods were used to analyse performance.

They suggested by using a deep learning-based intelligent strategy [24] that assaults on smart grids may be detected in real-time by detecting the injection of bogus data. In this method, the collected features and historical data were used to spot inauthentic data injection attacks as they happened. To further characterise the false data injection attack behaviour that endangers the power system's insufficient number of state measurement due to electricity theft, an optimisation model was also proposed. Deep learning was proposed for the internet of things in order to provide a distributed attack detection mechanism [25]. The primary goal of this plan was to use deep learning into cyber security in order to facilitate the identification of attacks in social IoT.

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

Using a deep learning strategy, they were able to detect cyberattacks [26] by training a previously formed neural network offline by modifying its weights using the training dataset. The neural network was then deployed in real-time online mode to detect cloud-based cyberattacks. In addition, three publicly available empirical datasets (KDDcup 1999, NSL-KDD, and UNSW-NB15) were used for the evaluation. Principal Component Analysis (PCA) was used to pick the most important features from those datasets, thus reducing the computing complexity required for cyber-attack detection. Petri net-based intrusion detection was proposed in CPS [27]. (PN). The primary goal of this method was to concurrently identify abuse and abnormality features of the CPSs. This method was well-suited for enterprise-level CPSs that use supervisory control and data acquisition (SCADA) systems. For this purpose, we suggest the use of a Neural First Order Hybrid Petri Net model (NFOHPN) coupled with online rapid Independent Component Analysis (ICA). Certain features from the KDD 99 dataset were extracted, and then used for the detection.

Deep learning-based detection of dynamic fake data injection threats in smart grid was demonstrated [28]. This method combines a convolutional neural network (CNN) and a long short-term memory network (LSTM) to simultaneously learn system states by monitoring both data measurements and network-level features. For the identification of anomalies in CPS, an approach based on transfer entropy measurements has been presented [29]. This method provides a novel distributed deep learning algorithm for progressively learning high-level features from data in order to identify cyberattacks in IoT. Early sensor measurements concentrated on transfer-entropy, which was subsequently analysed in terms of a variety of variables, including node, channel, and network. Afterwards, classifiers based on deep learning were created utilising the acquired measured values. In this instance, both ANN and DNN were used to train data that may detect cyberattacks on CPSs.

3. MODEL OF THE SYSTEM

In this model, the CPS is represented by a network of four agents, one of which assumes the position of system leader. The leader communicates with three other agents, providing them with control data and the appropriate directives. The working hypothesis is that each agent is a non-holonomic system. Therefore, the coordination problem for mobile agents is more difficult since the position and angle of the centre of the robot cannot be set while the time-varying feedback control technique is in effect [30]. Non-holonomic systems cannot be stabilised using static continuous state feedback. Finding out where each agent's hands are can make things much easier.

In this model, each component of the distributed control system is represented by an autonomous agent. Take into account a system consisting of n agents (e.g., robots) whose interactions follow a linear dynamical trajectory (either first-order or second-order dynamics) [31,32]. These agents use wireless communication to form an agreement on the leader value, and this network is characterised by a complete G-graph [33]. Each agent in this network uses the first-order linear consensus method to manage consensus at each time step, so that each agent's reference status is always a weighted mix of its current status and other Measured states that it receives from its neighbours. As shown in Figure 2.

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية

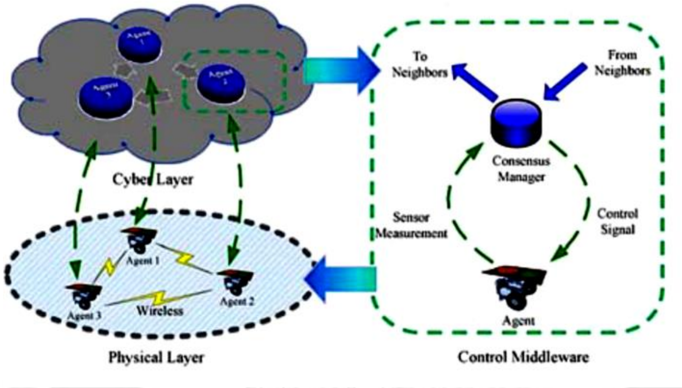

Figure 2. The CPS framework for distributed consensus control [25].

4. METHODOLOGY

The implementation begins once the data has been obtained from the CPS database, they are normalised so that any inconsistencies or duplicates can be deleted. A technique known as feature extraction is utilised for the purpose of data collection (LDA). In order to optimise the system, hybrid model of system (HMS-ACO) processes is employed (SFL-HMM). Figure 3 depicts the effectiveness of the suggested technique.

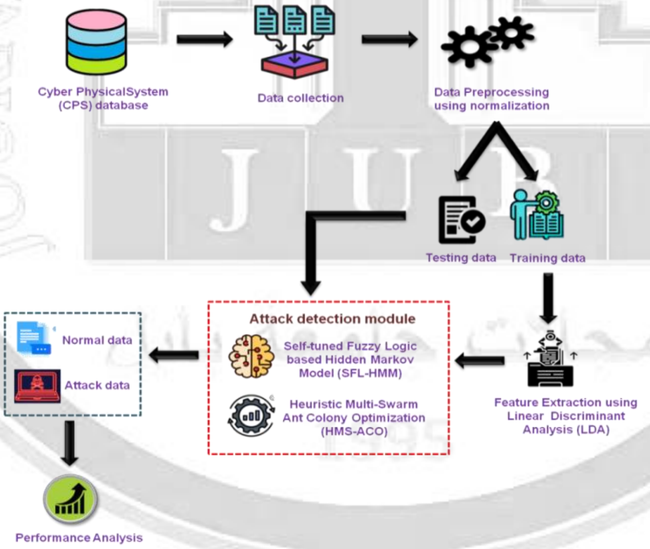
Cyber PhysicalSystem (CPS) database
Data collection
Data Preprocessing using normalization
Testing data
Training data
Attack detection module
Self-tuned Fuzzy Logic based Hidden Markov Model (SFL-HMM)
Heuristic Multi-Swarm Ant Colony Optimization (HMS-ACO)
Feature Extraction using Linear Discriminant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

Figure 3. Depicts the effectiveness of the suggested technique.

For the data set that was used is the KDD99 dataset, there is a total of forty-one features, and these features are suggestive of twenty-two different kinds of attacks. It is unknown whether the attacker was trying to fully breach the system or only gain access for a short period of time [34]. Table 1 presents and discusses the suggested dataset.

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

Table 1. The presents and discusses the suggested dataset.

Seq.	Feature Name	Data Types	Symbolizations
1ST	Interval	constant	/
2ND	Types of protocol Network S on the D	emblematic	UDP, TCP.and ICMP
3RD	assistance	emblematic	HTTP, and STMP
4TH	flag register	emblematic	SF, Szero, REJ, and etc.
5TH	No. of data bytes from S to D.	constant	/
6TH	bytes transferred from D to S.	constant	/
7TH	connection is from/to the same host/port; 0 -dwelling	emblematic	Zero, One
8TH	Wrong fragment	constant	/
9TH	critical	constant	/
10TH	hot	constant	/
11TH	failed login attempts	constant	/
12TH	successfully logged	emblematic	Zero, One
13TH	No. cooperated	constant	/
14TH	root shell is obtained 0 otherwise	constant	/
15TH	“su root” command attempted; 0 otherwise	constant	/
16TH	No. root	constant	/
17TH	No. file creations	constant	/
18TH	No. shell	constant	/
19TH	No. open files	constant	/
20TH	No. outbound cmds	constant	/
21ST	Host successfully logged	emblematic	Zero, One
22ND	Guest successfully logged	emblematic	Zero, One
23RD	Count up	constant	/
24TH	service connections to the same service count	constant	/

مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

25TH	connections that have “SYN” errors	constant	/
26TH	service connections to the same service serror rate	constant	/
27TH	connections that have “SYN” errors	constant	/
28TH	Rerror rate of service connections to the same service	constant	/
29TH	Rerror rate of service connections to the same	constant	/
30TH	Diff service connections to the same service rate	constant	/
31ST	service connections to the same service diff host rate	constant	/
32ND	bytes transferred from D to S host count	constant	/
33RD	bytes transferred from D to S host srv count	constant	/
34TH	bytes transferred from D to S _host same srv rate	constant	/
35TH	bytes transferred from D to S _host diff srv rate	constant	/
36TH	bytes transferred from D to S_host same src port rate	constant	/
37TH	bytes transferred from D to S host srv diff host rate	constant	/
38TH	Error rate to No. of	constant	/

مـجلة جـامعة بـابل للعلـوم الهندسية مـجلة جـامعة بـابل للعلـوم الهندسية مـجلة جـامعة بـابل للعلـوم الهندسية

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

	data bytes from S to D, error rate.		
39TH	No.of data bytes from S to D, for service location resource record error rate.	constant	/
40TH	Error rate to No. of data bytes from S to D, error rate.	constant	/
41ST	No.of data bytes from S to D, for service location resource record error rate.	constant	/

To complete the implementation process, the following steps were performed:

1. **The first step is the normalization of the data during processing:** This procedure converts values from -1 to 1. Normalization is needed when numerous quality limitations differ greatly. This scaling method is best for data without outliers. This proves the normalization theory. Don't cast data in the 0–1 range unless necessary.

$$\frac{valueAfterNomalization-zero}{one-zero}=\frac{valueBeforeNormalization-minimum}{maximum-minimum} \qquad (1)$$

$$\frac{valueAfterNomalization}{one}=\frac{valueBeforeNormalization-minimum}{maximum-minimum} \qquad (2)$$

$$valueAfterNom=\frac{valueBeforeNoma-minimum}{maximum-minimum} \qquad (3)$$

2.The second step is the extraction of features by using (LDA): LDA's goal is to find a projection vector that reduces the distance between samples of the same class while increasing their range. LDA creates this projection vector using Fisher criterion. Fisher criteria guide LDA.

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

Scatter matrices Tn and Tz are used to make internal and external class comparisons, respectively. Both Tn and Tz can be calculated with the following formulas:

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

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

$$m = arg\,\max_{m^S m=1} m^S\,(T_z - \lambda\, T_n) m \qquad (7)$$

Assume that is a small positive constant

The eigen vector with the lowest eigen value for the expression Tzm = Tnm is the best prediction vector, m, as shown by Eq. 7. In most cases, distinguishing between many groups requires more than just a single projection vector. Multiple-class classification is commonly accomplished in the real world by using a set of projection vectors that optimally satisfy the Fisher criterion. In this case, M=arg min Sr(Ms (tz-tn)M). Using the first k lowest eigenvectors of the matrix TzM = tnM, the projection matrix M can be built. To rephrase, M = [d1,...,dk] Rm*k represents the collection of k selected eigenvectors, where yji Rd and yji= MSCjibe stand for the discriminative feature vectors for each sample, respectively.

3. The third step Module of Attack Detection: this step consists of two parts.

A. SFL-HMM: In order to model ambiguity, the Fuzzy Logic-based Hidden Markov Model (SFL-HMM) makes use of multiple logics. The information gained here could also be used to complete a classification project. There is no requirement for numerical parity among demographic groups. In SFL-HMM, a fuzzy set-based Boolean logic approach, proposals can be represented in a continuous range of true (one) to false (zero) frequencies. Cyberattacks can be broken down into four categories: b1, b2, b3, and b4.

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

The four scenarios denoted by b1, b2, b3, and b4 all include different cutoff values for the provided variable. Figure 4 shows the interplay between two random procedures. One process has a set of undetectable states, while the second process contains observable states. In this case, A is the same as A1, A2, and so on up to AN, where N is the maximum number of concealed states that may be directly determined. The set of M variable symbols S= S1, S2, SM represents some other dynamical system. Both maximum probability estimation (MPE) and expectation maximisation (EM), which are frequently used to determine the SFL-HMM variable amount and the highly probable hidden states, respectively, can have been used to infer the hidden state sequence from the observable state categorization. To do this, we look for the dissimilarity between the two sequences. Figure 5 explains the SFL-HMM method.

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

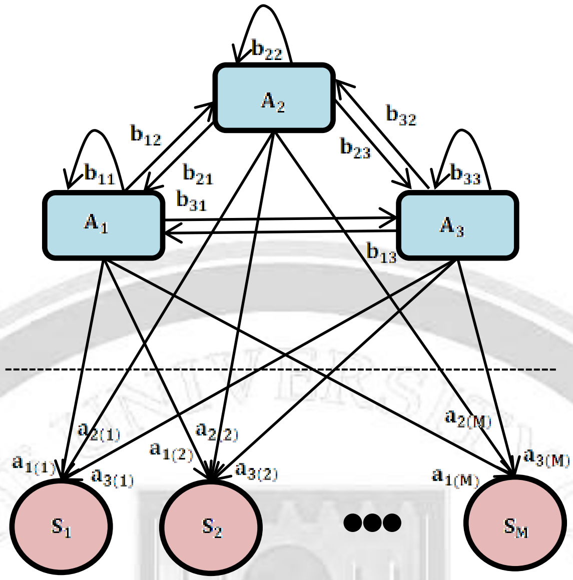

Figure 4. SFL-HMM Function.

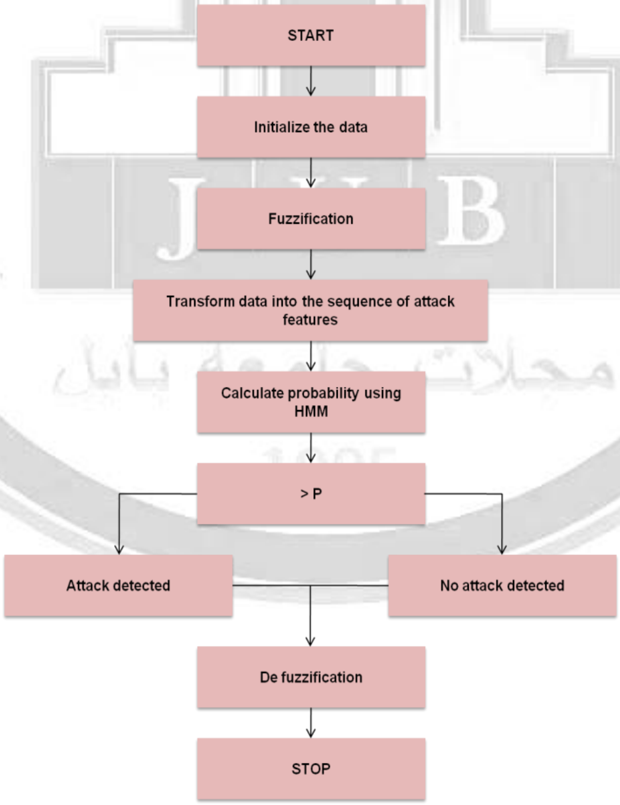

Figure 5. SFL-HMM Process.

www.journalofbabylon.com ISSN: 2616 - 9916 | info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com

B. HMS-ACO: the HMS-ACO is used to address issues with combinative optimisation, where V stands for the set of vertices (nodes) and E stands for the collection of sides. The amount of trail T0 along each of the graph edges is the same, even though the Zants avoid the net nodes on their way to the collection of alternatives. The rule for making this transition from an early notion is given by Eq. 9. After that, actions are carried out repeatedly until a termination condition is met. There are a few distinct phases to this procedure: assessing potential improvements to existing options, enhancing existing pathways, assessing potential improvements to existing solutions.

$$M_{xy}^{l}(s) = \frac{[\tau_{xy}]^{\alpha}[\eta_{xy}]^{\beta}}{\sum_{k\in R_j^l}[\tau_{xy}]^{\alpha}[\eta_{xy}]^{\beta}} if i \in I_l(j)n \qquad (9)$$

Optimization factor influence levels are discovered to be specified by and, independently, while (the heuristic swarm ant-colony). Sij denotes a route that exists on both I and j's surfaces. is yl is Ant k's collection of unexplored nodes. Members of the ACO family of algorithms use a wide range of approaches to selecting and updating nodes on the trail on the way to solving problems. In this study, The HMS-ACO was used to solve the issue of Cloud Service Composition. It is the HMS-ACO that is represented by the algorithm.

Algorithm: Optimization of the Heuristic Multi Swarm Ant Colony (HMSAC)

```
Input: Image and  Variables
Output: $B.D.T_{top}$
$B.D.T_{top\ ts} \leftarrow Produce\ Heuristic\ solve;$
$Pheromone \leftarrow InitializePheromone(Variables.\tau_o);$
$B.D.T_{top} \leftarrow Cost(T_g);$
While (-Stop Condition)
    For(x=1 To Variables, W)
        $Ti_{top} \leftarrow ConstructSolution(pheromone, Image\ , Variables);$
        If ($Ti_{topt} \leq B.D.T_{top}$ )
            $B.D.T_{top} \leftarrow Ti_{top};$
    End
    Local Update & Decay Pheromone. (Pheromone,$Ti_{top}$, $Variables$).
End
Back to ($B.D.T_{top}$)
```

ISSN: 2616 - 9916 | www.journalofbabylon.com | Journal.eng@uobabylon.edu.iq | info@journalofbabylon.com | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية

5. OUTCOMES

In this section, the proposed model was compared with the existing approaches and the system's performance was assessed under a number of cyberattack scenarios. Conventional models include: isolation forests [35], Kullback-Leibler distances [36], and Blockchains [37]. Based on the findings, a method for cyberattack detection was proposed that utilises a hybrid of the state-of-the-art (SFL-HMM) technology and the state-of-the-art (HMS-ACO) algorithm. To measure the Accuracy, the recognition threshold, true positive rate, and false positive rate as well as ROC.

A. Accuracy: One of the key aspects of a test's reliability is its capacity to tell the difference between benign and harmful information. It is important to know the fraction of times test results were categorically positive or negative in order to gauge a test's reliability. Mathematical proofs of this include:

$$Accuracy = \frac{True\ Positive+\ True\ Negative}{True\ Positive+\ \ True\ Negative\ +F\ alse\ Positive+\ False\ Negative} \tag{10}$$

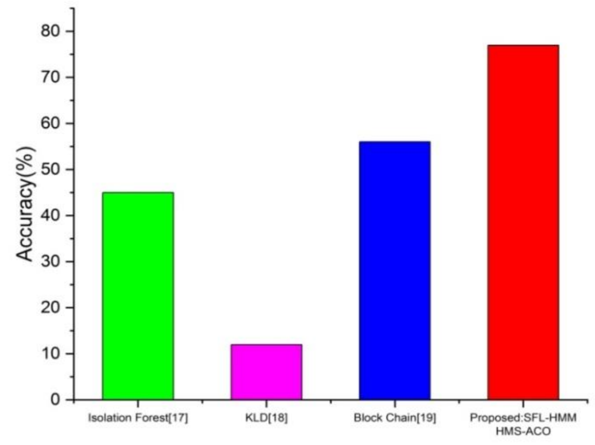

Figure 6. Compared the accuracy of both currently used methods and the proposed method.

As shown in Figure 6, the presently employed approaches compare to the proposed ones. The proposed strategy stands a much better chance of moving closer to the goal.

B. True Positive Rate (TPR): is measures how often optimistic class estimations match actual data.

$$True\ Positive\ Rate = \frac{True\ Positive}{True\ Positive\ +False\ Negative} \tag{11}$$

مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

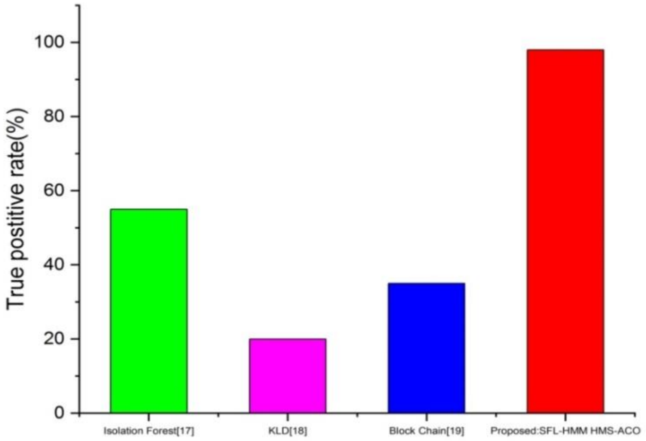

Figure 7. Compared the accuracy of both currently used methods and the proposed method.

Figure 7 compares the true positive rate of the existing method with that of the suggested one. The proposed work has a greater true positive rate than the existing work.

C. False Positive Rate (FPR): in CPS refers to the proportion of incorrect predictions made during a classification task compared to the total number of correct ones.

$$False\ Positive\ Rate\ = \frac{False\ Positive}{\textbf{False Positive}+True\ Negative} \qquad (12)$$

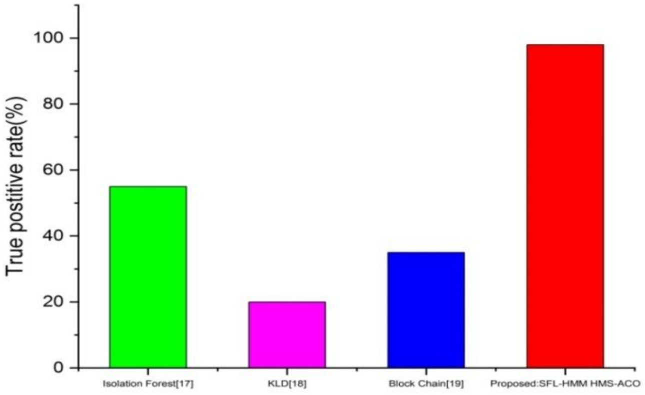

Figure 8. Compared the rate of false of both currently used methods and the proposed method.

D. Detection Threshold: is quickly cyberattacks are spotted is quantified by a metric called the detection threshold. Figure 9 compares the detection thresholds of the currently used methods to those of the suggested ones.

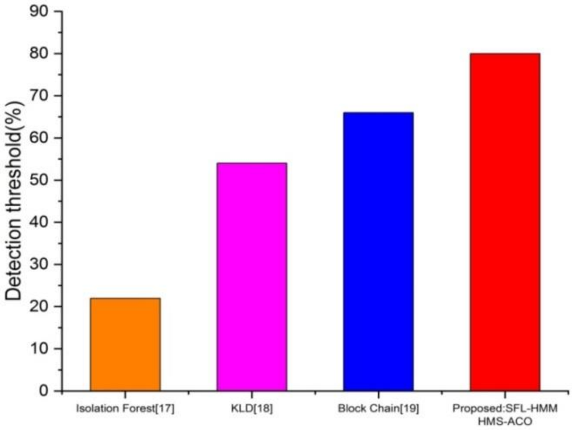

Figure 9. Compared the detection threshold of both currently used methods and the proposed method.

E. Receiver Operating Characteristic (ROC): is a graph showing the RFP vs. detection rate for different values of the preset threshold. The ROC curve for the proposed and existing methods is shown in Figure 10.

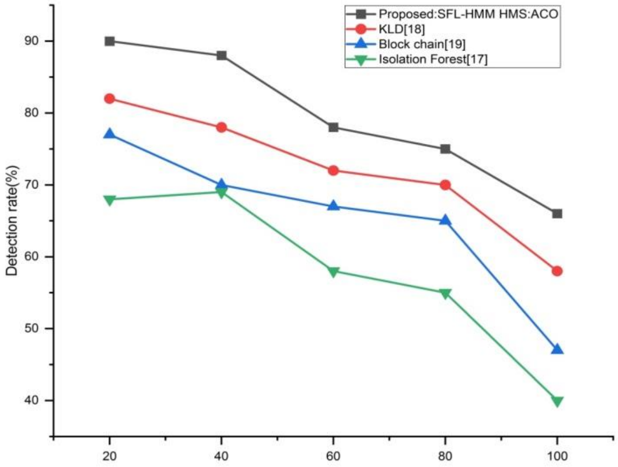

Figure 10. The RFP versus detection rate of the proposed method.

مـــجلـة جـــامعة بـــابـل للعلـــوم الهندسيـة مـــجلـة جـــامعة بـــابـل للعلـــوم الهندسيـة مـــجلـة جـــامعة بـــابـل للعلـــوم الهندسيـة

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

6. DISCUSSION

The outcomes presented above demonstrate that the proposed technique outperforms the alternatives under all conditions. The prevalent methods have a few flaws that need fixing. When it comes to uncovering recent criminal activity, conventional methods of detection are utterly worthless in Isolation Forest [38]. However, the performance of these detection approaches has been limited by the huge computing processing they require. This problem must be fixed along with lowering the rate of false negatives. Given the importance of a company's size, KLD [36] ratings become less reliable for investors concerned about the company's eco-efficiency. Blockchain [37] claims that cyberattacks are becoming more difficult to detect as time passes on because of their rising sophistication. It is becoming increasingly difficult for a single or standalone IDS node to detect all potential security breaches. Hence, a cyber-attack detection system was developed that combines heuristic multi-swarm optimisation with self-tuning fuzzy logic (HMS-ACO).

7. CONCLUSION

In this paper, a robust control consensus strategy was applied for complex discrete cyber-physical networks under attack by several nodes. With this control method, it was discovered that the system could remain stable in the face of cyber threats, isolate the compromised node, and retain performance. The main objective of this study was to use AI and ML methods to spot signs of an impending cyberattack on a real-world computer network. Numerous cyberattack methodologies were researched and analysed. Launching a cyberattack has seen a remarkable evolution in recent years. Since cybercriminals always develop novel countermeasures, innovative detection technologies will be required indefinitely to keep up with them. The detection of cyber attackers required the application of AI and ML approaches because of the large amount of information that had to be gathered from a wide range of sources. The (SFL-HMM) was presented which is dependent on HMS-ACO for the purpose of determining hacks cyber activity. The sensors that make up the technical system employed the procedures indicated in this research to collect. Subsequently, it was contrasted with other methods for coming up with fresh ideas. The next stage for the researchers, after creating a reliable prediction model, will be to create measures for avoiding harm in potentially risky scenarios. In order to counteract future attacks and adapt to user preferences, machine learning allows computers to "learn" from past examples. Cybersecurity may be made easier, more proactive, less expensive, and considerably more effective with the use of machine learning. The control system bases its decisions on the system's reported condition and, if an attack occurs, identifies it and isolates it so that it doesn't affect the behaviour of the other agents. In future work, agent-based attacks, as well as data mining and other machine learning methods to support vector machine (SVM) algorithms and neural network types like recurrent neural networks, can be investigated to evaluate system performance enhancements.

مجلـــة جـــامعة بـــابل للعلـــوم الهندسية مجلـــة جـــامعة بـــابل للعلـــوم الهندسية مجلـــة جـــامعة بـــابل للعلـــوم الهندسية

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

REFERENCES

[1]. Murad, M., Bayat, O., & Marhoon, H. M., 2021. Design and implementation of a smart home system with two levels of security based on IoT technology. Indonesian Journal of Electrical Engineering and Computer Science, 21(1), pp. 546-557.

[2]. Rajawat, A.S., Rawat, R., Shaw, R.N. and Ghosh, A., 2021. Cyber physical system fraud analysis by mobile robot. In ML for Robotics Applications (pp. 47-61). Springer, Singapore.

[3]. Wang, T., Liang, Y., Yang, Y., Xu, G., Peng, H., Liu, A. and Jia, W., 2020. An intelligent edge-computing-based method to counter coupling problems in cyber-physical systems. IEEE Network, 34(3), pp.16-22.

[4]. Li, B., Wu, Y., Song, J., Lu, R., Li, T. and Zhao, L., 2020. DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems. IEEE Transactions on Industrial Informatics, 17(8), pp.5615-5624.

[5]. Zhang, J., Pan, L., Han, Q.L., Chen, C., Wen, S. and Xiang, Y., 2021. Deep learning-based attack detection for cyber-physical system cybersecurity: A survey. IEEE/CAA Journal of AutomaticaSinica, 9(3), pp.377-391.

[6]. de Araujo-Filho, P.F., Kaddoum, G., Campelo, D.R., Santos, A.G., Macêdo, D. and Zanchettin, C., 2020. Intrusion detection for cyber–physical systems using generative adversarial networks in fog environment. IEEE Internet of Things Journal, 8(8), pp.6247-6256.

[7]. Maleh, Y., 2020. ML techniques for IoT intrusions detection in aerospace cyber-physical systems. In ML and Data Mining in Aerospace Technology (pp. 205-232). Springer, Cham.

[8]. Jamal, A.A., Majid, A.A.M., Konev, A., Kosachenko, T. and Shelupanov, A., 2021. A review on security analysis of cyber physical systems using ML. Materials Today: Proceedings.

[9]. Hussain, B., Du, Q., Sun, B. and Han, Z., 2020. Deep learning-based DDoS-attack detection for cyber–physical system over 5G network. IEEE Transactions on Industrial Informatics, 17(2), pp.860-870

[10]. Li, F., Shi, Y., Shinde, A., Ye, J. and Song, W., 2019. Enhanced cyber-physical security in internet of things through energy auditing. IEEE Internet of Things Journal, 6(3), pp.5224-5231.

[11]. Olowononi, F.O., Rawat, D.B. and Liu, C., 2020. Resilient ML for networked cyber physical systems: A survey for ML security to securing ML for cps. IEEE Communications Surveys & Tutorials, 23(1), pp.524-552.

[12]. Zhang, J., Pan, L., Han, Q.L., Chen, C., Wen, S. and Xiang, Y., 2021. Deep learning-based attack detection for cyber-physical system cybersecurity: A survey. IEEE/CAA Journal of Automatica Sinica, 9(3), pp.377-391.

[13]. Meleshko, A. V., V. A. Desnitsky, and I. V. Kotenko. "ML based approach to detection of anomalous data from sensors in cyber-physical water supply systems." In IOP conference series: materials science and engineering, vol. 709, no. 3, p. 033034. IOP Publishing, 2020.

[14]. Abokifa, A.A., Haddad, K., Lo, C. and Biswas, P., 2019. Real-time identification of cyber-physical attacks on water distribution systems via ML–based anomaly detection techniques. Journal of Water Resources Planning and Management, 145(1), p.04018089.

[15]. Jahromi, A.N., Karimipour, H., Dehghantanha, A. and Choo, K.K.R., 2021. Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber–Physical Systems. IEEE Internet of Things Journal, 8(17), pp.13712-13722

مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

[16]. Kwon, C. and Hwang, I., 2017. Reachability analysis for safety assurance of cyber-physical systems against cyber-attacks. IEEE Transactions on Automatic Control, 63(7), pp.2272-227.

[17]. Prasad, R. and Rohokale, V., 2020. Artificial intelligence and machine learning in cyber security. In Cyber Security: The Lifeline of Information and Communication Technology (pp. 231-247). Springer, Cham.

[18]. Sedjelmaci, H., Guenab, F., Senouci, S.M., Moustafa, H., Liu, J. and Han, S., 2020. Cyber security based on artificial intelligence for cyber-physical systems. IEEE Network, 34(3), pp.6-7

[19]. Tepjit, S., Horváth, I. and Rusák, Z., 2019. The state of framework development for implementing reasoning mechanisms in smart cyber-physical systems: A literature review. Journal of computational design and engineering, 6(4), pp.527-541.

[20]. Murad, A., Bayat, O., & Marhoon, H. M., 2021. Implementation of rover tank firefighting robot for closed areas based on arduino microcontroller. Indonesian Journal of Electrical Engineering and Computer Science, 21(1), pp. 56-63.

[21]. Karimipour, H. and Leung, H., 2020. Relaxation-based anomaly detection in cyber-physical systems using ensemble kalman filter. IET Cyper-Phys. Syst.: Theory & Appl., 5(1), pp.49-58.

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

[23]. Tan, S., Guerrero, J.M., Xie, P., Han, R. and Vasquez, J.C., 2020. Brief survey on attack detection methods for cyber-physical systems. IEEE Systems Journal, 14(4), pp.5329-5339.

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

[25]. Farivar, F., Haghighi, M.S., Jolfaei, A. and Alazab, M., 2019. AI for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT. IEEE transactions on industrial informatics, 16(4), pp.2716-2725.

[26]. Wu, M., Song, Z. and Moon, Y.B., 2019. Detecting cyber-physical attacks in CyberManufacturing systems with ML methods. Journal of intelligent manufacturing, 30(3), pp.1111-1123.

[27]. Sharmeen, S., Huda, S. and Abawajy, J., 2019, August. Identifying malware on cyber physical systems by incorporating semi-supervised approach and deep learning. In IOP Conference Series: Earth and Environmental Science (Vol. 322, No. 1, p. 012012). IOP Publishing.

[28]. Yeboah-Ofori, A., Islam, S. and Brimicombe, A., 2019, May. Detecting cyber supply chain attacks on cyber physical systems using Bayesian belief network. In 2019 International Conference on Cyber Security and Internet of Things (ICSIoT) (pp. 37-42). IEEE.

[29]. Luo, Y., Xiao, Y., Cheng, L., Peng, G. and Yao, D., 2021. Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. ACM Computing Surveys (CSUR), 54(5), pp.1-36.

[30]. Yang, H., Zhan, K., Kadoch, M., Liang, Y. and Cheriet, M., 2020. BLCS: Brain-like distributed control security in cyber physical systems. IEEE Network, 34(3), pp.8-15

[31]. AlZubi, A.A., Al-Maitah, M. and Alarifi, A., 2021. Cyber-attack detection in healthcare using cyber-physical system and ML techniques. Soft Computing, 25(18), pp.12319-12332.

[32]. Paredes, C.M., Martínez-Castro, D., Ibarra-Junquera, V. and González-Potes, A., 2021. Detection and Isolation of DoS and Integrity Cyber Attacks in Cyber-Physical Systems with a Neural Network-Based Architecture. Electronics, 10(18), p.2238.

[33]. Lu, Y., Huang, X., Dai, Y., Maharjan, S. and Zhang, Y., 2020. Federated learning for data privacy preservation in vehicular cyber-physical systems. IEEE Network, 34(3), pp.50-56.

[34]. Wan, B., Xu, C., Mahapatra, R.P. and Selvaraj, P., 2021. Understanding the Cyber-Physical System in International Stadiums for Security in the Network from Cyber-Attacks and Adversaries using AI. Wireless Personal Communications, pp.1-18.

[35]. Meira, J., Andrade, R., Praça, I., Carneiro, J. and Marreiros, G., 2018, June. Comparative results with unsupervised techniques in cyber-attack novelty detection. In International Symposium on Ambient Intelligence (pp. 103-112). Springer, Cham.

[36]. Bouyeddou, B., Harrou, F., Kadri, B. and Sun, Y., 2021. Detecting network cyber-attacks using an integrated statistical approach. Cluster Computing, 24(2), pp.1435-1453.

[37]. Ajayi, O., Cherian, M. and Saadawi, T., 2019, August. Secured cyber-attack signatures distribution using blockchain technology. In 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC) (pp. 482-488). IEEE.

[38]. Teyou, D., Kamdem, G. and Ziazet, J., 2019. Convolutional neural network for intrusion detection system in cyber physical systems. arXiv preprint arXiv:1905.03168.

info@journalofbabylon.com | Journal.eng@uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2616 - 9916

ISSN: 2616 - 9916 | www.journalofbabylon.com | Journal.eng@uobabylon.edu.iq | info@journalofbabylon.com

كشف وتحديد الهجمات الالكترونية في الانظمة السيبرانية الفيزيائية (CPS) من خلال تطبيق خوارزميات التعلم الالي

زينة عبد الحسين صالح

قسم الدراسات والتخطيط ، رئاسة جامعة بابل ، العراق

zina.badi@uobabylon.edu.iq

الخلاصة

بشكل عام ، تتكون الأنظمة السيبرانية الفيزيائية (المعروفة أيضًا باسم CPS) من مكونات متصلة بالشبكة تتيح الوصول عن بُعد والمراقبة والفحص. ونظرًا لأنه تم دمج هذه الانظمة في شبكة غير آمنة، قد تتعرض لهجمات إلكترونية متعددة. وفي حالة حدوث خرق لأمن الإنترنت، سيتمكن المخترق من إتلاف النظام ، مما قد يكون له آثار مدمرة. وبالتالي، من المهم للغاية الحفاظ على مصداقية الأنظمة السيبرانية الفيزيائية CPS. لقد أصبح من الصعب بشكل متزايد تحديد الاعتداءات على أنظمة (CPSs) حيث أصبحت هذه الأنظمة أكثر هدفًا للمتسللين والتهديدات الإلكترونية. من الممكن أن يجعل التعلم الآلي (ML) والذكاء الاصطناعي (AI) أيضًا الوضع أكثر أماناً,ويمكن أن تلعب التكنولوجيا القائمة على الذكاء الاصطناعي (AI) دورًا في نمو ونجاح مجموعة واسعة من أنواع المؤسسات المختلفة وبعدة طرق مختلفة. الهدف من هذا البحث وهذا النوع من تحليل البيانات هو تجنب اعتداءات CPS باستخدام تقنيات التعلم الآلي والذكاء الاصطناعي. تم تقديم إطارًا جديدًا لاكتشاف الهجمات الإلكترونية، والذي يستفيد من التعلم الآلي والذكاء الاصطناعي (ML). تبدأعملية تنظيف البيانات في قاعدة بيانات CPS بإجراء التطبيع للتخلص من الأخطاء والتكرارات ويتم ذلك بحيث تكون البيانات متسقة طوال الوقت. التحليل التمييزي الخطي هو الطريقة المستخدمة للحصول على الميزات ، وتعرف باسم (LDA). كآلية لتحديد الهجمات الإلكترونية، كانت العملية المستخدمة المقترحة هي عملية SFL–HMM بالتزامن مع إجراء HMS–ACO. تم تقييم الإستراتيجية الجديدة باستخدام محاكاة MATLAB، ومقارنة المقاييس التي تم الحصول عليها من تلك المحاكاة بالمقاييس الواردة من الطرق السابقة. لقد ثبت أن إطار عمل البحث أكثر فعالية بشكل كبير من التقنيات التقليدية في الحفاظ على درجات عالية من الخصوصية، كما قد اتضح من نتائج عدد من التحقيقات المنفصلة. بالإضافة إلى ذلك، من حيث معدل الاكتشاف، والمعدل الإيجابي الخاطئ، ووقت الحساب، على التوالي ، تتفوق الطريقة المقترحة في البحث على طرق الكشف التقليدية.

الكلمات الدالة: الذكاء الاصطناعي AI، الانظمة الفيزيائية السيبرانية CPS، الهجمات الإلكترونية، التعلم الآلي ML، تحليل التمييز الخطي LDA، نموذج ماركوف المخفي – منطق ضبابي ذاتي SFL–HMM ، التحسين الإرشادي متعدد الأسراب HMS–ACO.