Journal of Intelligent Systems and Internet of Things
Vol. 15, No. 02, PP. 41-54, 2025
DOI: https://doi.org/10.54216/JISIoT.150204

Deep Secure: An Integrated Approach to Anomaly Detection and Cryptographic Protection in Industrial Cyber-Physical Systems

Sameer Nooh[1,*]
[1]Information Systems Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
Email: snooh@kau.edu.sa

Abstract

Industrial Cyber-Physical System (CPS) signify a noteworthy development in industrial automation and control, combining physical and digital parts in order to improve the efficacy, trustworthiness, and functionality of numerous industrial procedures. Industrial CPS are helpful in a huge range of industries such as transportation, energy, manufacturing, and healthcare. Intrusion detection systems (IDs) assist as vigilant protectors, constantly observing network and physical modules for any illegal access, variances, or doubtful actions. They deliver initial threat recognition and prevent safety breaks and operating troubles. In addition, cryptographic protection guarantees the privacy, honesty and genuineness of data that spread across Industrial CPS systems. By utilizing innovative encryption and authentication devices, cryptographic solutions defense complex data from capture or damage preserving consistency and confidentiality of dangerous industrial procedures. The combination of these safety actions creates a strong defence device, boosting the flexibility of Industrial CPS besides developing cyber threats and protecting the reliability of vital industrial processes. This article presents a Deep Secure: An Integrated Approach to Intrusion Detection and Cryptographic Protection in Industrial CPS environment. The proposed model aims to integrate intrusion detection and cryptographic-based secure communication protocol for industrial CPS environments. The Deep Secure model comprises two major phases: intrusion detection and secure communication. Primarily, the intrusion detection process comprises a self-attention-based bidirectional long short-term memory (SA-BiLSTM) technique. Besides, the deer hunting optimization algorithm (DHOA) achieve hyperparameter tuning of the SA-BiLSTM technique. Moreover, a secure communication protocol is designed by the use of the ElGamal cryptosystem. The experimental result of the Deep Secure method was tested in terms of dissimilar measures. A comprehensive result analysis highlighted the advanced performance of the Deep Secure method when associated to other current approaches.

Received: September 22, 2024 Revised: November 15, 2024 Accepted: January 08, 2025

Keywords: Cyber-Physical System; Intrusion Detection; ElGamal cryptosystem; Anomaly Detection; Cyber Attacks

1. Introduction

Industrial CPSs succeed critical organizations by directing procedures depend on "physics" information collected by edge sensor systems. Current improvements in global communication as well as computing technology stimulated the fast integration of greatly connected systems to industrial CPSs [1]. The current scenario has seen quick improvements in CPSs due to high developments in computing, communication and related hardware techniques. A CPS is a combination of physical procedures, global computation, effectual communication and control [2]. In CPSs, several social and physical uses are implemented. The application area includes smart grids, health care, transportation networks, and water or gas distribution systems. Furthermore, wireless sensor and actuator networks [3], networked control systems and wireless industrial sensor networks are referred to as a subcategory of CPSs.

CPSs are significant, physically spread, combined, life-critical and heterogeneous methods in inserted devices as actuators and sensors interact to wisdom, observe and control the physical world [4]. In the CPS process, resource scheduling through several shared or individual networks plays a vital role. One of the crucial tasks is to choose which actuators or sensors must be stimulated to execute specific movements or how to manage sampling action accurately [5]. Owing to physical or technical restrictions, data between actuators, sensors and other networked components spread over networks without appropriate security shields. In addition, the interconnection of extensive networked components makes it complex to defend against in-built physical vulnerabilities [6]. The defence techniques mainly concentrate on CPS security namely game theories, anomaly detection; watermarking and secure routing cannot be useful to industrial CPS directly because it varies from CPSs in various aspects.

For industrial CPS, security tasks need unique solutions that reflect strict industrial environments [7]. If there is an increasing amount of publications, literature mainly concentrates on industrial CPS security due to its quite difference. This liberated performance and estimation of corresponding themes generate an unnecessary variety of evaluation metrics, taxonomies, test environments and implementation methods [8]. This one builds a challenging atmosphere for novel suggestions at the time of research outputs discussion in the united method. An IDS is an efficient safety design, which splits system movement metrics for recognizing mischievous actions in a system [9]. While other intrusion attacks are recognized by altering the system's high-period congestion stream. An IDS is a complete environment that observes network traffic, discovers malicious actions of malevolent and sends alert indications to the supervising station. Moreover, IDSs specially developed to discover several risky matters and realities in an environment [10].

This article presents a Deep Secure: An Integrated Approach to Intrusion Detection and Cryptographic Protection in Industrial CPS environment. The proposed model aims to integrate intrusion detection and cryptographic-based secure communication protocol for industrial CPS environments. The Deep Secure model comprises two major phases: intrusion detection and secure communication. Primarily, the intrusion detection process comprises a self-attention-based bidirectional long short-term memory (SA-BiLSTM) technique. Besides, the deer hunting optimization algorithm (DHOA) achieve hyperparameter tuning of the SA-BiLSTM technique. Moreover, a secure communication protocol is designed by the use of the ElGamal cryptosystem. The experimental result of the Deep Secure method was tested in terms of dissimilar measures.

2. Literature Works

Nagarajan et al. [11] present an anomaly recognition methodology by a combination of DL model called Convolutional Neural Networks (CNNs) with Kalman Filter (KF) established Gaussian-Mixture Model (GMM). This developed technique is mainly employed for detecting and recognizing irregular performance in CPS. Mainly it is essential to pre-process information by changing and clarifying unique data into novel setup as well as attain confidentiality protection of data. Then, the author designed GMM-KF combined deep CNN method for anomaly recognition as well as precisely valued subsequent prospects of anomalous and real actions in CPSs. Dalal et al. [12] developed a unique, actual encryption model for expecting cyber-attacks in physical methods which addresses these worries. The mentioned model employs Bayesian optimization approaches to fine-tune the LightGBM procedure's hyper-parameters.

Kalinin et al. [13] develop a complete method that signifies a dispersed efficient CPS's organization as graphs such as potential attacks and functional dependencies graph. Graph-based symbol permits to delivery of dynamic recognition of many cooperated nodes in efficient organization and adjusts to progressing intrusions. Nguyen et al. [14] project a protected intrusion, blockchain detection depending on data transmission with a method of classification for CPS in health-care regions. This proposed technology executes the data achievement procedure by employing sensor plans and IDs that take place by employing the deep belief network (DBN) technique. Additionally, the developed technique employs a multiple share creation (MSC) approach for several parts groups of the taken image and attains confidentiality as well as safety. In addition, blockchain methodology used for safe data transmission to a cloud server that performs ResNets depends on the detection method for classifying the occurrence of disease.

Jayagopal et al. [15] developed a new Clustered Federated Learning (CFL) model, which classifies cyber-threats beside industrial CPSs. A CFL design permits several CPSs to generate a wide method for upholding privacy. Abdel-Basset et al. [16] project a innovative joined DL approach Fed-TH for searching cyber-attacks against ICPSs that takes time-based and three-dimensional network data representations. Next, a container-based industrial edge calculating structure mainly intended to use Fed-TH as a risk-hunting microservice on appropriate edge servers at the time of preserving covered resource adaptation.

Eltanbouly [17] main goal is to improve DL-based IDs for identifying cyberattacks on CPS by employing multimodal learning models. This report's design, execution, and assessment of dual IDS solutions depend on dissimilar DL networks namely Recurrent Neural Networks (RNNs) and CNNs. For 1st IDS, Gramian Angular Field (GAF) was employed to adapt CPS time-series information to images that were fed to a three-dimensional

CNN to train an attack recognition classifier. The 2nd IDS employs RNN with a multi-modal attention technique for training attack detectors. Li et al. [18] project an anti-honeypot that allows an optimum attack plan for ICPS by using a new game theoretic technique. Particularly, interactions among attackers as well as ICPS defenders taken by a projected hybrid signal and frequent game. For instance, a non-cooperative dual performer one-shot game by imperfect data.

3. The Proposed Model

In this article, an innovative Deep Secure model in an Industrial CPS environment is presented. The proposed model aims to integrate intrusion detection and cryptographic-based secure communication protocol for industrial CPS environments. Fig. 1 portrays the complete flow of the proposed methodology.

A. Detection Process using SA-BiLSTM

Primarily, the intrusion detection process comprises the SA-BiLSTM model. For addressing the tasks modelled by BiLSTM, a self-attention-based deep neural network (DNN) was introduced by integrating LSTM cells [19]. This framework proficiently procedures sequential data and is capable of identifying significant features and handling variable-length sequences.

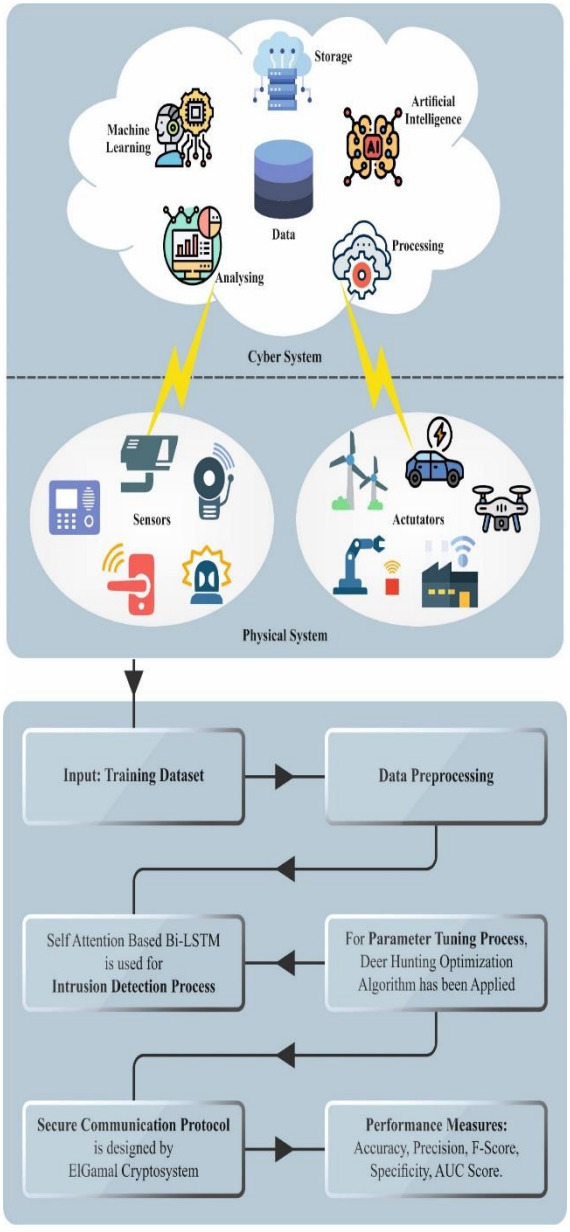

Figure 1. Overall flow of the deep secure model

By leveraging self-attention, this technique concentrates on most related portions of input while ignoring unrelated ones. The multi-head attention device advance to improve ability by allowing equivalent processing of dissimilar sequence shares.

LSTM is capable of learning and recollecting long-term needs as well as overcoming vanishing gradient difficulties so it is a dominant device for sequential data processing. The developed framework provides effective benefits over BiLSTM needs some computations and provides interpretability for a better understanding of forecasts. In this technique, a cell memory state as well as 3 gates are present. According to Eqs. (1)-(6), every LSTM cell's calculation is directed. The procedures inside the LSTM cell are conveyed as A_t, demonstrating the present input vector, h_{t-1} signifying the most current hidden layer (HL) and c_{t-1} denotes the latest memory cell state.

The input sequence endures treatment via BiLSTM, which is surveyed from left to right (Forward LSTM) as well as right to left (Backward LSTM). The results from the mentioned dual directions consequently concatenated to create a combined order of HL. Subsequently, a multi-head attention device has been used. The united HL is categorized into manifold "heads", and consideration weights are individually defined for every head. Then, these weights are employed to calculate a biased sum of HL signified by y_t. At last, attention-informed HL passes over entirely connected layers that result in the model's classification output.

$$inp_t = S_a\left(I_{A.Inp}A_t + R_{h.inp}h_{t-1} + b_v(inp)\right) \quad (1)$$

$$fg_t = S_a\left(I_{A.Fg}A_t + R_{h.Fg}h_{t-1} + b_v(Fg)\right) \quad (2)$$

$$out_t = S_a\left(I_{A.Out}A_t + R_{h.Out}h_{t-1} + b_v(Out)\right) \quad (3)$$

$$m_t = B\left(I_{At}A_t + R_{hc}h_{t-1} + b_v(c)\right) \quad (4)$$

$$c_t = Fg_t c_{t-1} + m_t . Inp_t \quad (5)$$

$$h_t = Out_t . B(c_t) \quad (6)$$

At time t, where inp_t signifies the input gate, fg_t denotes forget gate, out_t represents the output gate, and m_t signifies the input modulation gate. I_A refers to input weights. R represents recursive weights and bias vectors by b_v. An activation function of sigmoid definite by $S_a(A) = (1 + e^{-A})^{-1}$, and hyperbolic tangent function specified by $B(A) = (e^A - e^{-A})/(e^A + e^{-A})$. The vector fg_t delivers possible values for memory cell upgrade that result from present input and previous state over the function of $tanh$ activation. Forget gate fg_t takes part in a vital part in the removal of data that is interconnected before. An output gate out_t grips data for successive processes that rule the cell's output at time t. A hidden layer (HL) h_t designed by employing elementwise development of output gate vector out_t and out_t denotes current memory cell state afterwards predictable by tanh function. By succeeding this, the memory cell mentioned as c_t, is upgraded. Fig. 2 depicts the infrastructure of SA-BiLSTM.

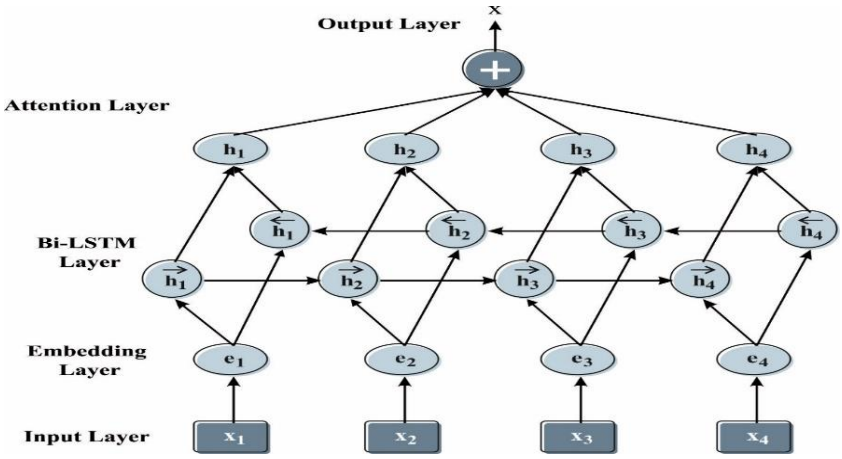

Figure 2. Structure of SA-BiLSTM

BiLSTM and multi-head attention are dual strong DL techniques united in the Multi-Head Attention-based BiLSTM (MHA-BiLSTM) framework. RNNs are capable of procedure sequences for forward as well as backwards recognized as bidirectional LSTMs. This proficiency allows a system to gather historical and then imminent information. Perversely, a method allows a network to focus on numerous basics of input series at once

and improves its ability to perfect long-distance needs. A BiLSTM layer procedure that inputs sequence in MHA-BiLSTM project initially to take time-based dependencies in data. Then, a particular order of HL is formed by concatenating output from forward as well as backward ways. Next, a system assumed multi-head attention to HL to empower it to focus on numerous segments of order. This is proficient by separating HL into numerous "heads" and calculating attention weights for every head separately. While the weighted sum is formed by uniting, attention weights and utilized as input for the next layer of networks. A final networking output is created by feeding attention layer output into many fully associated layers. A last SA-BiLSTM output attained by merging attention-weighted HL as shown below by Eq. (7):

$$y_t = \Sigma(\alpha_t \times h_t) \tag{7}$$

Whereas, Σ signifies the quantity of element-wise development of attention weights α_t and consistent HL denoted as h_t.

B. Hyperparameter Tuning using DHOA

In this work, the tuning process of the SA-BiLSTM method is accomplished by DHOA. DHOA is projected based on the deer hunting operations [20]. Most of the optimum capabilities of deer are vision and smell are 5 to 6 times greater than human vision and smell, correspondingly. Deer also identifies noises with very high frequency. According to the capabilities that deer have, it is capable of escaping from hunters. This formula determines the arbitrary predator population starting with the optimizer model:

$$X = \{x_1, x_2, \dots, x_n\}, 1 < i \leq n \tag{8}$$

At this point, X represents the entire population, and n determines the count of solutions (hunters' swarm).

Variable Initialization

A major variable in this method comprises wind and deer position angles. The solution space assumed under the method is round. Consequently, the boundary of the ring determines the wind angle.

$$\theta_i = 2\pi\delta \tag{9}$$

Whereas, δ signifies an arbitrary amount in [0, 1] range, and the existing iteration is defined by i. A deer angle of location is expressed below:

$$\omega_i = \pi + \theta \tag{10}$$

Whereas, θ stands for the wind angle.

Propagation of location

This stage comprises 2 variables that is place of the following hunter or successor place (Z) and the leader place or place of 1st finest hunter (Z^L).

The leader location

By implementing 1st iteration, the place has been upgraded for the hunters to acquire the finest place.

$$Z_{i+1} = Z^L - y \times S_w \times |L \times Z^L - Z_i| \tag{11}$$

Where Z_i implies existing places, Z_{i+1} refers to next places, S_w stands for arbitrary number based on wind velocity among zero and two, and Y and L illustrate vectors of co-efficient that are written as:

$$L = 2 \times \tau \tag{12}$$

$$y = \frac{25}{100} \times \log\left(I + \frac{1}{I_{\max}}\right)\beta \tag{13}$$

Whereas τ signifies an arbitrary amount between zero and one, I_{max} indicates maximal iteration, and β states a random variable between one and one. Based on process, (Z, X) dose signifies the main condition of predators, and this condition has been enhanced based on prey location. The optimum place represented by (Z^*, X^*) that achieved by enhancing place and utilizing Y and L variables. The hunters attempt to travel near the leader, thus once the leader makes an incorrect move, the hunters remain in their existing place. During this case of $S_w < 1$, the hunter movement is arbitrary and in different ways without concern for an angle of location.

The angle of location

By exploiting the angle of location from location upgrade modelling, search space is enhanced. The angle calculation is paramount for hunter condition preparation for prey is unaware of attack to be reasons for process of hunting prosperous.

$$a_i = \frac{1}{8} \times \pi \times \delta \tag{14}$$

According to the variances among the view angle of prey and wind angle, the variable is represented by which angle of location is upgraded.

$$d_i = \theta_i - a_i \tag{15}$$

The upgrading angle of location is as follows:

$$\omega_{i+1} = \omega_i + d_i \tag{16}$$

As said by the accomplished angle of location, a new place has been achieved as:

$$Z_{i+1} = Z^L - S_w \times |\cos(\omega_{i+1}) \times Z^L - Z_i| \tag{17}$$

Once the hunter is out of sight, the deer cannot see her or him.

The successor location

During this step, exploration is enhanced by utilizing encirclement approaches. By assuming a major random exploration, $the\ L$ amount is no longer assumed that one or more. Therefore, the exchange location is regarded as to upgrade location from a place of 1st optimum solution that makes a global search as:

$$Z_{i+1} = Z^S - y \times S_w \times |L \times Z^L - Z_i| \tag{18}$$

whereas, Z^s refers to the successor hunter location in the existing swarm.

The hunter condition was changed frequently based on the finest solution. This method offers the finest answer When $1 \leq |L|$. Whenever $1 > |L|$, the hunter is randomly elected.

The DHOA model originates a fitness function to get improved classification performance. It describes a positive integer to signify improved candidate output performance. In this research, the minimization of classifying error rate is measured as a fitness function mentioned in Eq. (24).

$$fitness(x_i) = ClassifierErrorRate(x_i)$$
$$= \frac{number\ of\ misclassified\ samples}{Total\ number\ of\ samples} * 100 \tag{19}$$

C. Secure Communication Protocol

At last, the secure communication protocol is designed by the use of the ElGamal cryptosystem. It is nothing but a public-private main cryptosystem with multiplicatively homomorphic property can be given as follows [21].

$$D\big(E(m_1) \cdot E(m_2)\big) = m_1 \cdot m_2. \tag{20}$$

Assume a publicly known cyclic group G of order q by publicly recognized generator g, public key is given as

$$h = g^r, \tag{21}$$

with $r \in \{1,2, \dots, q-1\}$ being selected at random manner. r is the private key.

Encryption of plaintext m to ciphertext c can be implemented as

$$c_1 = g^s, c_2 = m \cdot h^s, \tag{22}$$

With arbitrarily selected $s \in \{1,2, \dots, q-1\}$.

Computing the product of dual ciphertexts produces a product of consistent plaintext after decryption.

The ElGamal cryptosystem with multiplicatively homomorphic properties is transmuted into an additively homomorphic cryptosystem (Paillier) with the Cramer transformation.

The plaintext value to be converted must be in the exponent. m is transformed into m' as follows

$$m' = g^m \ mod\ q. \tag{23}$$

Then, the encryption is applied to m'. However, $g^{\Sigma_i m_i}$ yields as a plaintext after decryption. To retrieve the actual value $\sum_i m_i$ and to resolve discrete logarithm, one of 3 recovery models was used namely (i) Brute Force; (ii) Pollard's Lambda; or (iii) Baby Step Giant Step.

4. Experimental validation

The analysis of the deep secure model is achieved by employing the UNSW-NB15 dataset [22] comprising 10000 samples with ten classes as depicted below table 1:

Table 1: Specification of database

Classes	Sample Numbers
Normal	1000
Generic	1000
Exploits	1000
Fuzzers	1000
DoS	1000
Reconnaissance	1000
Analysis	1000
Backdoor	1000
Shellcode	1000
Worms	1000
Total Samples	10000

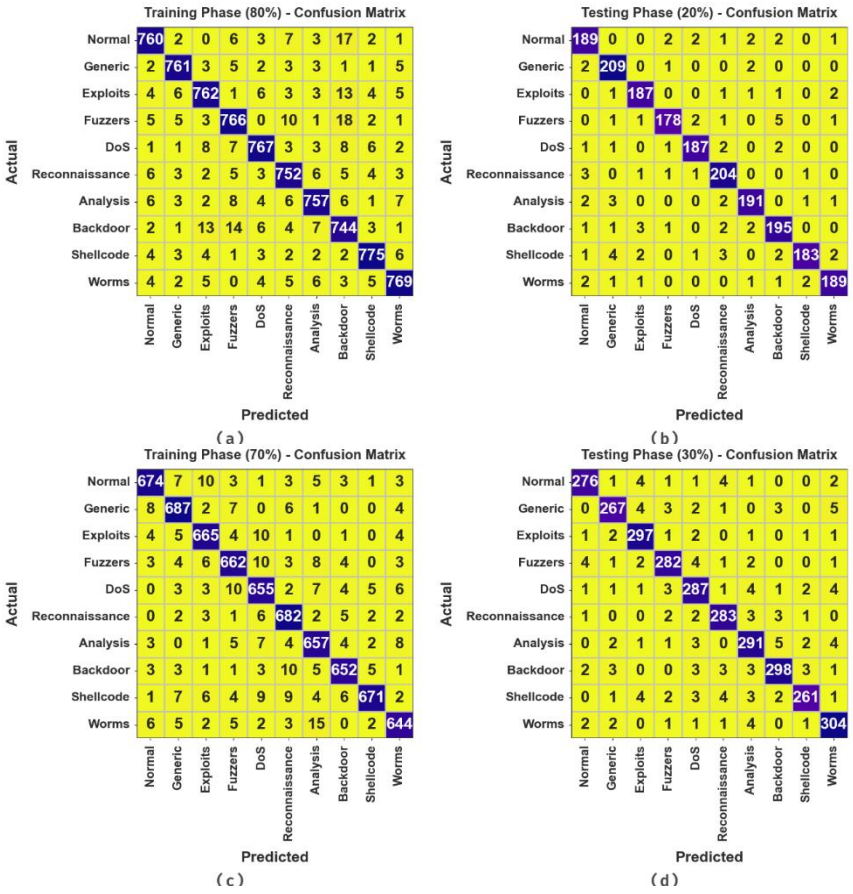

Figure 3. Confusion matrices of (a-c) 80:70 TRPH and (b-d) 20:30 TSPH

Fig. 3 reveals confusion matrices formed by a deep secure model below 80:20 and 70:30 of TRPH/TSPH. The outputs specify effective detection and classification of the overall 10 classes.

The detection results of the deep secure model are investigated on 80:20 of TRPH/TSPH in Table 2 and Fig. 4. The obtained results highlighted that the deep secure model attains effectual performance under all classes. With 80% of TRPH, the deep secure model offers an average $accu_y$ of 99.03%, $prec_n$ of 95.18%, $spec_y$ of 99.46%, F_{score} of 95.17%, and AUC_{score} of 97.31%. Besides, with 20% of TSPH, the deep secure methodology provides an average $accu_y$ of 99.12%, $prec_n$ of 95.66%, $spec_y$ of 99.51%, F_{score} of 95.60%, and AUC_{score} of 97.54%.

Table 2: Detection outcome of the deep secure model on 80:20 of TRPH/TSPH

Classes	$Accu_y$	$Prec_n$	$Spec_y$	F_{Score}	AUC_{Score}
Training Phase (80%)					
Normal	99.06	95.72	99.53	95.30	97.20
Generic	99.36	96.70	99.64	96.76	98.23
Exploits	98.94	95.01	99.44	94.72	96.93
Fuzzers	98.85	94.22	99.35	94.33	96.90
DoS	99.12	96.12	99.57	95.64	97.37
Reconnaissance	99.00	94.59	99.40	94.95	97.36
Analysis	99.04	95.70	99.53	95.16	97.08
Backdoor	98.45	91.06	98.99	92.31	96.29
Shellcode	99.31	96.51	99.61	96.57	98.12
Worms	99.19	96.13	99.57	95.95	97.67
Average	99.03	95.18	99.46	95.17	97.31
Testing Phase (20%)					
Normal	98.90	94.03	99.33	94.50	97.15
Generic	99.15	94.57	99.33	96.09	98.50
Exploits	99.30	95.90	99.56	96.39	98.22
Fuzzers	99.15	96.74	99.67	95.44	96.92
DoS	99.35	96.89	99.67	96.64	98.03
Reconnaissance	99.05	94.44	99.33	95.55	98.01
Analysis	99.15	95.98	99.56	95.74	97.53
Backdoor	98.85	93.75	99.28	94.43	97.20
Shellcode	99.05	97.86	99.78	95.06	96.10
Worms	99.25	96.43	99.61	96.18	97.78
Average	99.12	95.66	99.51	95.60	97.54

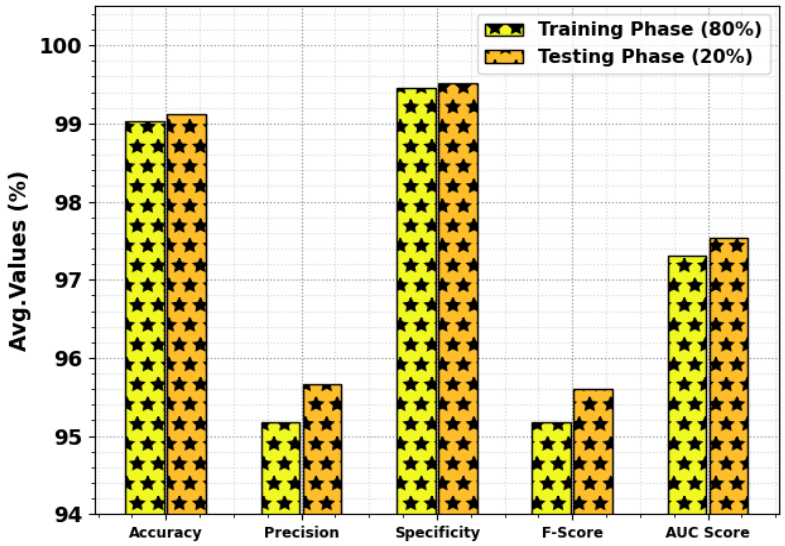

Figure 4. Average of the deep secure model on 80:20 of TRPH/TSPH

The classifying results of the deep secure models were examined on 70:30 of TRPH/TSPH in Table 3 and Fig. 5. The gained results underlined that the deep secure method extents effective performance below all classes. With 70% of TRPH, deep secure technology provides an average $accu_y$ of 99%, $prec_n$ of 95%, $spec_y$ of 99.44%, F_{score} of 94.98%, and AUC_{score} of 97.21%. In addition, with 30% of TSPH, the deep secure approach delivers an average $accu_y$ of 98.97%, $prec_n$ of 94.90%, $spec_y$ of 99.43%, F_{score} of 94.87%, and AUC_{score} of 97.14%.

Table 3: Detection outcome of the deep secure model on 70:30 of TRPH/TSPH

Classes	$Accu_y$	$Prec_n$	$Spec_y$	F_{Score}	AUC_{Score}
Training Phase (70%)					
Normal	99.09	96.01	99.55	95.47	97.24
Generic	99.09	95.02	99.43	95.55	97.76
Exploits	99.10	95.14	99.46	95.48	97.64
Fuzzers	98.84	94.30	99.36	94.23	96.77
DoS	98.74	93.17	99.24	93.71	96.74
Reconnaissance	99.09	94.33	99.35	95.52	98.04
Analysis	98.84	93.32	99.26	94.19	97.17
Backdoor	99.16	96.02	99.57	95.67	97.45
Shellcode	99.07	97.53	99.73	95.38	96.53
Worms	98.96	95.13	99.48	94.64	96.81
Average	99.00	95.00	99.44	94.98	97.21
Testing Phase (30%)					
Normal	99.17	96.17	99.59	95.67	97.38
Generic	98.97	95.36	99.52	94.51	96.60
Exploits	99.17	94.89	99.41	95.96	98.23
Fuzzers	99.03	95.27	99.48	95.11	97.22
DoS	98.70	93.18	99.22	93.64	96.66
Reconnaissance	99.10	94.97	99.45	95.45	97.69
Analysis	98.70	93.27	99.22	93.72	96.70
Backdoor	98.93	95.51	99.48	94.90	96.89
Shellcode	99.00	96.31	99.63	94.57	96.26
Worms	98.97	94.12	99.29	95.15	97.75
Average	98.97	94.90	99.43	94.87	97.14

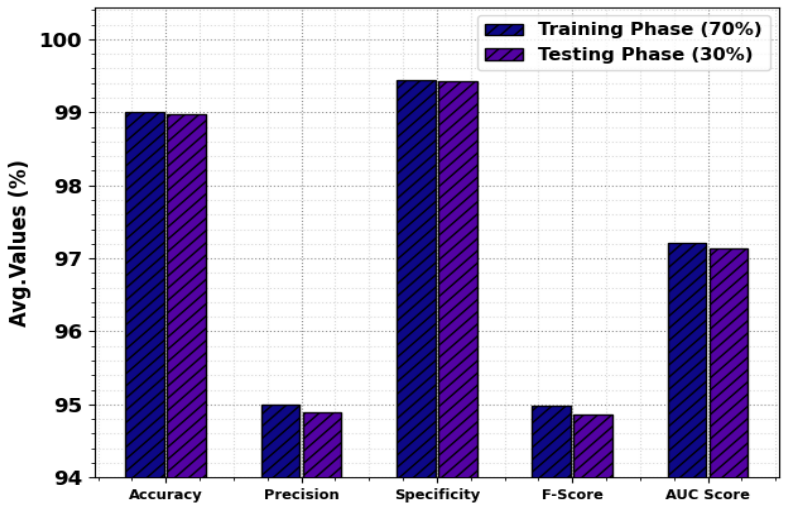

Figure 5. Average of the deep secure model on 70:30 of TRPH/TSPH

The training and validation accuracy curves of the deep secure technique shown in Fig. 6, offer valuable visions into the performance of the deep secure method around many epochs. These curves highlight vital insights into the learning procedure and the model's competence to simplify. Additionally, it is visible that there is a consistence development in TR and TS accuracy over enhancing epochs. It pointed out that the method's ability to learn and identify patterns in both TR/TS datasets. The increasing TR accuracy intends that the model adjust to TR data together with shines in making precise anticipations on before unseen data, accentuating its strong generalizability.

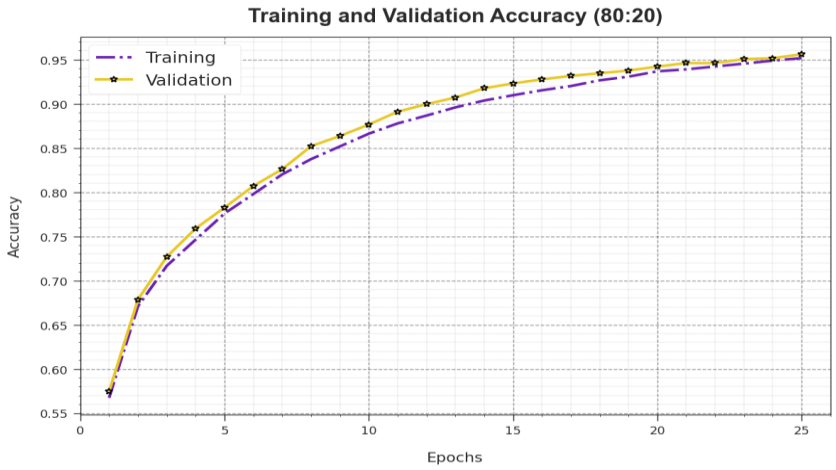

Figure 6. $Accu_y$ Curve of deep secure model on 80:20 of TRPH/TSPH

In Fig. 7, a complete view of TR/TS loss values for deep secure techniques across dissimilar epochs is signified. TR loss gradually lessens as the model increases its weights to mitigate classifying errors on both TR/TS datasets. These loss curves offer a perfect picture of how fine the method assists TR data, highlighting its capacity to professionally grasp patterns in either datasets. It is valuable to note that the deep secure method continuously improves its parameters for decreasing divergences among prediction as well as actual training labels.

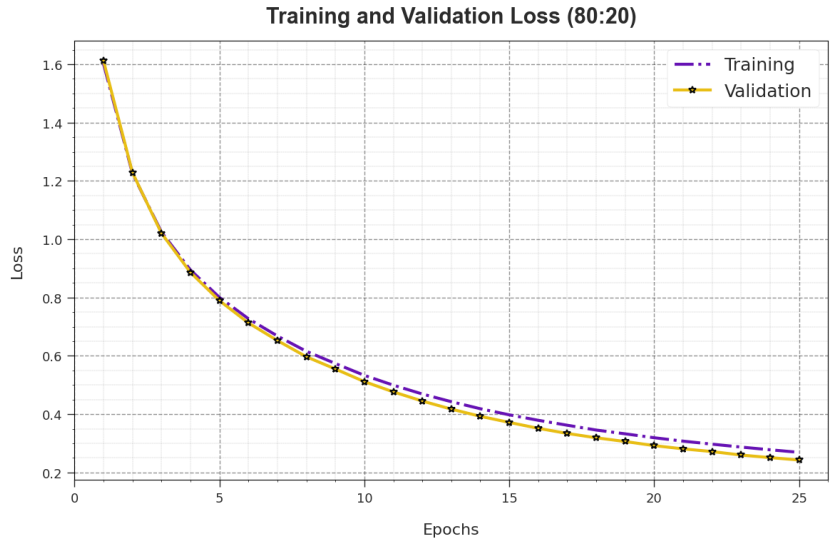

Figure 7. Loss curve of the deep secure model on 80:20 of TRPH/TSPH

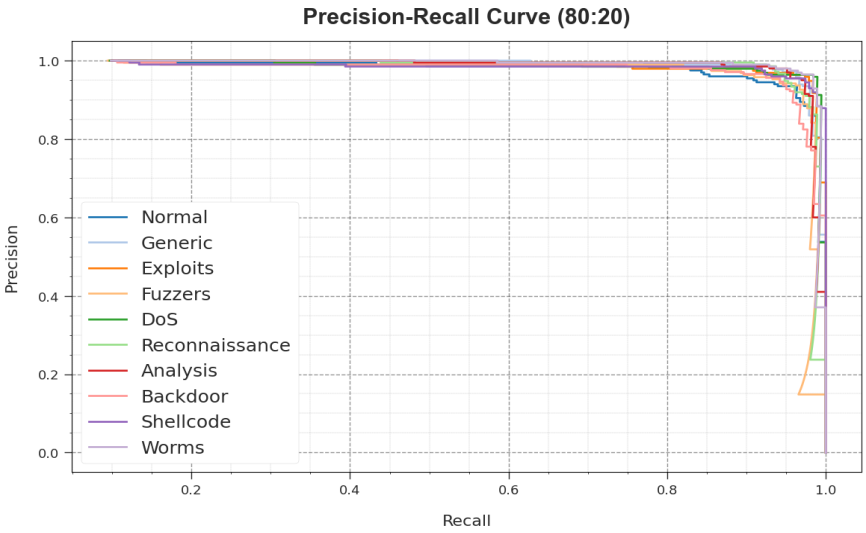

Figure 8. PR curve of the deep secure model on 80:20 of TRPH/TSPH

Concerning the precision-recall curve as given in Fig. 8, results approve that deep secure technology gradually achieves enhanced precision-recall values through each class. The results accentuate the effective aptitude of the method in the perception of diverse classes, underlining efficacy in the recognition of classes.

Moreover, in Fig. 9, ROC curves created by a deep secure technique, which shines in distinguishing among classes is presented. These curves exhibit respected visions into the balance between TPR and FPR through diverse classification thresholds and epochs. The results emphasizes the accurate classification performance below diverse class labels and performance in attempting diverse classification tasks.

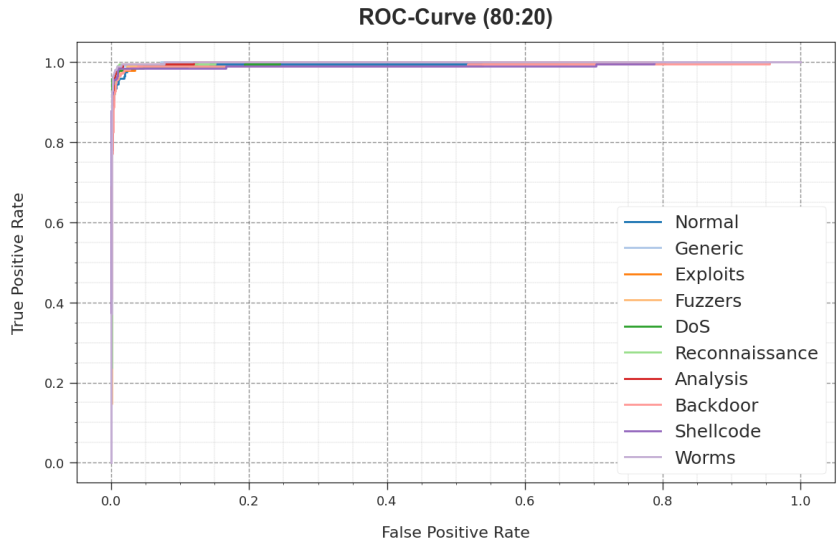

Figure 9. ROC curve of the deep secure model on 80:20 of TRPH/TSPH

A complete comparative result examination of the deep secure model is given in Table 4 and Fig. 10 [23]. The outputs represented that SVM as well as XGBoost-DT approaches reported poor performance while the NN model obtained slightly enhanced performance. Along with that, the LSTM, V-LSTM, and integrated rule-based models depict closer results. However, the deep secure model reaches superior performance with an $accu_y$ of 99.12%, $prec_n$ of 95.66%, $spec_y$ of 99.51%, and F_{score} of 95.60%.

Table 4: Comparative outcome of the deep secure model with present methods

Methods	Accuracy	Precision	Specificity	F-Score
Deep Secure Model	99.12	95.66	99.51	95.60
LSTM	98.80	93.26	95.25	92.55
Neural networks	94.04	94.43	96.16	93.62
Variational LSTM	97.09	92.26	95.66	92.15
XGBoost-DT	90.85	94.69	98.29	92.87
Support Vector Machine	86.04	94.13	96.29	94.14
Integrated rule-based Model	98.35	92.78	97.18	92.96

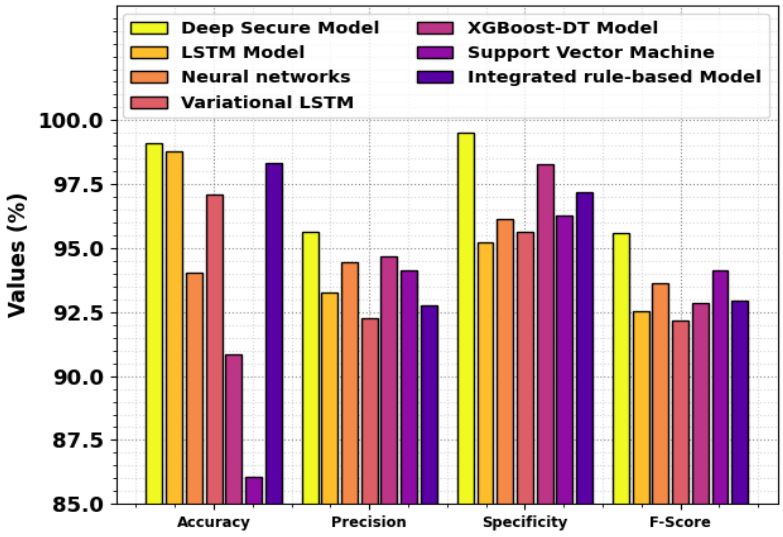

Figure 10. Comparative outcome of the deep secure model with existing methods

In Table 5 and Fig. 11, the computational time (CT) results of the deep secure model with recent approaches are provided. The results show that the deep secure model reaches effectual achievement with a lesser CT of 0.83s. Similarly, the LSTM, NN, V-LSTM, XGBoost-DT, SVM, and integrated rule-based models accomplish poor performance with increased CT values of 1.72s, 4.13s, 2.20s, 2.18s, 1.12s, and 2.23s, respectively. Thus, the deep secure method can be utilized for accomplishing security in the industrial CPS atmosphere.

Table 5: CT outcome of the deep secure model with existing methods

Methods	CT (sec)
Deep Secure Model	0.83
LSTM	1.72
Neural networks	4.13
Variational LSTM	2.20
XGBoost-DT	2.18
Support Vector Machine	1.12
Integrated rule-based Model	2.23

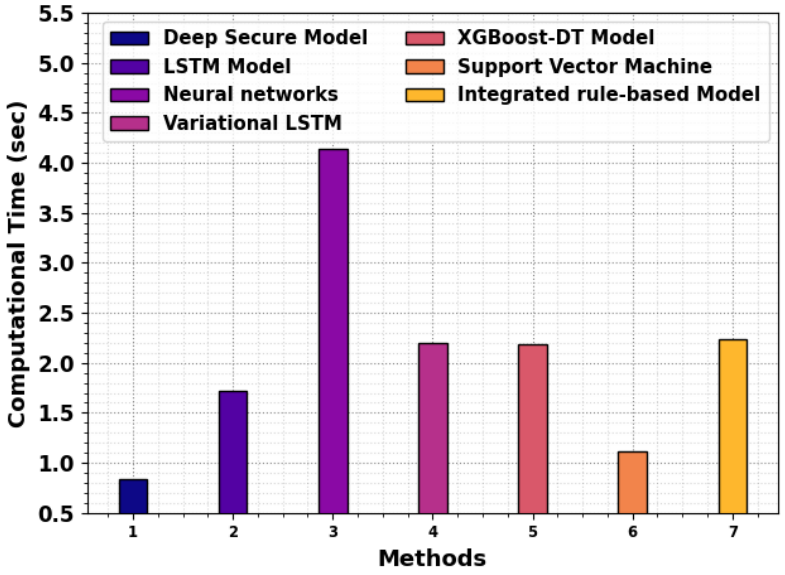

Figure 11. CT outcome of the deep secure model with present methods

5. Conclusion

In this article, a novel Deep Secure model in an Industrial CPS environment is presented. The proposed model aims to integrate intrusion detection and cryptographic-based secure communication protocol for industrial CPS environments. The Deep Secure model comprises two major phases: intrusion detection and secure communication. Primarily, the intrusion detection process comprises the SA-BiLSTM model. Besides, the hyperparameter tuning of the SA-BiLSTM model is achieved by DHOA. Moreover, a secure communication protocol is designed by the use of the ElGamal cryptosystem. The experimental result of the Deep Secure model tested in dissimilar events. A comprehensive result analysis highlighted the superior performance of the Deep Secure method over other current techniques.

Funding: "The author gratefully acknowledges technical support provided by the Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia."

Data Availability Statement: The data that support the findings of this study are openly available in Kaggle repository at https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15, reference number [22].

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] A.A. Nour, A. Mehbodniya, J.L. Webber, A. Bostani, B. Shah, B.Z. Ergashevich, and K. Sathishkumar, "Optimizing intrusion detection in industrial cyber-physical systems through transfer learning approaches," *Computers and Electrical Engineering*, vol. 111, p. 108929, 2023.

[2] M. Umer, S. Sadiq, H. Karamti, R.M. Alhebshi, K. Alnowaiser, A.A. Eshmawi, H. Song, and I. Ashraf, "Deep learning-based intrusion detection methods in cyber-physical systems: Challenges and future trends," *Electronics*, vol. 11, no. 20, p. 3326, 2022.

[3] V.F. Santos, C. Albuquerque, D. Passos, S.E. Quincozes, and D. Mossé, "Assessing machine learning techniques for intrusion detection in cyber-physical systems," *Energies*, vol. 16, no. 16, p. 6058, 2023.

[4] W. Lu, "Detecting malicious attacks using principal component analysis in medical cyber-physical systems," in *Artificial Intelligence for Cyber-Physical Systems Hardening*, Cham: Springer International Publishing, 2022, pp. 203–215.

[5] L. Almutairi, R. Daniel, S. Khasimbee, E.L. Lydia, S. Acharya, and H. Kim, "Quantum dwarf mongoose optimization with ensemble deep learning-based intrusion detection in cyber-physical systems," *IEEE Access*, 2023.

[6] M.R. Aliabadi, M. Seltzer, M.V. Asl, and R. Ghavamizadeh, "Artinali#: An efficient intrusion detection technique for resource-constrained cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 33, p. 100430, 2021.

[7] J.E. Efiong, B.O. Akinyemi, E.A. Olajubu, and G.A. Aderounmu, "GRASSMARLIN-based metadata extraction of cyber-physical systems intrusion detection in CyberSCADA networks," in *2022 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2022, pp. 1122–1128.

[8] L. Almuqren, M.S. Maashi, M. Alamgeer, H. Mohsen, M.A. Hamza, and A.A. Abdelmageed, "Explainable artificial intelligence-enabled intrusion detection technique for secure cyber-physical systems," *Applied Sciences*, vol. 13, no. 5, p. 3081, 2023.

[9] W. Li, Y. Wang, and J. Li, "A blockchain-enabled collaborative intrusion detection framework for SDN-assisted cyber-physical systems," *International Journal of Information Security*, pp. 1–12, 2023.

[10] A.K. Dutta, R. Negi, and S.K. Shukla, "Robust multivariate anomaly-based intrusion detection system for cyber-physical systems," in *Cyber Security Cryptography and Machine Learning: 5th International Symposium, CSCML 2021*, Be'er Sheva, Israel, July 8–9, 2021, vol. 5, pp. 86–93.

[11] S.M. Nagarajan, G.G. Deverajan, A.K. Bashir, R.P. Mahapatra, and M.S. Al-Numay, "IADF-CPS: Intelligent anomaly detection framework towards cyber-physical systems," *Computer Communications*, vol. 188, pp. 81–89, 2022.

[12] S. Dalal, M. Poongodi, U.K. Lilhore, F. Dahan, T. Vaiyapuri, I. Keshta, S.M. Aldossary, A. Mahmoud, and S. Simaiya, "Optimized LightGBM model for security and privacy issues in cyber-physical systems," *Transactions on Emerging Telecommunications Technologies*, p. e4771, 2023.

[13] M. Kalinin, E. Zavadskii, and A. Busygin, "A graph-based technique for securing the distributed cyber-physical system infrastructure," *Sensors*, vol. 23, no. 21, p. 8724, 2023.

[14] G.N. Nguyen, N.H. Le Viet, M. Elhoseny, K. Shankar, B.B. Gupta, and A.A. Abd El-Latif, "Secure blockchain-enabled cyber-physical systems in healthcare using deep belief network with ResNet model," *Journal of Parallel and Distributed Computing*, vol. 153, pp. 150–160, 2021.

[15] V. Jayagopal, M. Elangovan, S.S. Singaram, K.B. Shanmugam, B. Subramaniam, and S. Bhukya, "Intrusion detection system in industrial cyber-physical system using clustered federated learning," *SN Computer Science*, vol. 4, no. 5, p. 452, 2023.

[16] M. Abdel-Basset, H. Hawash, and K. Sallam, "Federated threat-hunting approach for microservice-based industrial cyber-physical system," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1905–1917, 2021.

[17] S.S. Eltanbouly, "Multimodal intrusion detection system for cyber-physical systems," Master's thesis, 2021.

[18] B. Li, Y. Xiao, Y. Shi, Q. Kong, Y. Wu, and H. Bao, "Anti-honeypot enabled optimal attack strategy for industrial cyber-physical systems," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 250–261, 2020.

[19] A. Manderna, S. Kumar, U. Dohare, M. Aljaidi, O. Kaiwartya, and J. Lloret, "Vehicular network intrusion detection using a cascaded deep learning approach with multi-variant metaheuristic," *Sensors*, vol. 23, no. 21, p. 8772, 2023.

[20] R. Pandi Selvam, K. Narayanasamy, and M. Ilayaraja, "Efficient deer hunting optimization algorithm based spectrum sensing approach for 6G communication networks," in *AI-Enabled 6G Networks and Applications*, 2023, pp. 111–129.

[21] F. Knirsch, A. Unterweger, M. Unterrainer, and D. Engel, "Comparison of the Paillier and ElGamal cryptosystems for smart grid aggregation protocols," in *ICISSP*, 2020, pp. 232–239.

[22] [Online]. Available: https://www.kaggle.com/mrwellsdavid/unsw-nb15.

[23] A.I. Alzahrani, A. Al-Rasheed, A. Ksibi, M. Ayadi, M.M. Asiri, and M. Zakariah, "Anomaly detection in fog computing architectures using custom tab transformer for Internet of Things," *Electronics*, vol. 11, no. 23, p. 4017, 2022.