Journal of Theoretical and Applied Information Technology
15th February 2022. Vol.100. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SECURE AND ENERGY-EFFICIENT MODEL FOR CPS USING DEEP LEARNING APPROACH

[1]DEEPTI JOON, [2]KHYATI CHOPRA

[1]GD Goenka University, Gurugram, India

[2]School of Engineering Sciences & Technology, Jamia Hamdard, India

E-mail: [1]joondeepti@gmail.com, [2]Khyatichopra134@gmail.com

ABSTRACT

The Cyber-Physical System (CPS) utilizes Learning Enabled Components (LECs) with neural networks for understanding and decision-making tasks. Neural Networks are commonly used for reasoning and making predictions about energy forecasts, but subsequently, the prediction-based application in security basic frameworks is not effective. LECs can work simpler as CPS if their expectations could be supplemented with a proper certainty in resource measurement that evaluates the amount of output. The paper presents a methodology which is Long Short Term Memory (LSTM)-Adam optimizer based Inductive Conformal Prediction (ICP) for proper usage of resources. The Triplet Network is designed to learn the input data information for estimating the comparability among the test models collects the information. The main aim of the research is to perform forecasting certainty to improve the learning of the neural network classifier. The present approach will select a significant level for overcoming the trade-off error and the main aim is to reduce the false alarms. The present research performs multiple predictions for the Triplet with k-Nearest Neighbour (k-NN) for Non-Conformity Measure (NCM) function that shows significant improvement at a higher level as LSTM and showed lesser error values of 5.86 when compared with the existing K-NN based ICP model that obtained error values of 16.5 and Triplet K-NN of 9.2.

Keywords: *Cyber-Physical Systems, Inductive Conformal Prediction, k-Nearest Neighbour, Long Short Term Memory-Adam Optimizer, Triplet.*

1. INTRODUCTION

Internet of Things (IoT) has revolutionized the available energy resources and is also utilized for the board of electric network frameworks. Presently, the old mechanical frameworks are furnished with electronic gadgets that robotize the customer needs as well as empower two route correspondences between the client and recommend providers called Smart Grid [1]. Although convenient technologies have been created to empower a protected correspondence among providers and buyers, CPS is still inclined to have security issues where particular users may approach specific clients' data [2]. CPSs has extensive attention in these ongoing years as the interdisciplinary addressed the designing technologies among the available spaces. The CPS includes subsystem parts such as sensors, regulators, and actuators that are interconnected with configuration out a shut control circle [3]. The CPS is discovered in various applications using numerous energy compelled gadgets that require effective reasonable plans for fostering. The CPS will manage the model to accompany the head viewpoints effectively to perform the activity, to perform low working, and control the energy effectively. The CPS will accompany a head viewpoint for managing the energy to reduce the number of fuel sources [4]. The CPS works effectively under energy source conditions for restricted fuel sources, and hence frameworks need to be planned with the objective of energy productivity [5].

Also, Machine Learning (ML) calculations are utilized in CPS applications to deal with dubious conditions. DNNs for instance, are utilized for discernment and dynamic undertakings in independent vehicles. Although numerous benefits are used for addressing high dimensional spaces

with approximates its complex structure capacity [6]. The normal DNNs are not straight forward and thus it legitimizes the expectations. Current structures are defined by considering many features and qualities, which makes it exceptionally challenging to think about their requirements [7]. To deal with high-dimensional continuous data and processes the nonconformity scores utilizing the inserting portrayals created through LSTM models that have low dimensional spaces consisting of information in it [8]. The main aim of the research is to improve the certainty among the test models during information collection from an image [9]. These representations are used to estimate the confidence of set predictions from the classifier is dependent on organizing the triplet neural networks [10]. Assessment of the proposed design has proven that CPS obtained from digital assaults shows an insignificant energy utilization without fundamentally affecting framework execution. The improvement however additionally diminished by decreasing the high dimensional spaces and the comparison with existing works gives an accompanying significant knowledge. The proposed LSTM based Adam optimizer for CPS showed lesser error values of 5.86 when compared with the existing K-NN based ICP model that showed error values of 9.2.

2. LITERATURE REVIEW

The existing methods involved in providing security by enhancing the CPS systems are as follows:

Sengan [11] developed Enhanced CPS with hybrid smart city cybersecurity architecture to provide a secure public data-smart network. The existing models examined the security concerns for Smart City infrastructure development both in terms of business operations and technological operations. In the developed model, a Hybrid Smart City Cyber Security Architecture (HSCCA) was developed for analyzing the safe data development against the threats. The developed model setup recommended storing the data and performed a layered presentation to explain the conveying participants made sure that the service is good for the end-users. The suggestions methods analyzed the Cyber Security (CS) for the smart cities highlighted the specific features challenges were generated for cybersecurity reviewed various aspects. However, in the smart city framework, risk factors were hacked at the basic level itself and the models utilized were of resistance to the risk alleviation techniques.

Boursinos and Koutsoukos [12] developed a Trusted Confidence Bounds for Learning Enabled CPS. In the existing models, Deep Neural Networks (DNN) was used that was non-transparent for making decisions showed difficulty for safety-critical systems. Therefore, the proposed approach was used to compute the confidence bounds based on ICP. The Triplet Network architecture learned the input data which was used for testing the similarity among the examples and estimated the confidence for set prediction from the classifier using the Neural Network architecture. However, even if DNN architecture is used as a triplet network, it required collecting the input vector across time and fed parameters for a layer resulted in a large set of parameters to train.

Jadoon [13] developed a modified Hopper-Blum (HB) protocol for automotive CPS in physical layer authentication. The energy and performances in the existing models, showed limitations in security when obtaining results. Accordingly, the present research work proposed an effective secret key age and the board system for giving secure correspondence to computational powerless remote gadgets for the validation conventions. The HB-PL validation was upgraded for an actual encryption technique that produced the length of a key of 128 pieces with less than 55 trade messages that diminished the code size and computational expense for the whole auto remote verification framework. However, the issues related to the security provided an enormous measure of resource utilization for information gain to give the best performances.

Ali [14] developed an Anonymous Orthogonal Code-based Privacy-Preserving Scheme for Industrial CPS. In the existing models, lots of protocols were developed for secure communication among the consumers and suppliers but they were prone to security issues, that led to illegal access to data of specific clients. In the created research an anonymous orthogonal code-based privacy-preserving scheme (ALPHA) for CPSs was proposed. The CPS was considered as a fundamental unit of the cutting-edge savvy lattice, which totaled the force utilization from the electronic gadgets by keeping the client data private, unknown, and untraceable. The created ALPHA, utilized symmetrical digit codes and an organized technique that confirmed and dealt with the secrecy and untraceable nature of client information alongside low correspondence and calculation overheads.

Jithish [15] developed a Decision-centric approach for secure and energy-efficient CPS.

However, in the existing models maximizing the efficiency of energy was important to improve security. Therefore, the present research work introduced a model which used reduced energy consumption as an optimal strategy for CPS which dynamically initialized the security mechanism for onset cyber-attacks. The developed model performed long-term continual operation for improving the security and therefore a Markov Decision Process (MDP) was utilized with threshold values to estimate the optimal energy for the security mechanism. However, a balance between energy efficiency and security was required to sustain the CPS designs and to balance the energy consumption.

Boursinos and Koutsoukos [16] performed assurance monitoring of learning-enabled CPS based on the inductive conformal prediction on the basis of distance learning. The assurance monitoring of CPS based learning enabled the conformal prediction. The developed model allowed a real time assurance which monitored the approach for transforming high dimensional inputs converted to lower sized embedding representations.

Dimitrios Boursinos [17] developed an assurance-based monitoring model for CPS using ML components. Thus, in order to handle the data with high dimension inputs, the scores were computed based on the learning models. The developed approach showed leveraging conformal prediction provided better confidence that allowed and ensured the bounded small error rate limited the number of inputs accurately. However, the approach needed to allow the selection of significant tradeoff errors and alarms that showed that the model failed to implement for real-time monitoring of CPSs.

The leveraging conformal prediction provided confidence with well calibrated that ensured bounded error rate at smaller quantity that were because of the inputs failed to obtain accurate prediction. However, the candidate decisions for prediction was required to be set that deal various cases made a decision confidently needed to satisfy the required higher significance levels.

3. PROPOSED METHOD

The present research work uses Inductive Conformal Prediction (ICP) for similarity estimation among the test input and the training data. The present approach efficiently learns the input representation and for similarity measurement, Euclidean distance is suitable. In the existing models, the DNN architecture is used as a triplet network but it required collecting the input vector across time. Thus, the parameter feeding for a layer resulted in a large set of parameters to train. Whereas, the LSTM can capture the dependency across the time sequences in input vectors, which in turn saves time as well as complexity.

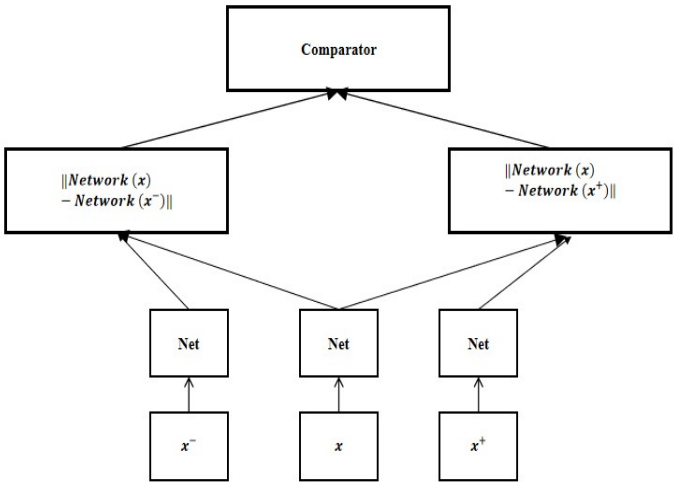

Figure 1: Triplet Network Structure

In the present work, an LSTM model is trained to compute the appropriate metric or distance learning for the model as it consists of three copies of a neural network that shares the common parameters as shown in Fig. 1. The training samples are

- Anchor samples x
- Positive sample x^+
- Negative sample x^-

The anchor and the positive samples belong to the same class whereas the negative sample comes under a different class. The final layer is known as $Network(x)$ that computes the neural network structure and the main objective is:

To maximize the distance among the inputs belonging to distinct classes based on Eq. (1).

$$Maximizedistance = | Network(x) - Network(x^-) | \quad (1)$$

To minimize the distance among the inputs in the same classes based on Eq. (2).

$$Maximizedistance = | Network(x) - Network(x^+) | \quad (2)$$

To perform the aforementioned objectives, the training process uses the loss function which is expressed as shown below in Eq. (3).

$$Loss(x,x^{+},x^{-}) = maximum(|\ Network(x) - Network(x^{+})\ | - |\ Network(x) - Network(x^{-})\ | + \alpha, 0) \quad (3)$$

where α is the value among negative and positive pairs.

The triplet network trains the sample randomly for training the anchor data to perform augmenting on the same data with a different label. The proposed model would lead to slow training and low performances resulted as shown in Eq. (4) failed to provide useful data features.

$$|\ Network(x) - Network(x^{-})\ | < |\ Network(x) - Network(x^{+})\ | \quad (4)$$

Thus training is performed for mining the data carefully at each iteration and shows improvement in the data. The triplets are formed randomly and are used for mining the samples to satisfy the below condition (5):

$$|\ Network(x) - Network(x^{-})\ | < |\ Network(x) - Network(x^{+})\ | \quad (5)$$

From the Eq. (4) and (5), the $Net(x)$ is the distance among the inputs used for calculating the similarity measures during the classification of training data. The training is performed for the LSTM classifier and embeds into the space for training. The distance is used by the ICP framework as described as follows.

3.1. Proposed Triplet based ICP

The proposed section describes the ICP based Triplet Network Architecture. Consider, the example of training, where the examples $z_1,....z_l$ are considered from each z_i pair (x_i, y_i) having the x_i feature vector with the label corresponds to y_i. Consider the input for the test sample as x_{l+1} that performs the classification as shown in Fig. 2. The ICP considers samples from $z_1,....z_{l+1}$ and these are independent and identically distributed from an unknown probability distribution. The significance level is chosen between [0, 1] that sets up possible labels denoted as $\Gamma^{\in}$ for an input x_{l+1}.

The probability of correct labels will not exceed $\in$ and is represented as $y_{l+1} \notin \Gamma^{\in}$. ICP measure is obtained based on dissimilarity metric which is known as Non-Conformity Measure (NCM) that gives examples for the set of $z_1,....z_l$.

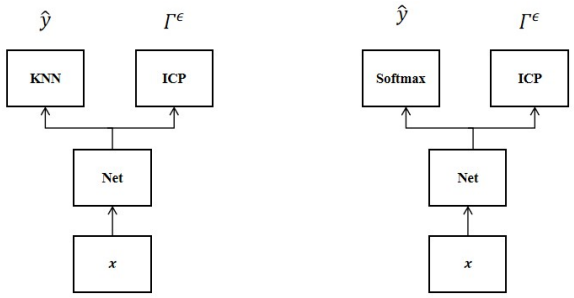

Figure 2: (a) LEC (b) LEC based LSTM classifier

The Triplet Network structure is used for estimating the encoding similarity by using the proposed approach where the inputs are embedded into space using Euclidean distance that measures the two samples for similarity measurement.

The proposed k-NN-NCM identifies similar examples for data training that counts for differently labeled data compared to candidate label y for testing the input x. The mapping is performed from one input space known as X up to the V embedding space at the last layer of a triplet. Where $f: X \to V$ maps the training of the triplet that is completed and computes for storing the encodings. Here, $v_i = f(x_i)$ is used for training the complete triplet scores and computes the encoding is expressed as $v = f(x)$. In the k-NN model, V computes for the labels and is stored with the multi-set is defined Ω .The k-NN includes the test sample x for non-conformity to label represented as 'y' and is expressed as shown in Eq. (6):

$$\alpha(x,y) = |\ I \in \triangleright\ \Omega : I \neq y\ | \quad (6)$$

The proposed k-NN-NCM is required for finding the most similar examples of the training set that has candidate labels as y. Input is defined as x, which is also known as the similar class belonging to the class "y" defined as shown in Eq. (7).

$$\alpha(x,y) = \frac{\min_{I=1,..,n:YI=Y} d(v,V_I)}{\min_{I=1,..,n:YI\neq Y} d(v,V_I)} \quad (7)$$

where $v = f(x)\ and\ V_I = f(x_I)$, the Euclidean distance is known as d that is having metric space as V. For the task simplification, the individual training samples are computed for the generation of large training amount data. This particular content belongs to each of the classes is

similar to that of computed with centroid is computed using the below Eq. (8).

$$\mu Y_I = \frac{\sum_{j=1}^{n_I} v_j^I}{n_I} \quad (8)$$

where μ_{yi} is equal to v_j^I represents the embedding representation for the j^{th} training examples is Y_I and n_I is known as the data training samples for class Y_I. The NCM function is expressed as shown below in Eq (9).

$$\alpha(x,y) = \frac{d(\mu_y, v)}{I = \min_{1,\ldots n: yI \neq y} d(\mu Y_I, v)} \quad (9)$$

Where $v = f(x)$.

The equation is computed based on the nearest centroid known as NCM stored at every class. The NCM $\alpha(x,y)$ which is used for measuring the similarity among the test input x, that is having the candidate label y consists of training data starting from $z_1,....z_l$. Eq. (9), states that the larger the values, the higher will be the dissimilarity indication.

However, measuring it is not ready to give important information and is used for comparing NCM values that compute the calibration using the labeled data. The training set $z_1,....z_l$ is considered and is split into two parts. The first part has the proper training set as $z_1,....z_m$ until up to size $m < l$ and is used for training the triplet network. The calibration set $(z_{m+1}...z_l)$ is defined as having size $l-m$. Thus, an Adam Optimizer is used that acts as the best among the adaptive optimizer in most cases. The adaptive learning rate is perfect for big datasets. The Adam optimized LSTM model generates the parameters consists of a visible layer which has one input, hidden, output layers and 4 neurons that make the single-valued prediction.

Firstly, the method is used to compute, NCMs $\alpha(X_I, Y_I)$, where $I = m+1...l$ with respect to all the examples for the calibration set. The x is the test example with the unknown label known as y, includes form sets as Γ^{ϵ} under all possible labels as $\tilde{y}$. The condition that needs to be followed is, $P(y \notin |\Gamma^{\epsilon}|)$. All the labels of the $\tilde{y}$ ICP will be updated on basis of the p-value function expressed as shown in Eq. (10).

$$P_j(x) = \frac{|\alpha \in A : \alpha \geq \alpha(x,j)|}{|A|} \quad (10)$$

A candidate label will be added to Γ^{ϵ} if the condition is $P_j(x) > \epsilon$.

Depending upon the ideal importance level there might be more than one potential labeled name. Even though these numerous labels can give helpful data, there is no approach for handling more than one potential label and the cases need to be limited. The main purpose is to calculate the output using the Eq. (11) and to compute the process of valid predictions. It will ensure the error rate and guarantees the input examples limits with a good model. The output generated is defined as shown in Eq. (11)

$$Out = \begin{cases} 0 & if\ |\Gamma^{\epsilon}| = 0 \\ 1 & if\ |\Gamma^{\epsilon}| = 1 \\ reject & if\ |\Gamma^{\epsilon}| > 1 \end{cases} \quad (11)$$

Eq. (11) indicates the solitary prediction that limits certainty and if the set Γ is void or has a different label then the Eq. (11) results in a reject state. If the output has been recognized with predictions and without predictions, then it prompts for the distinctive activity to the system. An empty set can sign out the information outside of the distribution while various potential names show that the precision of the basic model is lower than that of the picked ones.

4. RESULTS AND DISCUSSIONS

The present section is about the discussions for evaluation of the results obtained by the proposed triplet network that improves the computation level using ICP. The triplet function learns the parameter by using 4 hidden layers for the fully connected LSTM-Adam optimizer and the representations are learned by the triplet to give better cluster definition. The parameter settings for the proposed LSTM-Adam optimizer based on ICP are stated in table 1.

Table 1: Parameter settings for LSTM model

Layer	(type)
dense_1_input	(Input Layer)
activation_1	(Activation)

Journal of Theoretical and Applied Information Technology
15th February 2022. Vol.100. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

dense_1	(Dense)
activation_1	(Activation)
dense_2	(Dense)
activation_2	(Activation)
dense_3	(Dense)
activation_3	(Activation)
embedding	(Dense)

The proposed simulation runs in a desktop having Intel(R) Core(TM) i9-9900K CPU that has RAM of 32 GB with i9 core processor 9900K CPU and the RTX 2080 GPU with 8 GB memory. Fig. 3 shows the number of samples of training, calibration, and testing for the proposed research.

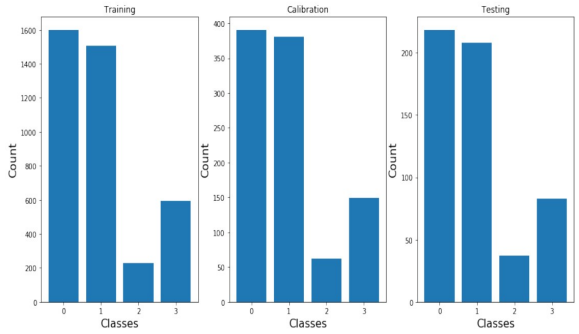

Figure 3: The number of samples of training, calibration, and testing

4.1. Quantitative Analysis

1) Confusion Matrix for test Data

The instances of predicted classes are used for representing the actual classes are represented in rows and columns. The confusion matrix generates two classes in the system that makes the system easy when mislabeled. The 2 dimensions are represented and expressed as shown in Fig. 4 that shows the actual and predicted classes as shown in Fig. 5.

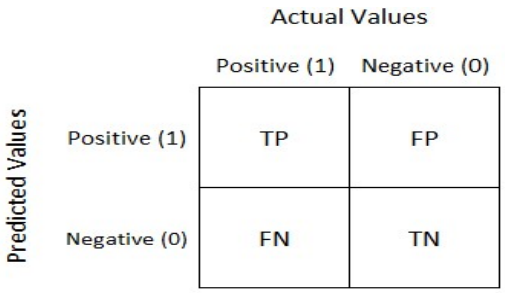

Figure 4: Confusion Matrix format

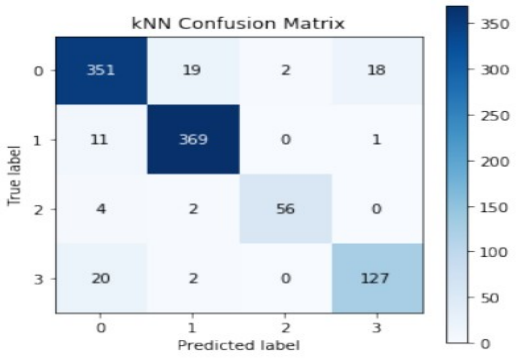

Figure 5: k-NN Confusion Matrix for the proposed LSTM-Adam optimizer based ICP

An example for Confusion Matrix is shown in Fig. 5.

First, verification of the error rates is done by the monitoring algorithm and the solutions are bounded at the significance level. The percentage of improper predictions is graphed against the Cumulative Error (CE) for different values as shown in Fig. 4. The CE is generated for various values obtained from the SCITOSG5 dataset using the centroid of the nearest neighbor. The confidence bounds show how the sets have multiple predicting candidates that are in the range $\in$ [0.001, 0.4], and Fig. 6 shows the plot of the calibration in terms of performance curves in Fig. 6. The multiple predictions decrease as fast as they increase and the error rate is generated as it linearly increases $\in$.

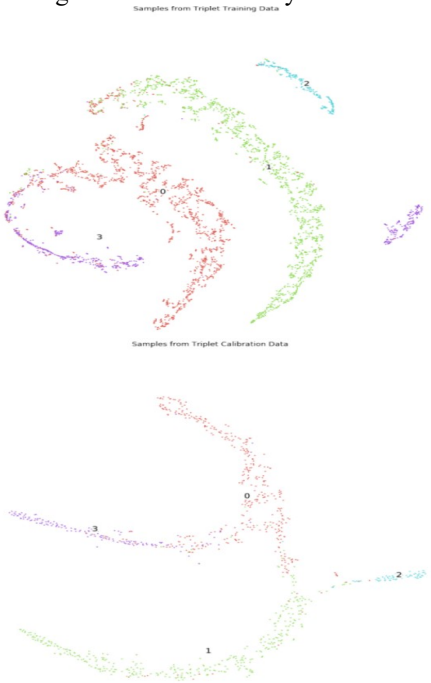

Figure 6: The plot of the training calibration data and samples from triplet training data in terms of performance curves

Journal of Theoretical and Applied Information Technology
15th February 2022. Vol.100. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The results prove that the LSTM with Adam optimizer-based ICP showed certainty that checked the triplet by approving them with the error rates. The current methodology chooses the importance level for compromising the errors and the fundamental target is to diminish the cautions raised. As the up-and-comer plays out various expectations, the Triplet with k-NN for NCM work fulfilled the importance at a more elevated level. At the point when the level is chosen, the triplet calculation utilized numerous multiple candidate predictions. The Train accuracy of 0.9414, Calibration accuracy of 0.9195, Triplet train data silhouette of 0.5952, and Triplet validation data silhouette of 0.5451 are obtained. Fig. 7 shows the plot for the number of nearest neighbors with respect to calibration. The X-axis is the 'Number of Nearest Neighbours' and Y-axis is the 'Calibration'. Similarly, Fig. 8 shows the percentage of Error and multiple predictions with respect to the calibration curve.

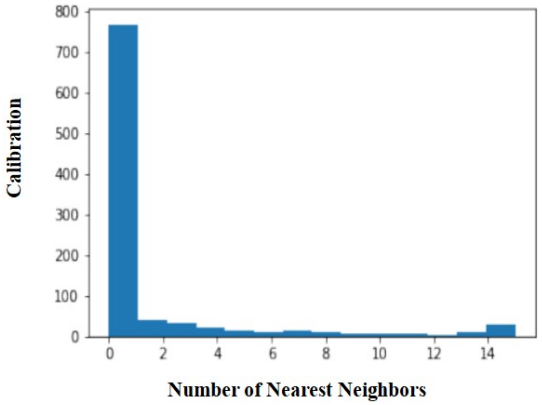

Figure 7: The plot for number of nearest neighbor with respect to calibration.

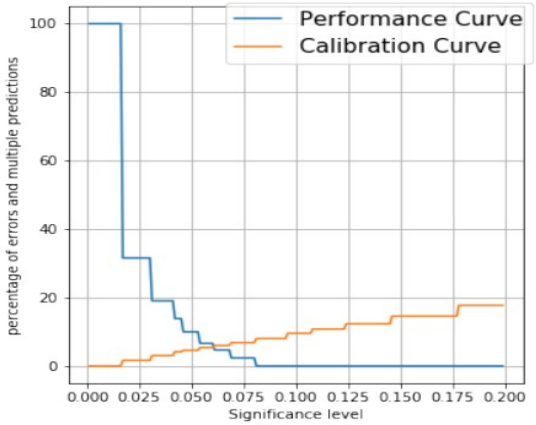

Figure 8: Percentage of Error and multiple prediction for the performance and calibration curve.

4.2. Comparative Analysis

The Table 2 shows the Comparative analysis for the existing and proposed models. The existing K-NN based Triplet architecture made candidate decisions for prediction using SCITOSG5 dataset required various cases satisfied the required higher significance levels and obtained 9.2 error rate. Similarly, when the KNN was used the model showed limitations in terms of computation resulting with an error rate of 16.5. The proposed LSTM with Adam optimizer-based ICP model used SCITOSG5 dataset showed that the confidence monitored the triplet ICP validates the error rates. The present research work selects the importance level to overcome the trade-off the errors and the main aim is to reduce false alarms that were raised as the candidate performed multiple predictions for the Triplet with k-NN. The NCM function satisfies to keep the significance at a higher level and showed error values of 5.86.

Table 2: Comparative analysis

Authors	Method	Error Rate
Dimitrios Boursino and Xenofon Koutsoukoss [17]	k-Nearest Neighbors	16.5
Dimitrios Boursinos and Xenofon Koutsoukos [16]	Triplet-KNN	9.2
Proposed	LSTM-Adam optimizer based ICP	5.86

5. THREATS TO VALIDITY

The present research work identifies threats to validate for the study:

Internal Validity:

The internal validity is dependent on the way evaluation is performed. Thus, the risk is reduced and the evaluation is not validated when the dataset was split into 2 subsets which means, 88 % was used for training, 12 % was used for testing evaluated the results. The validation has to be resized with more percentage of testing for proving the efficiency of the proposed model.

Construct Validity:

The threat is related to the criteria for evaluating the Adam optimizer because Adam with weight decay gets much lower test error. However, in the study, the testing data used for validating the

results was lower and the error rate obtained was fair enough but required improvement further.

6. CONCLUSION

DNN segments are being utilized in CPS to perform assignments such as perception and control. The ICP was utilized for adjusting probabilities forecasted in the sets with more than multiple choices for a given importance level. The Adam which is the best among the adaptive optimizers is utilized in a large portion of the cases. The boundaries of the optimized solution from the Adam optimized LSTM network have an input, hidden, and an output layer with 4 neurons of LSTM. The proposed LSTM with Adam optimizer-based ICP utilized the resources properly. The Triplet Network was designed for learning the input data information for estimating the comparability among the test models that will collect the information. The collected information will be processed to perform the forecasting certainty that improves the neural network classifier learning rate. The present research will select the significant level to overcome the tradeoff error rate which is caused because of false alarms which is an advantage of the model. The results show that the proposed framework of the triplet network for ICP makes the feature selection decline with a decision at a significant level. The advantage of the proposed model was the triplet networks which are usually used for higher-dimensional spaced applications. The limitation of the present research is that because of vanishing gradient problem, the class imbalance problem was occurred from the dataset. However, future work with respect to the proposed model needs an approach that would manage the ICP application for game plans with images, like the camera yields on self-driving vehicles.

REFRENCES:

[1] S. Adepu, N. K. Kandasamy, and A. Mathur, "Epic: An Electric Power Testbed for Research and Training in Cyber-Physical Systems Security", *In: Proc. of Computer Security, Springer, Cham*, pp. 37-52, 2019.

[2] M. Eckhart, and A. Ekelhart, "Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook", *Security and Quality in Cyber-Physical Systems Engineering*, pp. 383-412, 2019.

[3] H. Ge, D. Yue, X. P. Xie, S. Deng, and S. L. Hu, "Analysis of Cyber Physical Systems Security Issue via Uncertainty Approaches", *In: Proc. of Advanced Computational Methods in Life System Modeling and Simulation, Springer, Singapore*, pp. 421-431, 2017.

[4] D. Ding, Q. L. Han, Y. Xiang, X. Ge, and X. M. Zhang, "A Survey on Security Control and Attack Detection for Industrial Cyber-Physical Systems", *Neurocomputing*, Vol. 275, pp. 1674-1683, 2018.

[5] M. Wolf, and D. Serpanos, "Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems", *IEEE*, Vol. 106, No. 1, pp. 9-20, 2017.

[6] A. Burg, A. Chattopadhyay, and K. Y. Lam, "Wireless Communication and Security Issues for Cyber–Physical Systems and the Internet-of-Things", *IEEE*, Vol. 106, No. 1, pp. 38-60, 2017.

[7] J. Yang, C. Zhou, S. Yang, H. Xu, and B. Hu, "Anomaly Detection based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems", *IEEE Transactions on Industrial Electronics*, Vol. 65, No. 5, pp. 4257-4267, 2017.

[8] 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, 2019.

[9] D. P. Zegzhda, M. A. Poltavtseva, and D. S. Lavrova, "Systematization and Security Assessment of Cyber-Physical Systems", *Automatic control and computer sciences*, Vol. 51, No. 8, pp. 835-843, 2017.

[10] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Yao, "Deep Learning-Based Anomaly Detection in Cyber-Physical Systems: Progress and Opportunities," *ACM Computing Surveys*, Vol. 54, No. 5, pp. 1-36, 2021.

[11] S. Sengan, V. Subramaniyaswamy, S. K. Nair, V. Indragandhi, J. Manikandan, and L. Ravi, "Enhancing Cyber–Physical Systems with Hybrid Smart City Cyber Security Architecture for Secure Public Data-Smart Network", *Future generation computer systems*, Vol. 112, pp. 724-737, 2020.

[12] D. Boursinos, and X. Koutsoukos, "Trusted Confidence Bounds for Learning Enabled Cyber-Physical Systems", In: Proc. of IEEE Security and Privacy Workshops, *San Francisco, CA, USA*, pp. 228-233, 2020,

[13] A. K. Jadoon, J. Li, and L. Wang, "Physical Layer Authentication for Automotive Cyber

Physical Systems Based on Modified HB Protocol", *Frontiers of Computer Science*, Vol. 15, No. 3, pp. 1-8, 2021.

[14] W. Ali, I. U. Din, A. Almogren, and N. Kumar, "Alpha: An Anonymous Orthogonal Code-Based Privacy Preserving Scheme for Industrial Cyber Physical Systems", *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 1, pp. 7716-7724, 2020.

[15] J. Jithish, S. Sankaran, and K. Achuthan, "A Decision-Centric Approach for Secure and Energy-Efficient Cyber-Physical Systems", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, pp. 417-441, 2021.

[16] D. Boursinos, and X. Koutsoukos, "Assurance monitoring of learning-enabled cyber-physical systems using inductive conformal prediction based on distance learning", *AI EDAM*, Vol. 35, No. 2, pp. 251-264, 2021.

[17] D. Boursinos, and X. Koutsoukos, "Trusted confidence bounds for learning enabled cyber-physical systems", *In 2020 IEEE Security and Privacy Workshops (SPW)*, pp. 228-233, 2020.