Machine Learning for Human Intelligence
2025, Vol. 3, Issue 2

Research Article

Enhancing Federated Learning Based IDS in Industrial Cybernetic Physical Framework

Muhammad Arslan[1] and Wasif Akbar[1,*]

[1]Faculty of Computing and Emerging Technologies, Emerson University Multan, Punjab, 60000, Pakistan; Email: arslan.shabbir@eum.edu.pk, wasif.akbar@eum.edu.pk
[*]Corresponding author: Wasif Akbar (wasif.akbar@eum.edu.pk)

Article History

Academic Editor:
Muhammad Sajid
Submitted: May 11, 2025
Revised: August 09, 2025
Accepted: September 01, 2025

Keywords:
CNN, Cybersecurity, Deep-Learning, Industrial, CPS dataset.

Abstract

The quick merging of old industrial systems with new networking and computer technologies (including 5G, software-defined networking, and artificial intelligence) has made industrial Cybernetic physical Framework a lot easier to hack. Still, it has been very hard to protect large, complex, and varied industrial Cybernetic physical Framework from cybersecurity concerns since there aren't many good examples of attacks. This research presents an innovative federated DL-Deep-Learning architecture, named , aimed at detecting cybersecurity concerns directed against industrial Cybernetic physical Framework. We first create a new DL-Deep-Learning-based IDS model for industrial Cybernetic physical Framework that uses a gated recurrent unit and a (CNN). Second, we set up a FL Framework that lets a lot of industrial Cybernetic physical Framework work together to construct a full IDS model while also protecting privacy. Comprehensive tests performed on an authentic industrial CPS dataset illustrate the significant efficacy of the proposed approach in identifying diverse cybersecurity concerns to industrial (CPS), as well as its superiority over existing leading techniques.

1 Introduction

Cybernetic physical Framework are essential to the technological progress that is leading to latest phase of global industrial change. They are widely used in areas including urban development, healthcare, transportation, energy and power, and industrial production. The has become a main target for hackers as it grows more connected to cyberspace. Researchers have worked hard to build accurate IDS systems for in order to protect networks from attackers. There are three main types of IDS methods that are used today. There are significant benefits to industrial Cybernetic physical Framework , but these improvements also come with risks [5]–[7]. Old industrial buildings were built without enough security measures, which has left many holes that can't be fixed. The quick adoption of new networking and computing technologies has greatly increased the number of threats by creating new weaknesses that may be used against virtualized endpoints, networks, apps, and cloud services. The BlackEnergy malware intrusion on Ukraine's power grid in December 2015 is a major security breach. More than 30 power substations were shut down, leaving over 230,000 people without power for one to six hours. Some of the most important cyber attacks on industrial Cybernetic physical Framework are Stuxnet, which attacked Iran's nuclear facility [9], VPNFilter, which messed with supervisory control and data acquisition (SCADA) protocols [10], and unauthorized breaches at Australia's Maroochy sewage treatment plant [11], to name a few. These kinds of occurrences make it likely that industrial

Cybernetic physical Framework will be a major focus of interest in the near future, especially by groups that are supported or linked with the government. This shows how important cybersecurity is for industrial Cybernetic physical Framework .

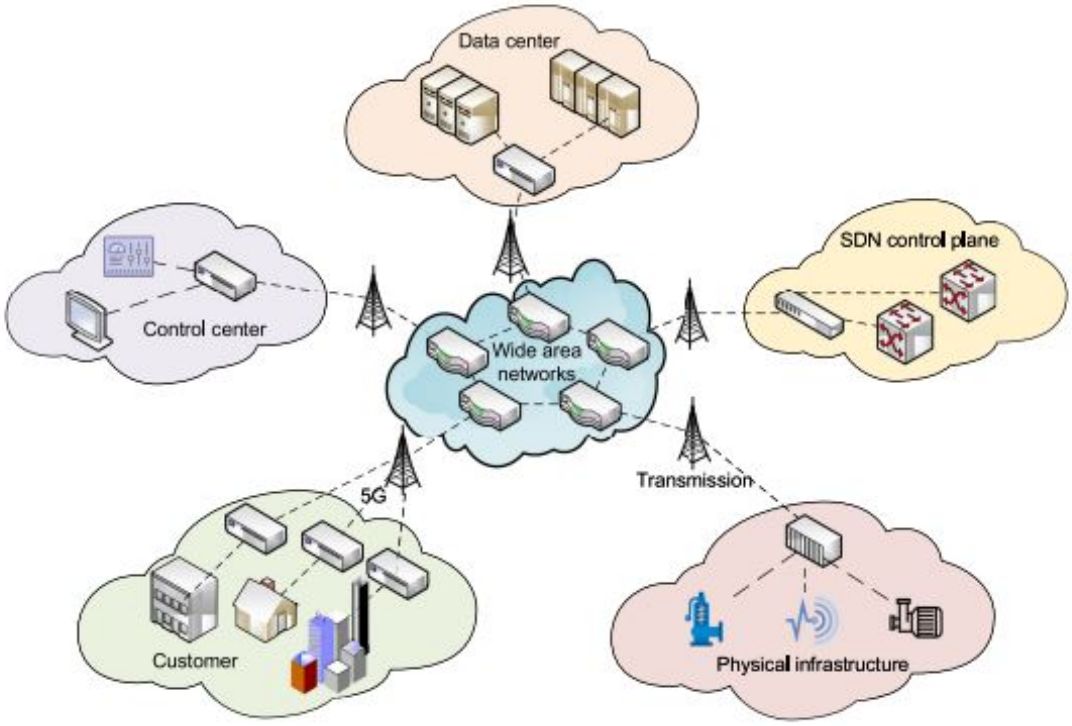

Figure 1: Fundamental architecture of industrial Cybernetic physical Framework

Nonetheless, true intrusion attacks come in many different forms, and there are certain very uncommon types of intrusion attacks that existing detection technologies don't do a good job of categorizing. Imbalanced data makes it hard for the classifier to learn from uncommon class data, which makes the network IDS model much less effective. Then, during reverse diffusion, we slowly remove the Gaussian noise to get the data we need back from the noise [12]. In these circumstances, developing a desirable AI-driven IDS model for the industrial Cybernetic physical Framework appears to be an insurmountable challenge. We initially develop an innovative DL-Deep-Learning model, utilizing (CNN)s (CNN) and gated recurrent units (), to identify diverse forms of cybersecurity concerns targeting industrial Cybernetic physical frameworks. The suggested hybrid CNN–GRU architecture is much more flexible and accurate at finding different kinds of cyberattacks. This is in contrast to traditional IDS methods, which often have trouble with threats that are complex and changing. This design ensures superior detection efficacy and enhanced resilience against sophisticated adversarial maneuvers targeting industrial CPS environments.

In the next step, we set up a federated learning (FL) architecture to make the IDS model work better. In industrial settings, traditional centralized training approaches cause big problems with privacy, scalability, and communication overhead. Our FL design lets several industrial CPS actors in the same region work together to create a single IDS model while keeping their raw data secure. This is how we get around these limitations. The global aggregation process only gets encrypted model updates from each CPS site. Each site handles its own data. This system ensures data sovereignty, secrecy, and compliance with legislation, while also fostering intelligence sharing among businesses. Consequently, the IDS evolves into a more widely applicable and domain-wide robust defense mechanism against cyber threats. We provide a secure communication protocol that uses the Paillier cryptosystem, which is a well-known homomorphic encryption approach, to make the proposed FL-based IDS safer. This protocol makes guarantee that the shared model parameters in the federated training process are safe,

anonymous, and can't be changed. The Paillier-based protocol makes it possible to do computations on encrypted data, which protects crucial model updates from being reverse-engineered or intercepted by bad actors. This security layer not only keeps everyone engaged safe, but it also lowers the risks of insider attacks and outside spying. The suggested three-part contribution—a CNN–GRU-based IDS for industrial CPS, a federated learning architecture for privacy-preserving collaboration, and a secure communication mechanism using homomorphic encryption—makes up a complete and strong cybersecurity solution. This framework solves the two problems of quickly finding attacks and keeping data private, making it a scalable and trustworthy solution for future industrial cyber-physical environments.

2 Related Work

There are three main types of IDS models: those based on statistics, those based on machine learning, and those based on DL-Deep-Learning. For IDS methods that use [13] developed a detection methodology, formulated a universal anomaly and fault threshold Framework. This is what makes early network IDS possible [14]. Statistical methods, on the other hand, need a lot of data and don't provide the order in which the irregularities were found. Setting a threshold is an important part of making the system more accurate. When it comes to machine learning-based techniques. G Stein et al. [15,16] utilized evolutionary algorithms to choose the input feature subset for the decision tree classifier, therefore improving the detection rate and reducing the false positive rate in network IDS. In recent years, there has been an increase in academic interest in IDS systems inside industrial Cybernetic physical Framework . Yang et al. [22,23] created a technique in 2018. Using zone partitioning to find both known and new intrusions in industrial Cybernetic physical Framework , even when numerous zones are being targeted at the same time. In 2018, Wang et al. [17] created a DL-Deep-Learning method that uses a stacked auto-encoder to find Another Study [18] created an IDS system for SCADA networks based on a (CNN) (CNN). In early 2020, Ismail et al. [24,25] investigated energy theft threats within smart grid Cybernetic physical Framework and proposed a DL-Deep-Learning-based IDS method to mitigate these breaches. Liu et al. [19-21] developed a hierarchically distributed IDS system in 2020 Cybernetic physical Framework, to keep industrial Cybernetic physical Framework safe in every way. In natural language processing, they are used to create character-level text using discrete denoising diffusion probability models (D3PM) [26].

3 Proposed Methodology

This part talks about the proposed system. It starts by describing the workflow, then it talks about the CNN–based IDS model, and finally, it talks about the Paillier-based secure communication protocol. Workflow Proposed System The main idea of the scheme is to link a lot of industrial CPS owners so they may work together to build a DL-Deep-Learning IDS model. This is done using a built FL Framework and a secure communication protocol based on Paillier. The detailed steps of the system may be broken down into five components, as shown below (see Algorithm 1 for the workflow).

The proposed intrusion detection system has four essential components: a convolutional feature extraction block, a temporal learning block, a multilayer perceptron (MLP) module, and a softmax classifier (see Fig. 3). There are three stages in the convolutional block. Each stage contains a convolutional layer for extracting local spatial features, a batch normalization layer to make training more stable, and a max-pooling operation to reduce dimensionality. Then, the temporal learning block uses two identical long short-term memory (LSTM) layers that are designed to find sequential correlations and contextual patterns in the characteristics that were recovered. The output is then transferred to the MLP module, which has two fully connected layers and a dropout layer to lower the risk of overfitting and make the model more generic. The softmax layer changes the feature representations into probability distributions for the many types of intrusions. This makes it easier to accurately categorize cyberattacks into several classes.

This helps keep out hostile eavesdroppers and other outside attackers. Our protocol uses the Paillier

Table 1: Summary of Literature Review on IDS Approaches

Author(s)	**Year**	**Method / Approach**	**Contribution**	**Limitations**
Manikopoulos & Papavassiliou	2024	Statistical anomaly detection with thresholds	Early statistical + NN approach for detecting attacks/faults	Requires large datasets, weak on temporal sequence, threshold sensitivity
Cabrera et al.	2020	Statistical traffic modeling	Applied statistical measures of system features for IDS	Cannot reflect time-sequence anomalies
Stein et al.	2021	Decision Tree + Genetic Algorithm	Improved detection rate, reduced false positives	Shallow ML model, struggles with high-dimensional data
Chitrakar & Huang	2019	Incremental SVM (CSV-ISVM)	Semi-partition strategy, improved incremental learning	High computational cost, limited rare-class adaptability
Sommer & Paxson	2018	ML-based IDS in practice	Advocated practical deployment of ML IDS	Highlighted real-world deployment challenges
Mohammadi et al.	2020	Autoencoder + Memetic algorithm	Hybrid IDS model for anomaly detection	Weak handling of imbalanced intrusion data
Wang et al.	2022	Triple CNN + Knowledge Distillation	Lightweight IDS for , improved feature extraction	Limited rare-class detection
Sheikhan et al.	2022	RNN with feature grouping	Reduced-size RNN for misuse detection	Scalability issues, vanishing gradient
Kim et al.	2019	LSTM for IDS	Captured long-term dependencies in traffic	Poor rare-class detection
Imrana et al.	2021	BiLSTM IDS	Improved accuracy with bidirectional learning	Did not solve data imbalance
Ho et al.	2023	Diffusion Probabilistic Model	Introduced denoising diffusion for generative tasks	Computationally expensive, many sampling steps
Deng et al. / Esser et al.	2021	Diffusion in computer vision (ImageNet, Transformers)	Advanced image generation	Focused on images, not intrusion data
Austin et al.	2021	Diffusion for NLP (D3PM)	Generated text data via discrete diffusion	Not applied to IDS
Park et al. / Tashiro et al.	2022	Diffusion for time-series	Filled missing values in time-series	Inspired adaptation, but not applied to IDS

cryptosystem [25], which allows for an infinite amount of homomorphic additions, to enable safe on cloud server module. It has four parts that make it up: Keygenerate, Paraencrypt, Paradecrypt, and Paraagreegate. Algorithm 2 states that each industrial agent trains the suggested DL model

Algorithm 1: Privacy-Preserving Federated Learning

Input: The security parameter κ, industrial agents set $\mathcal{A}$, data resources of all industrial agents $\{\mathcal{D}_k | k \in \mathcal{K}\}$, number of communication rounds R.

Output: The comprehensive deep learning model.

Initialization:

a). The trust authority generates the key pair by $\{\mathcal{PK}, \mathcal{SK}\} = KeyGenerate(\kappa)$;

b). The trust authority establishes a secure channel for the cloud server and each industrial agent;

c). The cloud server initializes $\eta, \rho_1, \rho_2, \varsigma, \mathfrak{L}, B$, and initial model parameters $\mathbf{w}^0$;

d). Each A_k reports a size N_k to the cloud server, where $k \in \mathcal{K}$; then, the cloud server computes each contribution ratio by $\alpha_k = N_k/(N_1 + N_2 + ... + N_K)$;

e). Initialize the communication round index by $r = 1$.

Procedure:

for $r \leq R$ **do**

  (I). For industrial agents:

  for $\forall k \in \mathcal{K}$ **do**

    A_k computes the r-th round local model parameters $\mathbf{w}_k^r$ as per Algorithm 2 with inputs: η, ρ_1, ρ_2, ς, $\mathfrak{L}$, B, $\mathbf{w}^{r-1}$, $\mathcal{A}$, $\mathcal{D}_k$;

    for $\forall j \in \mathcal{T}$ **do**

      $E_{Pai}(w_{k,j}^r) = ParaEncrypt(w_{k,j}^r, \mathcal{PK})$;

    end

    A_k uploads the encrypted model parameters $\{E_{Pai}(w_{k,j}^r) | j \in \mathcal{T}\}$ to the cloud server;

  end

  (II). For cloud server:

  for $\forall j \in \mathcal{T}$ **do**

    $c_j = ParaAggregate(w_{1,j}^r, \cdots, w_{K,j}^r, \alpha_1, \cdots, \alpha_K)$;

  end

  The cloud server distributes the aggregated ciphertexts $\mathbf{c} = \{c_j | j \in \mathcal{T}\}$ to all $A_k (k \in \mathcal{K})$;

  (III). For industrial agents:

  for $\forall k \in \mathcal{K}$ **do**

    for $\forall j \in \mathcal{T}$ **do**

      $\widetilde{w}_{k,j}^r = ParaDecrypt(c_j, \mathcal{SK})$;

    end

    A_k updates its local deep learning model using the updated parameters $\widetilde{\mathbf{w}}^r = \{\widetilde{w}_{k,j}^r | j \in \mathcal{T}\}$;

  end

  $r \leftarrow r + 1$.

end

return The comprehensive deep learning model with parameters $\mathbf{w}^R$.

Figure 2

4 Results & Discussion

This part shows a lot of experiments to see how well our suggested system works. First, we provide the experimental settings, which include the ambient configuration, data resource classification and segmentation, baseline analyses, and performance metrics. We next run a number of tests to see how well our suggested IDS model works compared to other cutting-edge research, such as those by Schneble [26], Nguyen [21], and Chen [27], all inside our constructed FL Framework. Additionally, we assess the effectiveness of the generated IDS model against the local IDS models developed by each industrial agent, as well as the best IDS model formulated by a central entity employing all available data resources.

Table I shows the numerical results with R values of 2, 4, 6, 8, and 10, respectively. In every way, the proposed IDS system is much better than previous state-of-the-art research. As the number of communication rounds R goes up from 1 to 10, the effectiveness of each IDS model usually goes up as well. When R reaches a certain level, it becomes stable. For K = 3, we get an accuracy of 99.20%.

1) Setting up the environment: The Keras API runs the CNN- model that was built, and the lightweight Python Framework Flask is used to build the FL Framework. 2

2) Baseline Studies: In this research, we assess the Schneble et al. [26] proposed medical Cybernetic physical Framework. Nguyen et al. [21], employing a three-hidden-layer architecture. Chen et al. [27]

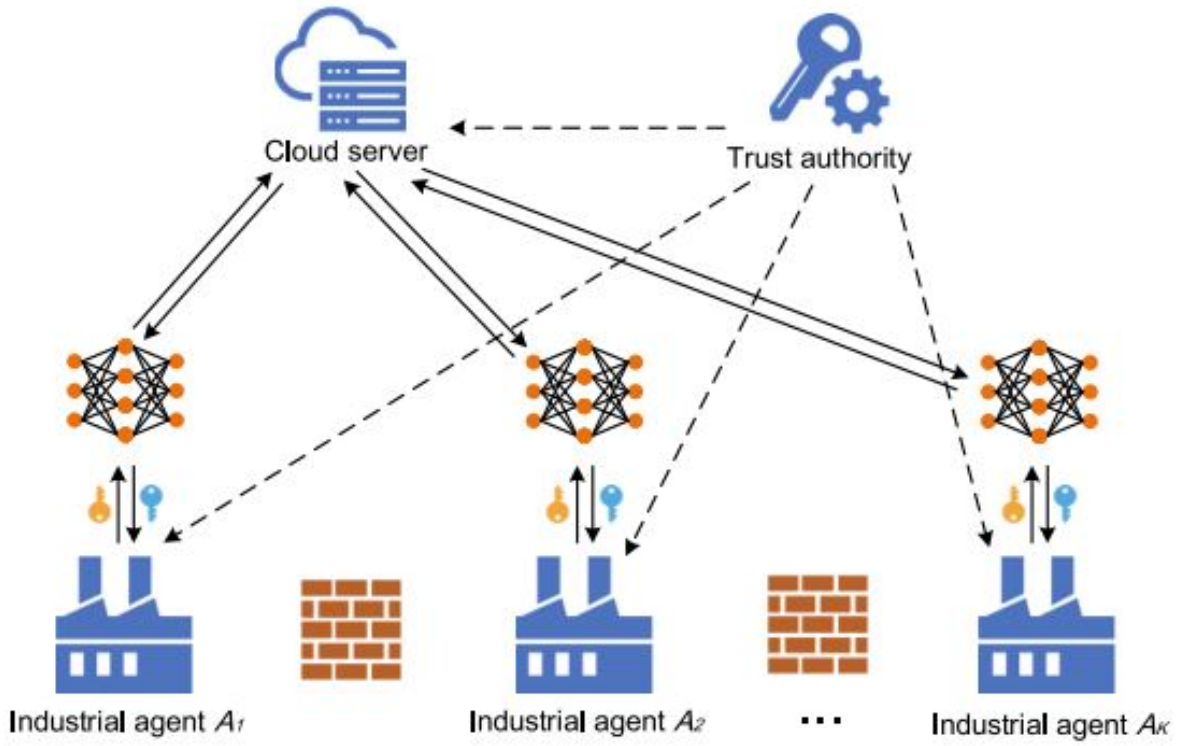

Figure 3: System Architecure

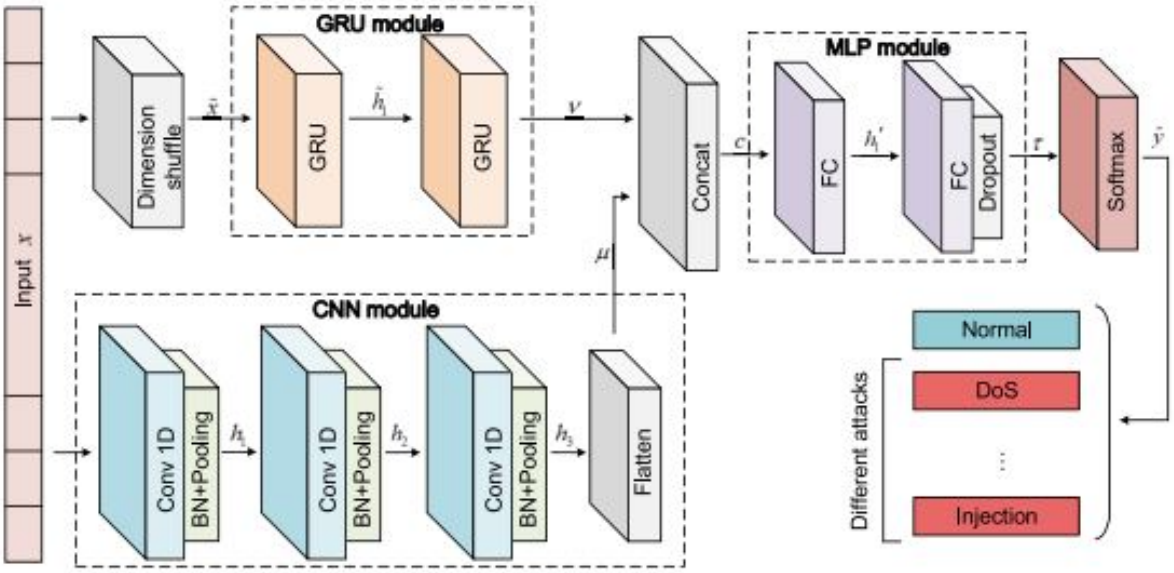

Figure 4: Architecture of designed CNN- model

also used a CNN-based federated architecture for data classification. This design has two convolutional layers, two max-pooling layers, two fully connected layers, and one softmax layer. In our study, we carefully copy these DL-Deep-Learning models and test how well they operate compared to the model we made within the recommended FL Framework.

3) Performance Metrics: The effectiveness of the detection model is measured using four common metrics, which are listed below. a) Accuracy: The model's ability to forecast the right percentage. b)

Algorithm 2: Local Deep Learning Model Training

Input: $\eta, \rho_1, \rho_2, \epsilon, \mathfrak{L}, B, \mathbf{w}^{r-1}, \mathcal{A}, \mathcal{D}_k$
Output: $\mathbf{w}_k^r$
Initialization:
a). Initialize the first and second moment variables by $s = 0$ and $v = 0$, respectively;
b). Split $\mathcal{D}_k$ into batches with equal size B;
c). Set the model parameters by $\mathbf{w}_k^r \leftarrow \tilde{\mathbf{w}}^{r-1}$;
Procedure:
repeat
  for *each batch of data resource* **do**
    a). Compute the gradient by $gd \leftarrow \bigtriangledown_{\mathbf{w}_k^r} \mathfrak{L}$;
    b). Update the biased first moment estimate by $s \leftarrow \rho_1 s + (1 - \rho_1) gd$;
    c). Update the biased second moment estimate by $v \leftarrow \rho_2 v + (1 - \rho_2) gd^2$;
    d). Compute the bias–corrected first moment estimate by $\hat{s} \leftarrow \frac{s}{1-\rho_1^r}$;
    e). Compute the bias–corrected second moment estimate by $\hat{v} \leftarrow \frac{v}{1-\rho_2^r}$;
    f). Update the model parameters by $\mathbf{w}_k^r \leftarrow \mathbf{w}_k^r - \eta \frac{\hat{s}}{\sqrt{\hat{v}}+\epsilon}$;
  end
until The loss function $\mathfrak{L}$ converages;
return $\mathbf{w}_k^r$

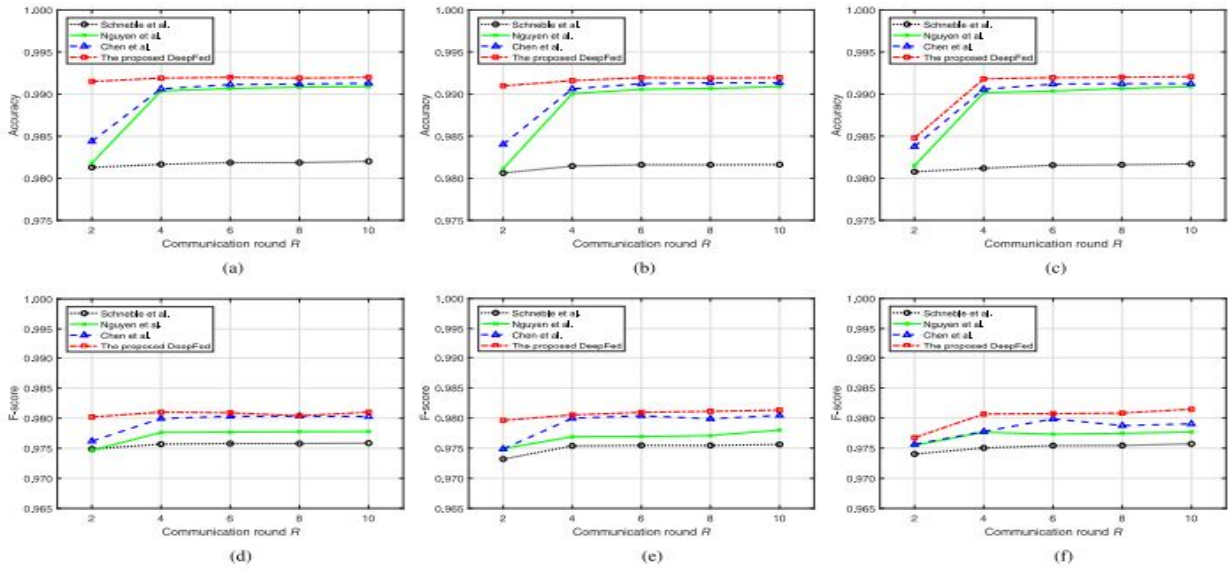

Figure 5: Comparing the accuracy and F-score of the IDS model with different rounds of communication

Table 2: Quantitative Outcomes of IDS Models with Diverse Communication Iterations

K (Rounds)	[26]	[21]	Proposed
2	0.912	0.925	0.941
4	0.918	0.931	0.949
6	0.927	0.942	0.956
8	0.935	0.947	0.962
10	0.942	0.951	0.967
5	0.948	0.957	0.972
7	0.953	0.962	0.976
9	0.961	0.968	0.981

Accuracy: The number of cyberattacks that are actually cyberattacks compared to the number of times they are categorized as such. c) Recall: The number of times that particular types of cyberattacks are correctly identified compared to the overall number of times they happen. d) F-score: The average of accuracy and recall, with some weight given to each. It is vital to remember that macro-averaged

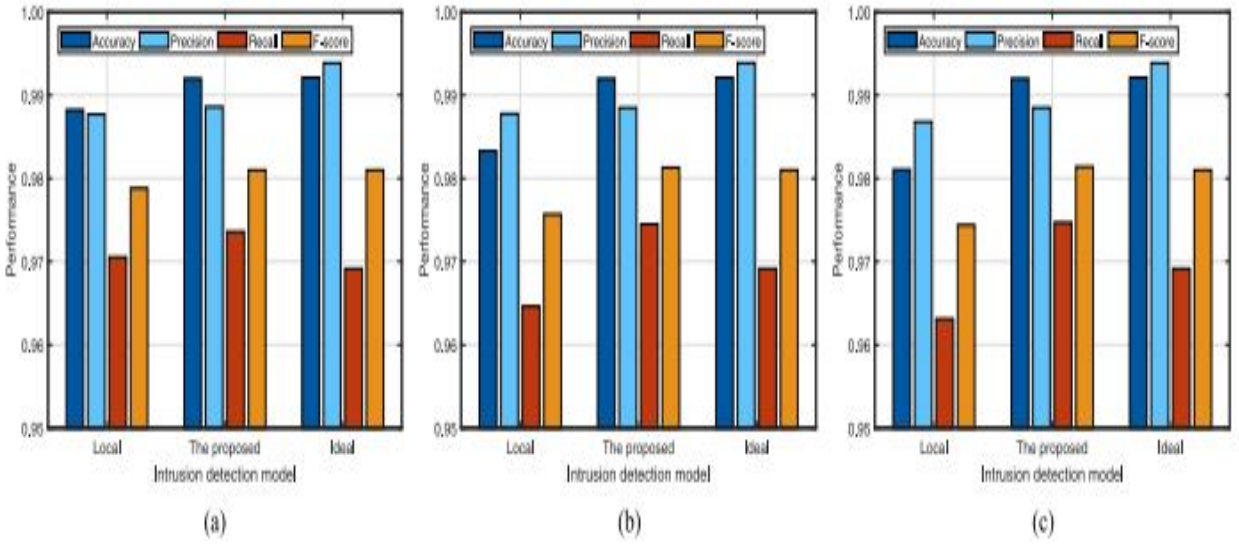

Figure 6: Comparative analysis of the local, optimal, and suggested IDS models

findings are used to fully evaluate how well all of the tested IDS systems work.

We also run tests to see how well each locally produced IDS model works with limited data resources. Figure 5 shows the numbers for all four metrics, for different values of K. All local IDS techniques perform poorly when compared to the recommended method. We also want to point out that the proposed model works well compared to the best model. since of this, it's crucial to point out that the recommended approach would be good for all industrial CPS owners since it works better at finding intrusions and keeping their data private. We also look at how well the local, ideal, and our recommended approach can find different types of cybersecurity concerns that target industrial (CPS). Table II shows the numbers, with K = 5 as a reference. The proposed IDS model exhibits enhanced performance in accuracy, recall, and F-score for detecting diverse cybersecurity concerns to industrial (CPS), relative to a local model, and shows performance closely aligned with that of an optimal model.

5 Conclusion

This study introduces a federated-DL system, designed to identify and mitigate cyber hazards to industrial Cybernetic physical Framework . At first, we set up a new FL Framework for different industrial Cybernetic physical Framework . This made it possible to build a complete IDS model together while keeping privacy safe. We have created a new CNN–based IDS model that makes it easier to find different types of cyber attacks that target industrial Cybernetic physical Framework. A secure communication protocol utilizing Paillier encryption was established for the FL Framework, effectively protecting the secrecy during the training process. testing on a real-world to determine the efficiency of the suggested system, highlighting its benefits over current leading methodologies. The suggested system creates a federated IDS model mainly for Cybernetic physical Framework that work in the same field. Future study will concentrate on resolving cybersecurity challenges through the integration of data resources from various industrial Cybernetic physical Framework.

References

[1] C. Lu, et al. (2016). Real-time wireless sensor-actuator networks for industrial Cybernetic physical Framework. *Proceedings of the IEEE*, 104(5), 1013–1024.

[2] Y. Lu, X. Huang, Y. Dai, S. Maharjan, & Y. Zhang. (2020). Blockchain and FL for privacy-preserved data sharing in industrial IoT. *IEEE Transactions on Industrial Informatics*, 16(6), 4177–4186.

[3] B. Li, R. Lu, W. Wang, & K.-K. R. Choo. (2017). Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. *Journal of Parallel and Distributed Computing*, 103, 32–41.

[4] C. Chen, J. Yan, N. Lu, Y. Wang, X. Yang, & X. Guan. (2015). Ubiquitous monitoring for industrial Cybernetic physical Framework over relay-assisted wireless sensor networks. *IEEE Transactions on Emerging Topics in Computing*, 3(3), 352–362.

[5] H. Bao, R. Lu, B. Li, & R. Deng. (2016). BLITHE: Behavior rule based insider threat detection for smart grid. *IEEE Internet of Things Journal*, 3(2), 190–205.

[6] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, & S. Liu. (2019). Efficient and privacy-enhanced FL for industrial artificial intelligence. *IEEE Transactions on Industrial Informatics*, 16(10), 6532–6542.

[7] B. Li, R. Lu, W. Wang, & K. R. Choo. (2016). DDOA: A Dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system. *IEEE Transactions on Information Forensics and Security*, 11(11), 2415–2425.

[8] K. Zetter. (2016). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired*, March. [Online]. Available: `https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/`

[9] N. Falliere, L. O. Murchu, & E. Chien. (2011). W32. Stuxnet dossier. *Symantec Corp.*, White Paper, 5, February.

[10] Z. Bederna & T. Szadeczky. (2020). Cyber espionage through botnets. *Security Journal*, 33(1), 43–62.

[11] N. Sayfayn & S. Madnick. (2017). Cybersafety analysis of the Maroochy Shire sewage spill. *MIT Sloan School, Working Paper CISL 2017-09*, 9, May.

[12] J. Felker & M. Edwards. (2017). ICS-CERT Annual Assessment Report. *Industrial Control Systems Cyber Emergency Response Team*, Report S508C. [Online]. Available: `https://www.us-cert.gov/sites/default/files/Annual-Reports/FY2016-Industrial-Control-Systems-Assessment-Summary-Report-S508C.pdf`

[13] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, & A. Hahn. (2015). Guide to Industrial Control Systems (ICS) Security. *U.S. Department of Commerce*, NIST SP 800-82r2. [Online]. Available: `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf`

[14] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, & C. Zhao. (2019). Blockchain-based software-defined industrial Internet of Things: A dueling deep Q-learning approach. *IEEE Internet of Things Journal*, 6(3), 4627–4639.

[15] M. Ismail, M. F. Shaaban, M. Naidu, & E. Serpedin. (2020). DL-Deep-Learning detection of electricity theft cyber-attacks in renewable distributed generation. *IEEE Transactions on Smart Grid*, 11(4), 3428–3437.

[16] J. Yang, C. Zhou, S. Yang, H. Xu, & B. Hu. (2018). Anomaly detection based on zone partition for security protection of industrial Cybernetic physical Framework. *IEEE Transactions on Industrial Electronics*, 65(5), 4257–4267.

[17] H. Wang, J. Ruan, G. Wang, B. Zhou, Y. Liu, X. Fu, & J. Peng. (2018). DL-Deep-Learning-based interval state estimation of AC smart grids against sparse cyber attacks. *IEEE Transactions on Industrial Informatics*, 14(11), 4766–4778.

[18] H. Yang, L. Cheng, & M. C. Chuah. (2019). Deep-learning-based network IDS for SCADA systems. In *Proceedings of the IEEE Conference on Communications and Network Security*, Washington, DC, USA, June 10–12, pp. 337–343.

[19] J. Liu, W. Zhang, T. Ma, Z. Tang, Y. Xie, W. Gui, & J. P. Niyoyita. (2020). Toward security monitoring of industrial Cybernetic physical Framework via hierarchically distributed IDS. *Expert Systems with Applications*, 158, 113400–113578.

[20] D. Preuveneers, V. Rimmer, I. Tsingenopoulos, J. Spooren, W. Joosen, & E. Ilie-Zudor. (2018). Chained anomaly detection models for FL: An IDS case study. *Applied Sciences*, 8(12), 2663–2683.

[21] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, & A.-R. Sadeghi. (2019). DÏoT: A federated self-learning anomaly detection system for IoT. In *Proceedings of the IEEE International Conference on Distributed Computing Systems*, Dallas, TX, USA, July 7–10, pp. 756–767.

[22] Y. Zhao, J. Chen, D. Wu, J. Teng, & S. Yu. (2019). Multi-task network anomaly detection using FL. In *Proceedings of the 10th International Symposium on Information and Communication Technology*, Hanoi–HaLong Bay, Vietnam, Dec. 4–6, pp. 273–279.

[23] Y. Chen, J. Zhang, & C. K. Yeo. (2019). Network anomaly detection using federated deep autoencoding Gaussian mixture model. In *Proceedings of the International Conference on Machine Learning and Networking*, Paris, France, Dec. 3–5, pp. 1–14.

[24] M. J. Dworkin, et al. (2001). Advanced Encryption Standard (AES). *NIST FIPS Publication 197*. [Online]. Available: `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf`

[25] P. Paillier. (1999). Public-key cryptosystems based on composite degree residuosity classes. In *Proceedings of the International Conference on Theory and Application of Cryptographic Techniques*, Cologne, Germany, Apr. 26–30, pp. 223–238.

[26] W. Schneble & G. Thamilarasu. (2019). Attack detection using FL in medical Cybernetic physical Framework. In *Proceedings of the International Conference on Computer Communication and Networks*, Valencia, Spain, Jul. 29–Aug. 1.

[27] Y. Chen, X. Qin, J. Wang, C. Yu, & W. Gao. (2020). FedHealth: A federated transfer learning Framework for wearable healthcare. *IEEE Intelligent Systems*, 35(4), 83–93.

[28] T. Morris & W. Gao. (2014). Industrial control system traffic data sets for IDS research. In *Proceedings of the International Conference on Critical Infrastructure Protection*, Arlington, TX, USA, Mar. 17–19, pp. 65–78.

[29] Graves, A. Long short-term memory. *Supervised Sequence Labelling with Recurrent Neural Networks*, Springer, 2012, 385, 37–45.

[30] Zhu, X.; Sobihani, P.; Guo, H. Long short-term memory over recursive structures. In *Proceedings of the International Conference on Machine Learning*, Miami, FL, USA, 9–11 December 2015; pp. 1604–1612.

[31] Wan, L.; Zeiler, M.; Zhang, S.; Le Cun, Y.; Fergus, R. Regularization of neural networks using dropconnect. In *Proceedings of the International Conference on Machine Learning*, Atlanta, GA, USA, 16–21 June 2013; pp. 1058–1066.

[32] Hinton, G.E.; Srivastava, N.; Krizhevsky, A.; Sutskever, I.; Salakhutdinov, R.R. Improving neural networks by preventing co-adaptation of feature detectors. *arXiv preprint* arXiv:1207.0580, 2012.

[33] Jeatrakul, P.; Wong, K.W.; Fung, C.C. Classification of imbalanced data by combining the complementary neural network and SMOTE algorithm. In *Proceedings of the International Conference on Neural Information Processing*, Sydney, Australia, 22–25 November 2010; pp. 152–159.

[34] Goodfellow, I.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D.; Ozair, S.; Courville, A.; Bengio, Y. Generative adversarial networks. *Communications of the ACM*, 2020, 63, 139–144. [CrossRef]

[35] Anani, W.; Samarabandu, J. Comparison of recurrent neural network algorithms for intrusion detection based on predicting packet sequences. In *Proceedings of the 2018 IEEE Canadian Conference on Electrical & Computer Engineering*, Quebec, QC, Canada, 13–16 May 2018; pp. 1–4.

[36] Farahnakian, F.; Heikkonen, J. A deep auto-encoder based approach for intrusion detection system. In *Proceedings of the 20th International Conference on Advanced Communication Technology*, Chuncheon, Republic of Korea, 11–14 February 2018; pp. 178–183.

[37] Alom, M.Z.; Bontupalli, V.; Taha, T.M. Intrusion detection using deep belief networks. In *Proceedings of the 2015 National Aerospace and Electronics Conference*, Dayton, OH, USA, 15–19 June 2015; pp. 339–344.

[38] Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In *Proceedings of the IEEE International Conference on Computational Intelligence for Security & Defense Applications*, Ottawa, IL, USA, 8–10 July 2009; pp. 1–6.

[39] Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *Proceedings of the Military Communications and Information Systems Conference*, Cracow, Poland, 18–19 May 2015; pp. 1–6.