
# Smart Sensor Networks for Industrial IoT Applications

**Nihal N. Mostafa[1,*], Esmeralda Kazia[2]**

[1]Faculty of Computers and Informatics, Zagazig University, Zagazig, Sharqiyah, 44519, Egypt,
[2]Faculty of Applied Sciences and Creative Industries,Tirana ,Albania,1001
Emails: nihal.nabil@fci.zu.edu.eg; e.kazia@umb.edu.al

**Abstract**

Smart Sensor Networks (SSNs) are an indispensable part of the Industrial Internet of Things (IIoT), which seeks to improve efficiency, productivity, and safety in different industrial applications. SSNs consist of a large number of sensors, regularly deployed in a wireless ad-hoc network, which communicates with each other and with other devices, such as gateways and servers. Nevertheless, the building of SSNs in IIoT environments encounters many challenges, such as trust management, data reliability, privacy, and security. These challenges necessitate proposing novel solutions and protocols, to provide a reliable, secure, and efficient SSN. To this end, this study presents a novel DL system that can effectively discriminate between normal traffics and malicious traffic in SSNs. A convolutional feature extractor is developed to learn important discriminative features necessary for the early detection of security threats in SSNs. Then, an improved LSTM (ILSTM) is presented to model the temporal dynamics of the SSNs flows, which helps model long interdependency between traffic samples. A focal loss function is applied to deal with the imbalance between class samples. Experimental analysis is performed on an open-source SSN security dataset, named WSN-DS, the findings demonstrated the competitive advantages of our system over the prevailing solutions.

**Keywords:** Industrial Internet of Things ( IIoT); Smart Sensors; Wireless Sensor Networks; Intelligent Models

## 1. Introduction:

The Industrial Internet of Things (IIoT) is a rapidly growing field that aims to enhance industrial processes and systems through the integration of connected devices, sensors, and machines. The IIoT provides several benefits, such as increased efficiency, productivity, and safety, as well as improved product quality and reduced operational costs. However, the implementation of the IIoT also poses several challenges that need to be addressed. One of the main challenges is the integration of legacy systems, which often use proprietary protocols and technologies, with new IoT devices and systems [1-5]. This requires the development of new standards and protocols to ensure interoperability and seamless integration. Another challenge is the management of large amounts of data generated by IIoT devices and systems. This data needs to be processed, analyzed, and acted upon in real-time to provide actionable insights and enable timely decision-making. This requires the development of new data management and analytics tools and techniques, as well as the integration of existing ones. In addition, the security of IIoT systems and devices is a critical challenge that needs to be addressed. IIoT devices are often deployed in harsh and remote environments, making them vulnerable to cyber-attacks and unauthorized access. This requires the development of new security technologies and protocols to ensure the confidentiality, integrity, and availability of IIoT systems and data. Further, the trust management of IIoT devices and systems is a key challenge, particularly for those deployed in data-sensitive applications, in which devices usually host critical information that needs a high level of trust to deal with it [5-8].

Smart Sensor Networks (SSNs) are a key component of the Industrial Internet of Things (IIoT) and play a crucial role in enabling real-time monitoring, control, and optimization of industrial processes and systems. SSNs are composed of a large number of sensors, often deployed in a wireless ad-hoc network, which communicates with each other and with other devices, such as gateways and servers. The deployment of SSNs in IIoT applications provides several



DOI: https://doi.org/10.54216/JISIoT.080204
Received: Decebmer 31, 2022 Accepted: February 19, 2023

benefits, including improved operational efficiency, increased productivity, enhanced product quality, and reduced maintenance costs [8-10]. SSNs enable real-time monitoring and control of industrial processes, allowing for proactive maintenance and fault diagnosis, which helps to minimize downtime and improve overall efficiency. SSNs also enable the collection of large amounts of data, which can be analyzed to provide insights into industrial processes and systems and enable optimization. However, the design and implementation of SSNs for IIoT applications pose several challenges, such as power management, network scalability, data reliability, and security. These challenges require the development of new technologies and protocols, as well as the integration of existing ones, to provide a reliable, secure, and efficient SSN [10-14].

Though the promising role of SSNs in IIoT applications, they still suffer from several security risks, resulting from the vulnerabilities of these networks to cyber-attacks, which can take various forms, such as denial of service attacks, data breaches, and malware infections. Denial of service attacks can disrupt the functioning of the SSN by overwhelming it with traffic, while data breaches can compromise the confidentiality and integrity of the data transmitted by the SSN. Malware infections can also compromise the security of the SSN by allowing attackers to gain unauthorized access to the network and its devices [14-17]. To mitigate these risks, it is essential to implement robust security measures to protect SSNs from cyber-attacks. This includes the use of encryption to protect data transmitted over the network, the implementation of access control mechanisms to prevent unauthorized access to the network and its devices, and the use of intrusion detection and prevention systems to detect and prevent cyber-attacks. In addition, it is crucial to ensure that SSN devices are regularly updated and patched to address security vulnerabilities and to train employees on cybersecurity best practices to prevent human error and ensure compliance with security policies [18-20].

Machine learning (ML) is a promising research direction for detecting and mitigating cyber-attacks on SSNs operating, in which ML algorithms are applied to train on large datasets of network traffic to identify patterns and anomalies that may indicate the presence of a cyber-attack [19]. There are several ML techniques that can be used for cyber-attack detection in SSNs. One approach is supervised learning, where ML algorithms are trained on labeled datasets of network traffic to learn to classify traffic as either normal or malicious. Another approach is unsupervised learning, where ML algorithms are trained on unlabeled datasets of network traffic to identify patterns and anomalies that may indicate the presence of a cyber-attack [20].

Deep learning, a subset of ML that involves the use of artificial neural networks, has also been used for cyber-attack detection in SSNs. Deep learning algorithms can learn complex patterns and features in network traffic, making them particularly effective for detecting advanced cyber-attacks. However, the effectiveness of ML algorithms for cyber-attack detection in SSNs depends on the quality and diversity of the training datasets, as well as the accuracy of the algorithms. It is essential to continually update and improve the ML models to ensure that they can detect the latest cyber threats. In addition, ML algorithms can be used in conjunction with other security measures, such as access control mechanisms and intrusion detection and prevention systems, to provide a comprehensive and robust security solution for SSNs in IIoT applications.

In response to the security challenges in SSNs, this work proposes a deep learning system to detect security attacks based on spatial temporal representations of traffic flows. An improved feature extractor is designed with an intelligent convolutional extractor, where the long-term dependencies are captured with improved long-sort term memory (ILSTM), with improved gating.

The remaining of this work is structured as follows:

- Section 2 presents an analytical review of the state-of-the-art related studies.
- Section 3 provides a detailed methodology of the proposed system for securing SSNs in IIoT scenario.
- Section 4 debates the performed experiments and the corresponding results.
- Section 5 concludes our contributions and findings.

## 2. Related Work

The use of SSNs is becoming increasingly popular in IIoT applications, as it allows for real-time monitoring, data analysis, and optimization of industrial processes. There have been several research studies in this era, and some of the prominent ones are discussed in the following. In [1], the authors presented a stochastic system mobile converge



DOI: https://doi.org/10.54216/JISIoT.080204
Received: Decebmer 31, 2022 Accepted: February 19, 2023

cast and evaluated to learn path period times, by bearing in mind parameters containing network replicas, SSN scope, and agility decorations of network essentials. In [2], the authors presented a secure navigation algorithm for small aerial robots to use within the IIoT of factories, which tried to tackle the inability of micro aerial robots to carry the bulky obstacle detection sensors necessary for local navigation. Their proposed algorithm was guided by SSM comprised of a three-dimensional range finder to prevent colliding with static and moving obstacles in an indoor industrial setting. The micro flying robot needs only a route tracking controller, and it didn't do any complicated calculations. In [3], the authors presented a tentative study of discriminatory supportive communicating protocols that are executed in off-the-shelf IEEE 802.15.4-compatible campaigns and assessed in an industrial SSN system. They defined three applied relay modernization systems to activate relay selection namely episodic, adaptive; and reactive relay assortments. In [4], the authors developed a routing scheme for enhancing throughput and reductions of end-to-end latency in industrial cognitive radio sensor networks (ICRSNs) according to ISA100.11a, whereby the throughput was downgraded through interference from primary SSNs. Their proposed scheme focused on big-scale SSNs, where the data were usually promoted through diverse clusters on the route to the sink. By approximating the supreme route's throughput, the data could be promoted over the most ideal route. In [5], the authors presented an energy-aware routing protocol, called Energy-Aware Reliable and Quick (EARQ) routing, for industrial SSNs to enhance the reliability and real-time performance of communication while minimizing energy consumption. EARQ utilized a cross-layer approach to achieve energy efficiency, reliability, and real-time performance. It considered the energy levels of the sensor nodes, the transmission rates, and the routing paths.

In [6], the authors developed a Q-learning dependable routing with a weighted agent tactic, in which an agent was enabled to adapt to the influences of a cutting-edge graph-routing procedure. The statuses of the agent were signified via a group of scores, and the actions transform the scores throughout the tasks of SSN. These methods assigned the rewards to the agent once the latency of SSN diminutions or the predictable network period upsurges. In [7], the authors presented a clock skew estimation technique for synchronizing nodes in industrial SSN without using timestamps, which was demonstrated problematic because of the limited bandwidth and energy resources of these networks. They developed a two-step strategy that applied a phase-locked loop (PLL) to estimate the frequency difference to estimate the clock skew between nodes, then calculated the clock skew based on the frequency difference and the time difference between the clocks. In [8], the authors investigated the impact of eavesdropping attacks on industrial SSNs and developed a detection method based on a statistical analysis of intercept behavior. This method involved comparing the expected number of intercepted packets to the actual number of intercepted packets to determine if an eavesdropping attack was present. In [9], the authors proposed a Quality of Service (QoS) framework for completely arbitrary hybrid wired/wireless SSN, ensuring that both the latency constraint and the objective dependability of each application are met. Our system includes the first proposed reliability-based scheduling for SSNs that can meet the goal of dependability despite dynamic interference. In [10], the authors presented an obstacle-aware intelligent fault detection scheme for industrial SSNs to improve the accuracy and reliability of fault detection. Their scheme was designed as a two-stage approach, in which a support vector machine (SVM) classifier was applied to identify normal and abnormal operating conditions based on sensor data. Then, a dynamic Bayesian network (DBN) was applied to incorporate obstacle information into the fault detection process and improve the accuracy and reliability of the results. In [11], the authors studied the clock synchronization arrangements of the active node and eavesdropping node with instant clock modification. Then, they used a maximum-likelihood predictor for the clock skew and the conforming Cramer–Rao lower bounds with gaussian delays in consideration.

## 3. The proposed Smart Sensors Model for IIoT Applications

This section argues the methodology of the proposed DL system for detecting cyber-attacks on SNN in complex IIoT environments. The structural design of the proposed model is illustrated in Figure 1. As shown, the proposed system consists of three main layers namely feature extractor, temporal fusion, and classification.

To begin, feature extraction is an important step to understand and learn the important patterns in SSN data that are necessary to classify it as normal or attack. Convolutional models have shown great success in various image and signal-processing tasks. In the context of intrusion detection, convolutional models can be used to extract relevant features from the network traffic data, which can then be used to classify normal and malicious traffic. The rudimentary idea, here is to feed the network traffic, $X_0$, data as input to the convolutions which applies a series of



DOI: https://doi.org/10.54216/JISIoT.080204
Received: Decebmer 31, 2022 Accepted: February 19, 2023

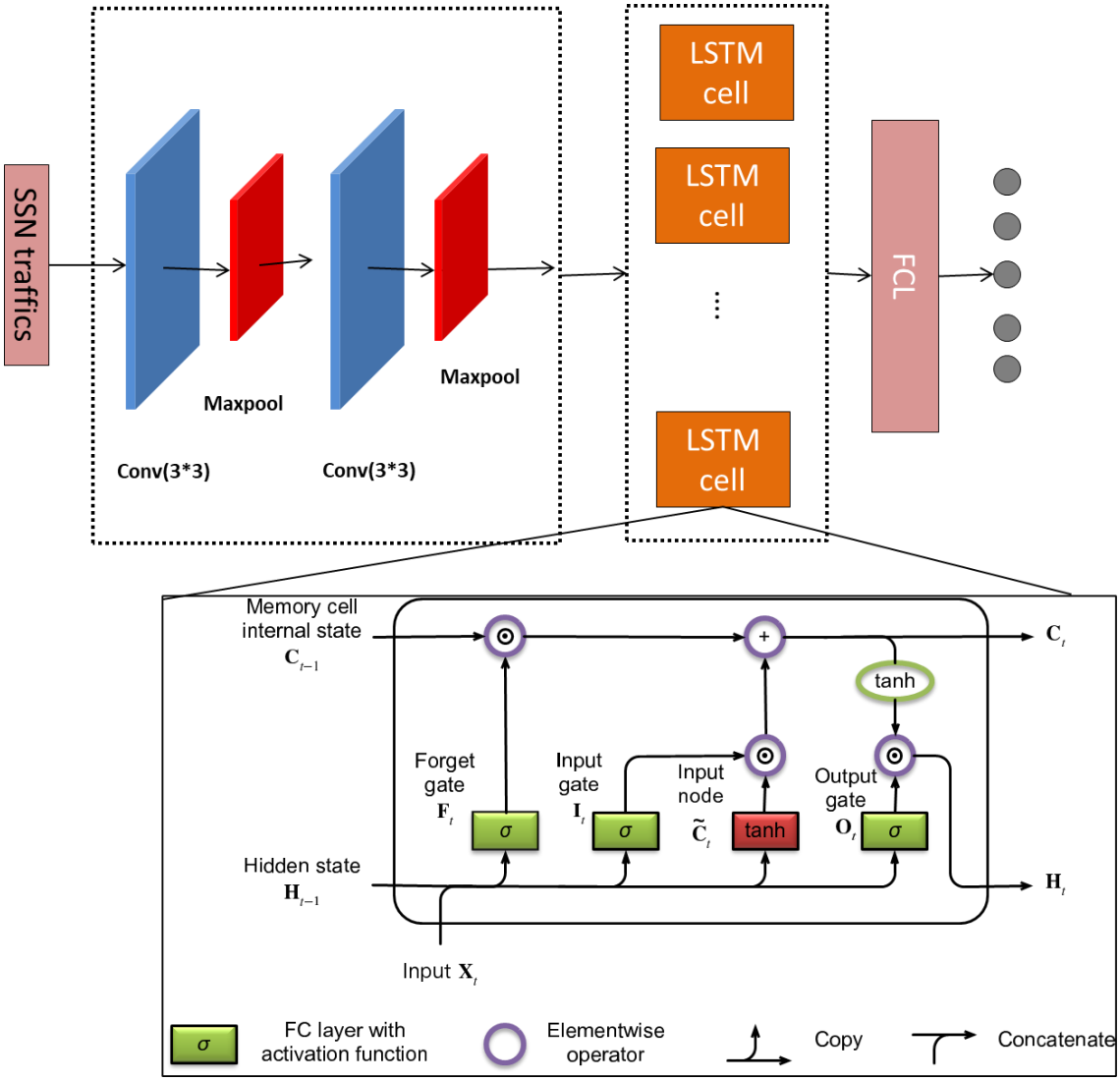


*Figure 1: visualization of the architecture of the proposed system for detecting security threats in industrial SSNs.*

convolutional filters to the data to extract features that are relevant for intrusion detection. These features are then combined using pooling layers and passed on to one or more fully connected layers for classification.
Specifically, by stacking multiple convolutional kernel $k$, with learning parameters $w_k$, and bias $b_k$, we can express the convolutional feature extraction as follows:

$$X_k = f(w_k * X_{k-1} + b_k), \quad (1)$$

The symbol $X_k$ denote the output of the $k-th$ layer. The symbol $*$ denotes convolution operation, while the $f(.)$ denote activation procedure. To accelerate the training of our model we choose the rectified linear unit (ReLU) for activating the convolutional kernels in our feature extractor. The $ReLU$ could be mathematically defined as follows:

$$ReLU(X_i) = \begin{cases} X_i & (X_i > 0) \\ 0 & (X_i \leq 0) \end{cases}, \quad (2)$$

To have perfect feature extraction, we need to keep only important features as we go deeper into the network. Pooling layers are generally used in deep networks for downsampling, reducing the spatial dimensions of the feature maps while retaining the most important information. The pooling layer operates on each feature map separately, using a sliding window to extract the maximum or average value in each window. Average pooling is a type of pooling layer, where the average value within each window is taken as the output. Max pooling is the most commonly used type of



DOI: https://doi.org/10.54216/JISIoT.080204
Received: Decebmer 31, 2022 Accepted: February 19, 2023

pooling layer. In max pooling, the maximum value within each window is selected as the output for that window. For example, a max pooling layer with a pool size of 2 and a stride of 2 would divide the feature map into non-overlapping $2 \times 2$ windows and output the maximum value within each window. Because max pooling can preserve more important information than average pooling, we decide to use it in our feature extractor. This can be calculated as follows:

$$Q_j = Max(P_j^0, P_j^1, P_j^2, P_j^3 \dots P_j^t), \quad (3)$$

where $Q_j$ signifies the outcome of the pooling area $j$, $P_j^i$ denote the $i - th$ component of the pooling area $j$

To capture the temporal dynamics, we present an improved variant of the LSTM (ILSTM) introduced after convolutional layers to enable capturing the long-term dependencies within the traffic flows of SSN. Among the existing recurrent networks, the enhanced gating of our LSTM enables removing the issues of vanishing gradients, which leads to more stabilized training. Similar to the traditional LSTM, our design of ILSTM involves a set of primary elements such as memory, a gate for input, a gate for output, and a gate for forgetting. The memory is in charge of keeping the information at the current time and the three gating mechanisms regulate the flow of information into and out of the memory. The computation of ILSTM can be expressed as follows.

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \quad (4)$$
$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \quad (5)$$
$$c_t = \tanh(W_c \cdot [h_{t-1}, x_t] + b_c) \quad (6)$$
$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \quad (7)$$
$$h_t = o_t \cdot \tanh(c_t) \quad (8)$$

By the end of the model, two linear layers are applied to calculate the final decision about the input.

The last layer is implemented using SoftMax activation to map the learned information into a probability score between 0 to 1. This can be mathematically expressed as follows:

$$\hat{y}_i = \frac{e^{\hat{y}_i}}{\sum_{k=1}^{K} e^{\hat{y}_i}} \quad (9)$$

The focal loss is used as our objective during the training, which is formulated as follows:

$$FL = -\sum_{i=1}^{M} y_i (1 - \hat{y}_i)^{\gamma} \, log(\hat{y}_i), \quad \gamma \geq 0 \quad (10)$$

where $y_i$ denote the ground-truth mask, and $\hat{y}_i$ is the systems' estimated probability for the i-th class. The $\gamma$ denotes concentrating parameter, while $(1 - \hat{y}_i)^{\gamma}$ is the regulating element.

## 4. Results and Discussion

In this section, we discuss the experimental analysis made to evaluate and understand the behavior of our model. In our experiments, we use the WSN-DS dataset [14] to train and evaluate the proposed system. the dataset contains a total of 374661 belonging to 5 distinct classes namely normal, Blackhole, Grayhole, Flooding, and Scheduling attacks. The class distribution of the WSN-DS dataset is reported in Table 1. it is worth noting that the data suffer from high-class imbalance.

Table 1. Summary statistic of WSN-DS dataset

| CLASS | #SAMPLES |
|---|---|
| ▪ NORMAL | 340066 |
| ▪ GRAYHOLE | 14596 |



DOI: https://doi.org/10.54216/JISIoT.080204
Received: Decebmer 31, 2022 Accepted: February 19, 2023

| | |
|---|---|
| ▪ **BLACKHOLE** | **10049** |
| ▪ **TDMA** | **6638** |
| ▪ **FLOODING** | **3312** |

A confusion matrix is a popular performance indicator that is used in this work to evaluate the performance of our system. As shown in Figure 2, the confusion matrix is a table composed of four values: true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN), which summarizes the number of correct and incorrect predictions made by a model for each class**.** From these values, several metrics can be calculated to evaluate the performance of the model, including accuracy, precision, recall (also known as sensitivity), and specificity. It is notable that the proposed system achieved 99% accuracy in detecting normal and TDMA traffics, and detecting the grayhole, blackhole, and flooding with 90%, 82%, and 89% accuracy. This high variability in the detection performance of each class can be attributed to the high-class imbalance in the training data.

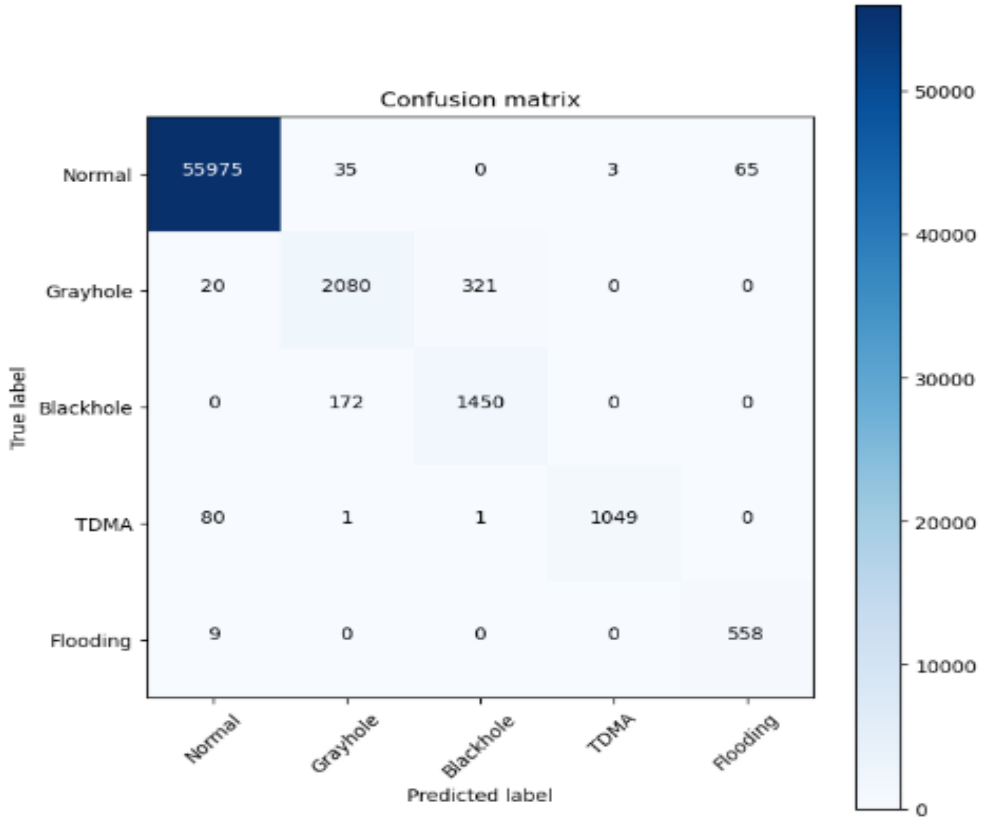


*Figure 2: confusion matrix of the proposed DL system*

More, the classification ability of the proposed model can be further demonstrated by visualizing the training curves for the proposed model by plotting the false positive rate against true positive counterparts. Figure 3 shows the ROC curves for the prediction of our system on different classes, and also displays the area under the curve (AUC) associated with each class. It is worth noting that the AUC value reaches its highest with 99% at normal and TDMA classes, which conforms to our findings from the confusion matrix. In general terms, the proposed system can resist the problem of class imbalance and achieve robust detection performance.



DOI: https://doi.org/10.54216/JISIoT.080204
Received: Decebmer 31, 2022 Accepted: February 19, 2023

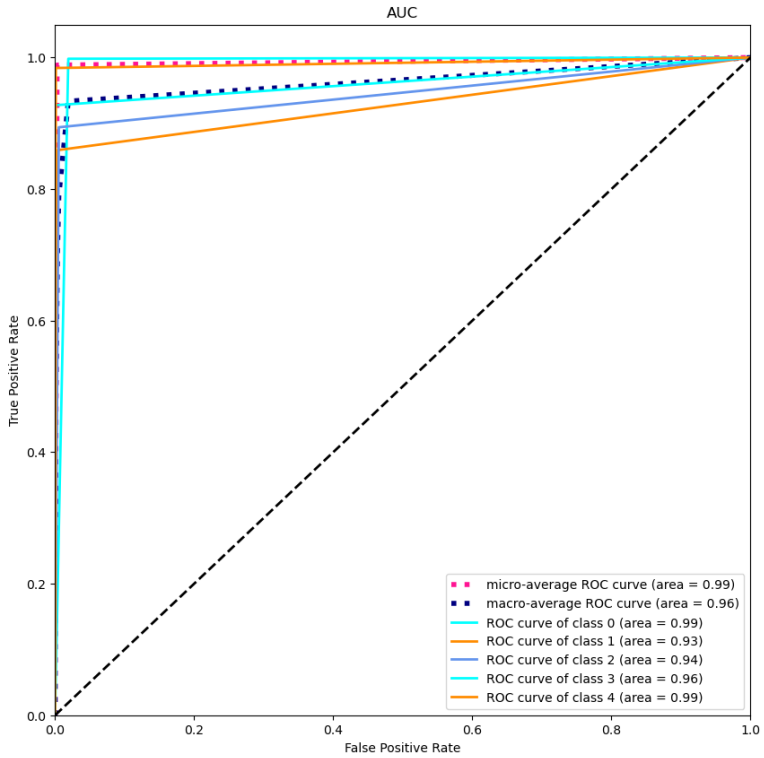


*Figure 3: visualization of the ROCAUC curves of the proposed model. Normal=class 0, blackhole=class 1, Grayhole=class 2, Flooding=class 4, Scheduling=class 3.*

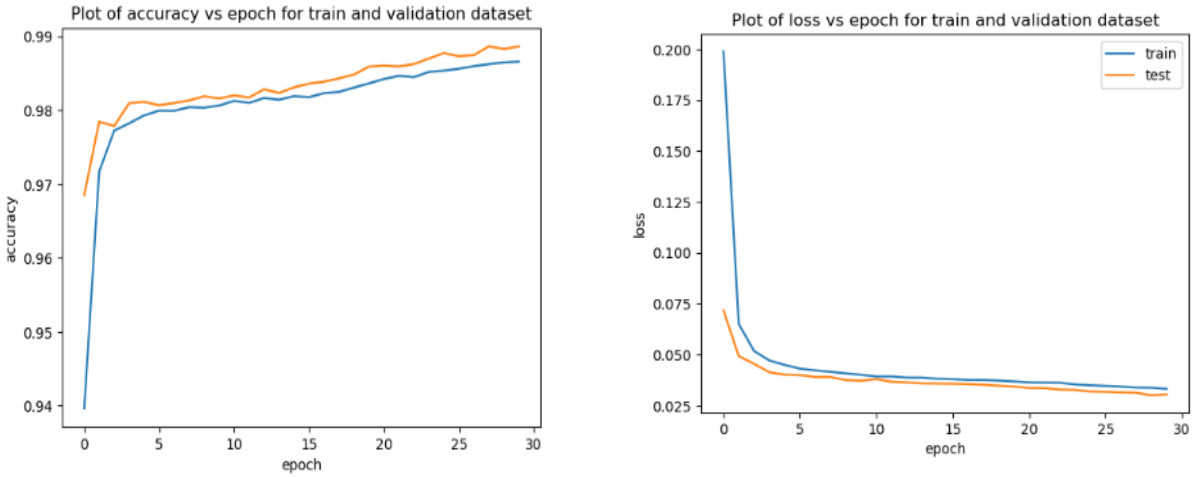


*Figure 4: visualization of the training accuracy (left) and training loss curves (right) for the proposed DL system.*

Beyond and above, the learning curves are an important graphical analysis tool that shows the behavior of a model during the learning process and identifies potential issues such as overfitting or underfitting. Figure 4 shows the learning curves plot two measures over the course of training: the training error (or loss) and the validation error. The training error measures how well the model fits the training data, while the validation error measures how well the model generalizes to new, unseen data. It is notable that the proposed model shows stable and consistent learning



DOI: https://doi.org/10.54216/JISIoT.080204
Received: Decebmer 31, 2022 Accepted: February 19, 2023

behavior during the training phase. Moreover, we could also observe that our model can converge rapidly after 30 epochs.

## 5. Conclusion

This study introduces a new deep learning system that can effectively detect and identify cyber-attacks threatening the security of SSNs in IIoT environments. The traffic flows of SNNs are fed into our system, which is composed of recurrent and convolutional layers that enable the detection of temporal and positional patterns of attacks. This building allows the network to extract relevant features from the input data while preserving the temporal dynamics. an intelligent focal loss function is used in our system to tackle class imbalance problems. Experimental findings on the WSN-DS dataset show that the proposed system is very competitive and can perfectly detect security threats against SSNs in the context of industrial applications.

## References

**[1]** Z. Qin, D. Wu, Z. Xiao, B. Fu, and Z. Qin, "Modeling and Analysis of Data Aggregation From Convergecast in Mobile Sensor Networks for Industrial IoT," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4457-4467, Oct. 2018, doi: 10.1109/TII.2018.2846687.

**[2]** H. Li and A. V. Savkin, "Wireless Sensor Network Based Navigation of Micro Flying Robots in the Industrial Internet of Things," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3524-3533, Aug. 2018, doi: 10.1109/TII.2018.2825225.

**[3]** N. Marchenko, T. Andre, G. Brandner, W. Masood and C. Bettstetter, "An Experimental Study of Selective Cooperative Relaying in Industrial Wireless Sensor Networks," in *IEEE Transactions on Industrial Informatics*, vol. 10, no. 3, pp. 1806-1816, Aug. 2014, doi: 10.1109/TII.2014.2327915.

**[4]** P. T. A. Quang and D. -S. Kim, "Throughput-Aware Routing for Industrial Sensor Networks: Application to ISA100.11a," in *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 351-363, Feb. 2014, doi: 10.1109/TII.2013.2255617

**[5]** J. Heo, J. Hong and Y. Cho, "EARQ: Energy Aware Routing for Real-Time and Reliable Communication in Wireless Industrial Sensor Networks," in *IEEE Transactions on Industrial Informatics*, vol. 5, no. 1, pp. 3-11, Feb. 2009, doi: 10.1109/TII.2008.2011052.

**[6]** G. Künzel, L. S. Indrusiak and C. E. Pereira, "Latency and Lifetime Enhancements in Industrial Wireless Sensor Networks: A Q-Learning Approach for Graph Routing," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5617-5625, Aug. 2020, doi: 10.1109/TII.2019.2941771.

**[7]** H. Wang, F. Yu, M. Li and Y. Zhong, "Clock Skew Estimation for Timestamp-Free Synchronization in Industrial Wireless Sensor Networks," in *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 90-99, Jan. 2021, doi: 10.1109/TII.2020.2975289.

**[8]** Y. Zou and G. Wang, "Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack," in *IEEE Transactions on Industrial Informatics*, vol. 12, no. 2, pp. 780-787, April 2016, doi: 10.1109/TII.2015.2399691.

**[9]** S. Zoppi, A. Van Bemten, H. M. Gürsu, M. Vilgelm, J. Guck and W. Kellerer, "Achieving Hybrid Wired/Wireless Industrial Networks With WDetServ: Reliability-Based Scheduling for Delay Guarantees," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 2307-2319, May 2018, doi: 10.1109/TII.2018.2803122.

**[10]** G. Kaur, P. Chanak and M. Bhattacharya, "Obstacle-Aware Intelligent Fault Detection Scheme for Industrial Wireless Sensor Networks," in *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 6876-6886, Oct. 2022, doi: 10.1109/TII.2021.3133347.

**[11]** H. Wang, L. Shao, M. Li, B. Wang and P. Wang, "Estimation of Clock Skew for Time Synchronization Based on Two-Way Message Exchange Mechanism in Industrial Wireless Sensor Networks," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4755-4765, Nov. 2018, doi: 10.1109/TII.2018.2799595.

**[12]** Osama Maher , Elena Sitnikova, A Trustworthy Learning Technique for Securing Industrial Internet of Things Systems, Journal of Intelligent Systems and Internet of Things, Vol. 5, No. 1, 2021 : 33-48 doi : https://doi.org/10.54216/JISIoT.050104



DOI: https://doi.org/10.54216/JISIoT.080204
Received: Decebmer 31, 2022 Accepted: February 19, 2023

**[13]** M. Magno, D. Boyle, D. Brunelli, E. Popovici and L. Benini, "Ensuring Survivability of Resource-Intensive Sensor Networks Through Ultra-Low Power Overlays," in *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 946-956, May 2014, doi: 10.1109/TII.2013.2295198.

**[14]** Almomani, I., Al-Kasasbeh, B. and Al-Akhras, M., 2016. WSN-DS: A dataset for intrusion detection systems in wireless sensor networks. *Journal of Sensors*, *2016*.

**[15]** S. Gupta, A. K. Sahoo and U. K. Sahoo, "Wireless Sensor Network-Based Distributed Approach to Identify Spatio-Temporal Volterra Model for Industrial Distributed Parameter Systems," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7671-7681, Dec. 2020, doi: 10.1109/TII.2020.3004159.

**[16]** Ahmed Abdelmonem , Shimaa S. Mohamed, Internet of Things risks, benefits, challenges in industrial application: Survey, American Journal of Business and Operations Research, Vol. 8 , No. 1, 2022 : 47-59 doi: https://doi.org/10.54216/AJBOR.080105

**[17]** N. T. Tuan, D. -S. Kim and J. -M. Lee, "On the Performance of Cooperative Transmission Schemes in Industrial Wireless Sensor Networks," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4007-4018, Sept. 2018, doi: 10.1109/TII.2018.2846671.

**[18]** Lobna Osman, Multi-criteria Decision Making Model for Industrial Arc Welding Robot, International Journal of Wireless and Ad Hoc Communication, Vol. 4 , No. 1 , (2022) : 19-30 doi: https://doi.org/10.54216/IJWAC.040102

**[19]** P. Gope, A. K. Das, N. Kumar and Y. Cheng, "Lightweight and Physically Secure Anonymous Mutual Authentication Protocol for Real-Time Data Access in Industrial Wireless Sensor Networks," in *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 4957-4968, Sept. 2019, doi: 10.1109/TII.2019.2895030.

**[20]** G. Bloom, G. Cena, I. C. Bertolotti, T. Hu, N. Navet and A. Valenzano, "Event Notification in CAN-Based Sensor Networks," in *IEEE Transactions on Industrial Informatics*, vol. 15, no. 10, pp. 5613-5625, Oct. 2019, doi: 10.1109/TII.2019.2904082.



DOI: https://doi.org/10.54216/JISIoT.080204
Received: Decebmer 31, 2022 Accepted: February 19, 2023