*Salud, Ciencia y Tecnología - Serie de Conferencias*. 2024; 3:934
doi: 10.56294/sctconf2024934

**Category: STEM (Science, Technology, Engineering and Mathematics)**

**ORIGINAL**

# Enhancing Industrial Security with IoT-based Passive Intrusion Detection and Segmentation

## Mejora de la seguridad industrial con segmentación y detección pasiva de intrusiones basada en IoT

Arunkumar S[1], Gowtham M.S[2], Revathi N[3], Krishnaprasath V.T[4]

[1]Department of EEE, Nehru Institute of Engineering and Technology, Nehru gardens, Thirumalayampalayam, Coimbatore, Tamilnadu, India.
[2]Department of Electronics and Communication Engineering, Karpagam Institute of Technology, Coimbatore, Tamilnadu, India.
[3]Department of ECE, Nehru Institute of Engineering and Technology, Coimbatore, Tamilnadu, India.
[4]Department of Artificial Intelligence and Data Science, Nehru Institute of Engineering and Technology, Coimbatore, Tamilnadu, India.

**Cite as:** Arunkumar S, Gowtham M, Revathi N, Krishnaprasath V. Enhancing industrial security with IoT-based passive intrusion detection and segmentation. Salud, Ciencia y Tecnología - Serie de Conferencias. 2024; 3:934. https://doi.org/10.56294/sctconf2024934

**Submitted:** 10-02-2024 **Revised:** 01-05-2024 **Accepted:** 19-06-2024 **Published:** 20-06-2024

**Editor:** Dr. William Castillo-González

## ABSTRACT

**Introduction:** passive intrusion detection in industrial environments can be challenging, especially when the area being monitored is vast. However, with the advent of IoT technology, it is possible to deploy sensors and devices that can help with mass segmentation of passive intrusion. Hence, this approach deploys ML (Machine Learning) algorithm as improvised (Convolutional Neural Network) CNN support for identifying and avoid illegal access to critical areas in real time, ultimately improving security and safety in industrial environments.
**Methods:** in turn the proposed algorithm can detect patterns and anomalies that could indicate a passive intrusion. In order to discover the patterns and connections between the various sensor data points, DL (Deep Learning) techniques like CNNs, Recurrent Neural Networks (RNNs), and Autoencoders (AE) may be trained on massive datasets of sensor data.
**Results:** then, the robust technique DL (Deep Learning) can be utilized for ID (Intrusion Detection) the industrialized settings, when specifically combined with other IoT devices like sensors and alert systems. Thus, the model is trained and tested. Finally, it achieved 98,51 % and 94,85 % accuracy accordingly.
**Conclusion:** these frameworks after the completing training phase can be employed for the novel sensor data's actual analysis and also for the anomalies detection as it reveals a potential ID.

**Keywords:** Convolutional Neural Networks (CNN); IoT; Recurrent Neural Networks (RNN); Passive (ID) Intrusion Detection.

## RESUMEN

**Introducción:** la detección pasiva de intrusiones en entornos industriales puede ser un desafío, especialmente cuando el área que se monitorea es extensa. Sin embargo, con la llegada de la tecnología IoT, es posible implementar sensores y dispositivos que puedan ayudar con la segmentación masiva de la intrusión pasiva. Por lo tanto, este enfoque implementa un algoritmo ML (aprendizaje automático) como soporte CNN improvisado (red neuronal convolucional) para identificar y evitar el acceso ilegal a áreas críticas en tiempo real, lo que en última instancia mejora la seguridad en entornos industriales.
**Métodos:** a su vez el algoritmo propuesto puede detectar patrones y anomalías que podrían indicar una intrusión pasiva. Para descubrir los patrones y las conexiones entre los distintos puntos de datos de los sensores, se pueden entrenar técnicas de DL (aprendizaje profundo) como CNN, redes neuronales recurrentes

(RNN) y codificadores automáticos (AE) en conjuntos de datos masivos de datos de sensores.
**Resultados:** luego, la técnica robusta DL (Aprendizaje profundo) se puede utilizar para la identificación (detección de intrusiones) en entornos industrializados, cuando se combina específicamente con otros dispositivos de IoT como sensores y sistemas de alerta. Así, el modelo se entrena y prueba. Finalmente, logró una precisión del 98,51 % y del 94,85 % en consecuencia.
**Conclusión:** estos marcos después de completar la fase de capacitación se pueden emplear para el análisis real de los datos del nuevo sensor y también para la detección de anomalías, ya que revela una identificación potencial.

**Palabras clave:** Redes Neuronales Convolucionales (CNN); IoT; Redes Neuronales Recurrentes (RNN); Detección de Intrusiones Pasivas (ID).

## INTRODUCTION

The method of avoidance of illegal activities, or loss, or stealing or leaking data of the industrial methods, Net, and properties can be defined as IS (Industrial security). The risk of cyber-attacks is growing in the interconnected world nowadays. Then, it will lead to crucial attacks with loss of efficiency, and affecting the sensitive data.

An effective technique that has the potential for the IS advancements was IoT-based solutions. It can be employed for monitoring and data collection from IS, and also deliver actual time insights in the potential security risks. Monitoring network traffic for the malicious activity despite of creating additional traffic can be accomplished by passive ID. It is the efficient way for the security risks detection and reduction.

The method of segmenting a net into more compressed and isolated can be named as segmentation. It will support in the improvements of IS thereby diminishing the vulnerable attack area, also having the potential breach impacts.

Industrial organizations may improve their protection against those security risks with the IoT-based solutions utilization of the passive ID and segmentation. It will ensure prompt monitoring and reacts to the security risks, and enhancing the total safety status of industrial systems.

IS is paramount in safeguarding against unauthorized access, data breaches, and other malicious activities that could disrupt operations or compromise sensitive information. With the increasing interconnectedness of industrial systems, the risk of cyber-attacks has become a significant concern. In response to these threats, innovative approaches leveraging Internet of Things (IoT) technology have emerged as promising solutions for enhancing industrial security. By deploying sensors and devices throughout industrial environments, organizations can gather real-time data and insights, enabling proactive measures to mitigate security risks. One such approach is passive intrusion detection (ID), which involves monitoring network traffic and identifying potential threats without generating additional traffic or causing disruptions. Passive ID is particularly effective in industrial settings where maintaining operational efficiency is crucial. Segmentation, the process of dividing a network into smaller, isolated segments, plays a vital role in enhancing industrial security. By reducing the attack surface and limiting the potential impact of breaches, segmentation strengthens overall defense mechanisms. In this study, suggesting a novel approach to passive ID in industrial environments with IoT-based solutions and machine learning (ML) algorithms. Specifically, employing CNNs, RNNs, and AEs to analyze massive datasets of sensor data and detect patterns indicative of unauthorized access or anomalies.

### Critics study

At the very beginning of the decade, study on the security risks related to IoTat was led by Atzori et al.[1] and Weber[2]. IoT privacy and security issues were briefly discussed by Atzori et al.[1], with an emphasis on RFID and wireless sensor networks (WSNs). Conversely, Weber[2] concentrated on RFID and IoT security laws, privacy laws, and private information safety. Information privacy, safety, and confidence regarding IoT security were discussed by Miorandi et al.[3]

Ziegeldorf et al.[4] researched IoT privacy risks and problems in detail. From the perspective of IoT architecture, Zhao and Ge[5] divided IoT into perception, transport, and application layers and discussed the security issues surrounding each layer. Jing et al.[6] examined each layer's characteristics, security issues, and remedies. IoT security discussions evolved, researchers began to focus on specific technologies and scopes. For instance, Fremantle and Scott[7] we investigated the IoT security middleware, whereas Granjal et al.[8] The investigation pertained to the security aspects of communication protocols utilised in the Internet of Things (IoT). The analysis encompassed the physical and medium access control layers, as well as the IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) and routing protocol for (LLN) Low power and Lossy Networks RPL. Nguyen et al.[9] focused on the protection against assaults and the security of IoT and

https://doi.org/10.56294/sctconf2024934

WSN communication protocols. Airehrour et al.[10] A comprehensive security analysis was performed on routing protocols for the IoT, with a specific focus on LLN. Qin et al.[11] explained briefly the data-centric approach to IoT security. Loi et al.[12] consumer IoT gadgets have been the focus of their attention. Meanwhile, IoT application and architectural security using blockchain has been studied by Fernández-Caramés et al.[13] and Lao et al.[18] Hassija et al.[14] including a discussion of IoT application security, while Berkay et al.[15] and Tabrizi and Pattabiraman[16] examined IoT security from the standpoint of the coding environment and the code itself. Lastly, Amanullah et al.[17] examined how big data, IoT security, and deep learning are related, and Joao et al.[19] surveyed IoT risk concepts and assault routes.

These studies on the security of the Industrial IoT (IIoT) focus on the use of deep learning to the identification of potential dangers[20,21,22] and on the deployment of decentralized blockchain technology.[22,23] They do not, however, undertake a thorough security examination of IIoT architecture and contemporary commercial solutions. This raises concerns about the industry present security solutions suitability for IIoT architectural security.

An Ensemble network ID method utilising proven statistical flow features has been suggested by Moustafa et al.[23] The intention is to reduce harmful occurrences, particularly botnet assaults on the DNS, HTTP, and MQTT protocols utilized in IoTs networks. Their initial study involves a thorough examination of the TCP/IP framework and then FE (Feature Extraction) process from the MQTT, HTTP, and DNS network traffic protocols. The authors utilize their own extractor module for generating further statistical features of the transactional flows while additionally employing the Bro-IDS tool for basic features.

As such, to simplify the NIDS and lower its computing cost, features are filtered such that only the most significant ones are chosen. The researchers in this stage by using the correlation coefficient on resultant features. Finally, an (EL) Ensemble Learning model called AdaBoost is created to identify the assaults. 3 distinct ML techniques: Decision Tree (DT), Naive Bayes (NB), and Artificial NN (ANN) algorithms are combined to form the basis of the technique. The (CEM) Correlated Entropy Method, which was determined from the (FV) Feature Vectors, was a major factor in the selection of these classification strategies. When utilizing the AdaBoost (Adaptive Boosting) technique, the detection efficiency is better than when employing every ML methodology on their own.

An EF (Error Function) is implemented when the FVs differ significantly. In order to calculate the error value for all instances of the dispersed input data, the EF is crucial. It is feasible to comprehend and assess which learners are more qualified to categorize every instance according to this error value. Comparing the ensemble approach to current (SOTA) State-Of-The-Art methods, the experiment outcomes provide a low FPR (False Positive Rate) (ranging from 0,01 % and 0,72 %) and a high DR (Detection Rate) (95,25 %–99,86 %). To corroborate the conclusions, the authors used simulated IoT sensor data from the UNSWNB15 and NIMS botnet databases.

Additionally, an offline IDS for IoT networks[24] makes utilization of a Multi-Layer Perceptron (MLP), a kind of supervised ANN. The ANN is composed of three layers, and the neurons in the HL (Hidden Layer) and OL (Output Layers) convert their input values to a particular output value using a unipolar sigmoid TF (Transfer Function). A SL (Stochastic Learning) approach with a MSE (Mean Square Error) function was used to train the network. Both feed-forward and backward training algorithms were used in the training procedure. The ANN analyzes Internet packet traces and looks for DoS and DDoS attacks in IoT networks in order to carry out its mission. 4 client nodes and a server relay node made up a test system that was employed to assess the IoT IDS.

In addition to DDoS attacks from 3 hosts, all transferring over 10 million UDP packets at wire speed, the server node was also targeted by a DOS attack from a single host that transmitted more than 10 million UDP packets. Their simulations' outcomes revealed a 99,4 % detection accuracy and a 0,6 % FPR. A total of 2313 samples made up the training dataset that the researchers applied; 496 of these samples were chosen for testing and 496 for validation.

**Security challenges and concerns on IIOT**

IoT connects all "things" at all time. These "things" often have three main characteristics in industry: heterogeneity, individuality, and connectedness. Security and privacy issues have become more difficult as IIoT has developed and supported numerous companies. The notable characteristics of IIoTs were thought to be their high heterogeneity, massive size of "things," and cyber-physical systems.

It also worsened continuously due to those security risks. It ocuurs with the source of traditional technique issues like APT (Advanced Persistent Threats).

Connecting physical assets, sensors, and other devices to the internet obtained through operating industries in the modernized manner of the IIoT. It permits for the data transmission and thus improved automation. Significant risks and concerns are posed by the IIoT. Few security risks and concerns associated with IIoT are listed below:

- Cyberattacks: There will be major threats in the cyber-attacks, as numerous devices are interconnected. The suspicious activities can be detected through the cybercriminals with the IIoT device utilization in order to steal sensitive data, cause physical harm or interrupt operations.
- Data privacy: Large amounts of data can be transmitted and gathered by the IIoT devices, few of

https://doi.org/10.56294/sctconf2024934

the data may require security as it has sensitive data. Major threats in the data breaches comprises of reputation loss, financial loss and legal issues.

- Complexity: The multiple layers of hardware and software in the complicated IIoT devices. Efficiently detecting and diminishing security risks posed by this complexity.
- Lack of standardization: Since there is no standard framework for IIoT security and it may cause suspicious and irregular activities in several devices.
- Legacy systems: Before the IIoT existence, there are several industrial systems created and it is difficult to secure them effectively. In the Old dated systems, installing new security features may be expensive and also time-consuming.

Thus, an extensive approach can be essential for addressing those issues and concerns about the improvement in security and its application at all levels in the IIoT settings, constant monitoring and suspicious activity detection.

## METHOD

### Architectural Components in Proposed Methodology

Figure 1 presents the architectural components. In the data preprocessing stage, the raw sensor data undergoes cleaning, noise reduction, and scale adjustment to ensure its quality and suitability for analysis. The network architecture is then designed, typically comprising convolutional layers for extracting local features, pooling layers for downsampling, and fully connected layers for feature extraction and final output generation. Modernized CNN ensembles are employed for improved accuracy and flexibility. During training, the CNN learns normal and abnormal activities from labeled data, continuously adjusting weights to minimize output variance. Evaluation assesses the CNN's performance using separate datasets, measuring accuracy, precision, and recall. Finally, the trained CNN-based anomaly detection system is deployed in real-world industrial settings, integrating it into existing security systems for real-time monitoring and alerting.

The modernized CNN for anomaly detection in the sensor data contains the following steps listed below:

- Data preprocessing: The initial stage is the data pre-processing. The data cleaning, noise removing and adjusting scales can be done during these procedures,
- Network architecture: The conventional CNN structure can be constructed through the multiple layers of (CL) convolutional layers, pooling and FC (Fully Connected) layer. The downsampled feature maps are obtained by the pooling layers and the CL gathers the local features from the input data and the FC layers generates the extracted features, and the final output was created. For improving IDS accuracy and flexibility, the modernized CNN ensemble with CNN frameworks, as it contains several structures and hyperparameters.
- Training: For training the CNN, the normal and abnormal sensor data can be utilized. The normal and abnormal activities was learned by the networks throughout training. During training the weights can be adjusted continuously for the variance among expected and actual outputs reduction.
- Evaluation: The CNN's performance is examined after it has been trained using a different dataset. In this assessment, the network's ability to identify abnormalities is measured for accuracy, precision, and recall.
- Deployment: The final step is to deploy the CNN-based anomaly detection system in a real-world setting. This involves integrating the network into an existing industrial security system and setting up a real-time monitoring and alerting system.

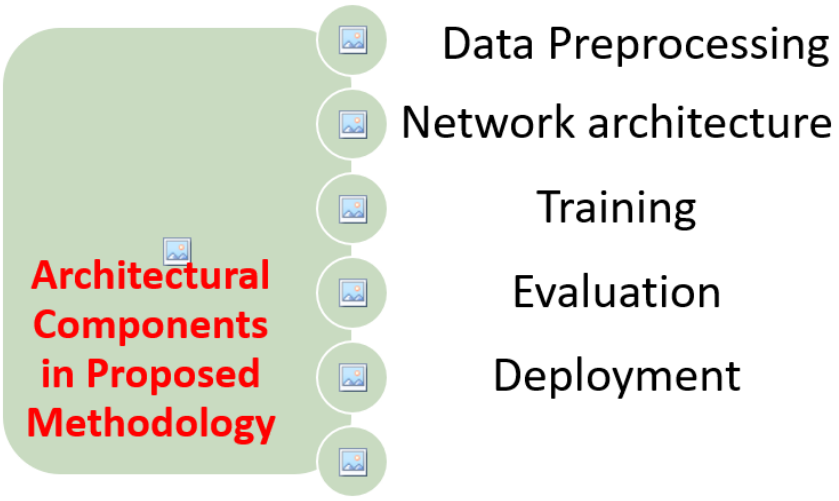


**Figure 1.** Architectural Components

https://doi.org/10.56294/sctconf2024934

**Role of Dataset**

We have used the benchmark dataset for the Distributed Smart Space Orchestration System (DS2OS) obtained from Kaggle as an open data collection supplied by Pahl and Aubet. With the aid of DS2OS, an imaginary IoT environment's artificial data set was gathered. Traces from several IoT simulation sites employing various services, such as light controllers, thermometers, movement sensor values, washing machines, battery and temperature status, and smart door and smartphone manipulation, are included in this data collection. 347,935 normal and 10,017 abnormal data points make up the dataset's 357,952 data points. 13 characteristics, presented in table 2, may be divided into eight classes in the DS2OS dataset. Normal data is included in these classes, along with seven different forms of attacks, including Denial of Service, scan, malicious control, malicious operation, espionage, data probing, and assaults with faulty configuration. The following is a short description of each of these classes in this data set:

- Normal: Typical information that is accurate and thorough.
- Denial of Service: The target is assaulted by an attacker's excessive packets, which prevent the server or other device from using the service.
- Scan: Data corruption may result by scanning the system to obtain data using hardware.
- Malicious control: An attacker may be able to get a working session key or successfully intercept network traffic thanks to a software flaw. A bad individual may control the whole system in this manner.
- Malicious operation: Usually, malicious software is at blame for these assaults. Malware describes bogus actions that obstruct the primary function. The device's performance may be negatively impacted by this malicious activity.
- Spaying: An attacker exploits the system vulnerabilities for acquiring the unauthorized access to the system through a hidden way also gathering the significant information. In this se, data manipulation will pose a risk for the system.
- Data probing: New data type for the raw information was replaced by the attacks as they generate threatening nodes.
- Incorrect setup: It will lead to the data interruption.

**Data Pre-processing**

The specific standard techniques needed for data preprocessing in Improvised Convolutional Neural Network (CNN) for anomaly detection in sensor data are as follows: Data cleaning involves removing any noise, missing values, or outliers from the sensor data that could affect the performance of the network. In order to ensure that the network is trained on high-quality data and can generalize effectively to fresh data, this is a crucial step.

Data normalization is another important technique in data preprocessing, which involves scaling the data to a common range and distribution. By ensuring that every incoming data has a same scale, this may help the network function better, which can reduce the impact of any features that have a large range of values. Data augmentation increases dataset size and network generalization. In following that Feature extraction is performed before feeding the sensor data into the CNN, it may be necessary to extract relevant features from the raw data. This can involve applying signal processing techniques, such as Fourier transforms or wavelet transforms, to extract time or frequency domain features. In sequence, Dimensionality reduction technique as PCA is used to reduce reducing input characteristics and increasing network efficiency.

**Role of improvised CNN**

Image recognition and computer vision use CNNs. However, they can also be applied to other types of data, including sensor data. Figure 2 represents a Role of improvised CNN to learn by being exposed to a large collection of sensor data throughout training to identify patterns and relationships between different sensor readings. Deep learning techniques are often used in the realm of industrial security for anomaly identification. Anomaly detection involves monitoring a system for unusual behavior might reveal a potential security risk. Implementing an ensemble of multiple CNN models with different architectures and hyperparameters are done in improvised CNN for the intrusion detection system. A CNN may be taught to recognize patterns of typical behaviour and identify anomalies that differ from these patterns by training it on a large batch of sensor data. Real-time monitoring is another key aspect of industrial security. By deploying a CNN-based anomaly detection system that can operate in real-time, potential security threats can be detected and addressed quickly, before they can cause significant damage. Overall, deep learning algorithms such as CNNs have shown great promise in enhancing industrial security by enabling real-time monitoring and detection of potential security risks based on large datasets of sensor data.

https://doi.org/10.56294/sctconf2024934

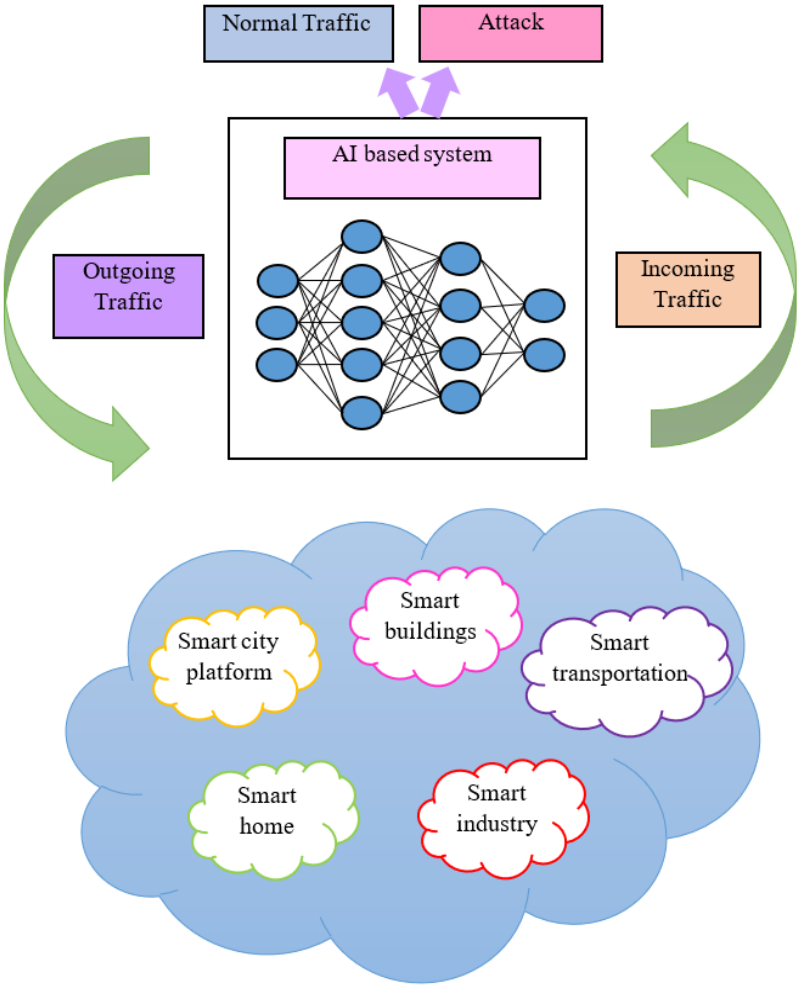


**Figure 2.** Improvised CNN architecture

1. Define the CNN architecture
a. Initialize a sequential model
b. Add a convolutional layer (CL) with a specified amount of filters, kernel size, AF, and input shape
c. Add a max pooling layer with a specified pool size
d. Repeat steps b and c for the desired amount of layers
e. Flatten the output of the final CL
f. Add one or more FC (Fully Connected) layers with a specified amount of units and AF
g. Add an output layer with a sigmoid AF (Activation Function)
h. Implement an ensemble of multiple CNN models with different architectures and hyperparameters
2. Compile the model
a. Specify the loss function, optimizer, and performance metric
3. Train the model a. Specify the batch size, amount of epochs, and validation split b. Fit the model to the training data and validate on the validation data
4. Calculate the model performance a. Calculate the model on the test data and calculate the performance metrics like accuracy, precision, and recall b. Adjust the model architecture and hyperparameters as needed
5. Use the model for anomaly detection a. Input a new sensor data sample b. Obtain the predicted output from the model c. Compare the predicted output to a threshold value d. If the predicted output is below the threshold value, classify the sample as normal; otherwise, classify it as anomalous

**Figure 3.** Pseudocode implementation of a CNN algorithm for anomaly detection in sensor data

https://doi.org/10.56294/sctconf2024934

*Deployment of improvised CNN*

In sequence to Data Preprocessing, CNN is deployed. CL, pooling, and FC layers are generally included in several levels of a CNN's architecture for anomaly identification in sensor data.

A CNN's convolutional layer filters new data to extract local characteristics. Each filter performs a dot product among the input data and the filter weights at each point as it slides across the input data. A set of (FM) Feature Maps demonstrating the existence of various local features in the input data is the CL's output. After the CL, a pooling layer is usually added, which down samples the FM to lessen their dimension and upsurge their power to small variations in the input data. Max pooling is a common pooling operation that chooses the maximum value within a small rectangular window of the FM. For extracting progressively complicated features from the input data, the CL and pooling layers are often repeated many times. Following reducing, one or more FC layers are employed to the output of the last CL, which process the extracted features to generate the final output. CNNs learn to spot deviations from usual behaviour during training. Minimizing a loss function that compares expected and actual outputs achieves. Once the CNN has been trained, it can be used to detect anomalies in new sensor data by comparing the predicted output to a threshold value.

*Performance model of the CNN architecture*

a. Initialize a sequential model

b. Add a CL with a specified amount of filters, kernel size, AF, and input shape using formula

Convolutional output layer = activation (convolution (input, filter) + bias) ------- (1)

c. Add a maximum layer of pooling with a predetermined pool size.

Max pooling layer: = max_pooling(input, pool_size) ---------- (2)

d. Repeat steps b and c for the desired number of layers

e. The last convolutional layer's output should be flattened

Flatten layer: = flatten(input) ---------- (3)

f. Add a given number of units and activation functions to one or more completely linked layers

Fully connected layer: = activation (dot (input, weight) + bias) ----- (4)

g. A sigmoid activation function output layer should be added.

Output layer: = sigmoid (dot (input, weight) + bias) ------- (5)

In sequence to CNN proposed model is done, compilation is done by

Compile model: = model.compile(loss='binary_crossentropy', optimizer='adam', metrics=['accuracy']) ---------- (6)

Training model is done by

Train:=model.fit(x_train,y_train,batch_size=batch_size,epochs=epochs,validation_split=validation_split) --(7)

**Model Validation**

Compilation of the model are performed via Specifing the loss function, optimizer, and performance metrics. Training the model is done via Specifing the batch size, number of epochs, and validation split. In sequence to that, fit the model for data training as well as validation.

## RESULT AND DISCUSSION

When evaluating the merits of the proposed strategy, a variety of performance criteria are taken into consideration.

- Accuracy: The proportion of normal and abnormal data that the IDS accurately anticipated is represented by accuracy.
- Precision: When compared to all recordings that the IDS has accurately identified as normal, the accuracy is the percentage of normal recordings that are correctly detected.

https://doi.org/10.56294/sctconf2024934

- Recall: It will measure the correctly predicted positive IDS occurred.
- F1-score: The accuracy of recall and harmonic mean are employed for the creation of the F1-score.

**Table 1.** Performance criteria for evaluating the merits of the proposed strategy

| Model | Accuracy | Precision | Recall | F1-Score |
|---|---|---|---|---|
| Simple CNN | 92,1 | 92 | 91,4 | 91,7 |
| RNN | 93,6 | 95 | 92 | 93,5 |
| Auto Encoder | 94,4 | 96,4 | 93 | 94,7 |
| GAN | 96,7 | 96,5 | 95,4 | 95,9 |
| Improvised CNN | 98,7 | 98,9 | 97,6 | 98,2 |

## CONCLUSION

Passive ID provided by IoT via enhanced CNN is an affordable and expandable solution that can assist in addressing the security issues that industrial companies are facing. Organizations may guarantee safety, safeguard assets and operations, and reduce risks by putting this strategy into practice. The enhanced CNN framework is a perfect tool for spotting intrusion attempts since it is especially good at spotting odd patterns and behaviors. The model is a reliable means of preserving the IS since it can also pick up on novel threat vectors and adjust to them. As a result, the enhanced CNN algorithm serves as a perfect tool for spotting intrusion attempts because it is especially good at spotting odd patterns and behaviors. The framework is an effective way of preserving the IS since it can also pick up on emerging threat vectors and adjust to them.

## REFERENCES

1. Atzori L, Iera A, and Morabito G. The internet of things: A survey. Computer networks, 54(15), pp. 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010.

2. Weber RH. Internet of Things-New security and privacy challenges. Computer law & security review, 26(1), pp. 23-30. https://doi.org/10.1016/j.clsr.2009.11.008.

3. Miorandi D, Sicari S, De Pellegrini F, and Chlamtac I. Internet of things: Vision, applications and research challenges. Ad hoc networks, 10(7), pp. 1497-1516. https://doi.org/10.1016/j.adhoc.2012.02.016.

4. Zhao K, and Ge L. A survey on the internet of things security. In Ninth international conference on computational intelligence and security, pp. 663-667. https://doi.org/10.1109/CIS.2013.145.

5. Ziegeldorf JH, Morchon OG, and Wehrle K. Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), pp. 2728-2742. https://doi.org/10.1002/sec.795.

6. Fremantle P, and Scott P. A security survey of middleware for the Internet of Things. PeerJ PrePrints, 3, pp. 1-22. https://dx.doi.org/10.7287/peerj.preprints.1241v1.

7. Görmüş S, Aydın H, and Ulutaş G. Security for the internet of things: a survey of existing mechanisms, protocols and open research issues. Journal of the Faculty of Engineering and Architecture of Gazi University, 33(4), pp. 1247-1272.

8. Nguyen KT, Laurent M, and Oualha N. Survey on secure communication protocols for the Internet of Things. Ad Hoc Networks, 32, pp. 17-31. https://doi.org/10.1016/j.adhoc.2015.01.006.

9. Airehrour D, Gutierrez J, and Ray SK. Secure routing for internet of things: A survey. Journal of Network and Computer Applications, 66, pp. 198-213. https://doi.org/10.1016/j.jnca.2016.03.006.

10. Qin Y, Sheng QZ, Falkner NJ, Dustdar S, Wang H, and Vasilakos AV. When things matter: A survey on data-centric internet of things. Journal of Network and Computer Applications, 64, pp. 137-153. https://doi.org/10.1016/j.jnca.2015.12.016.

11. Loi F, Sivanathan A, Gharakheili HH, Radford A, and Sivaraman V. Systematically evaluating security and privacy for consumer IoT devices. In Proceedings of the Workshop on Internet of Things Security and Privacy, pp. 1-6. https://doi.org/10.1145/3139937.3139938.

12. Fernández-Caramés TM, and Fraga-Lamas P. A Review on the Use of Blockchain for the Internet of Things. Ieee Access, 6, pp. 32979-33001. https://doi.org/10.1109/ACCESS.2018.2842685.

13. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, and Sikdar B. A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access, 7, pp. 82721-82743.

14. Berkay Celik Z, Fernandes E, Pauley E, Tan G, and McDaniel P. Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities. arXiv e-prints, pp.arXiv-1809. https://doi.org/10.48550/arXiv.1809.06962.

15. Tabrizi FM, and Pattabiraman K. Design-level and code-level security analysis of IoT devices. ACM Transactions on Embedded Computing Systems (TECS), 18(3), pp. 1-25. https://doi.org/10.1145/3310353.

16. Amanullah MA, Habeeb RAA, Nasaruddin FH, Gani A, Ahmed E, Nainar ASM, Akim NM, and Imran M. Deep learning and big data technologies for IoT security. Computer Communications, 151, pp. 495-517. https://doi.org/10.1016/j.comcom.2020.01.016.

17. Lao L, Li Z, Hou S, Xiao B, Guo S, and Yang Y. A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. ACM Computing Surveys (CSUR), 53(1), pp. 1-32. https://doi.org/10.1145/3372136.

18. Sequeiros JB, Chimuco FT, Samaila MG, Freire MM, and Inácio PR. Attack and system modeling applied to IoT, cloud, and mobile ecosystems: Embedding security by design. ACM Computing Surveys (CSUR), 53(2), pp. 1-32. https://doi.org/10.1145/3376123.

19. Polychronou NF, Thevenon PH, Puys M, and Beroulle V. A comprehensive survey of attacks without physical access targeting hardware vulnerabilities in iot/iiot devices, and their detection mechanisms. ACM Transactions on Design Automation of Electronic Systems (TODAES), 27(1), pp. 1-35. https://doi.org/10.1145/3471936.

20. Gaspar PD, Fernandez CM, Soares VN, Caldeira JM, and Silva H. Development of technological capabilities through the internet of things (Iot): Survey of opportunities and barriers for iot implementation in Portugal's agro-industry. Applied Sciences, 11(8), pp. 1-18. https://doi.org/10.3390/app11083454.

21. Wu Y, Wang Z, Ma Y, and Leung VC. Deep reinforcement learning for blockchain in industrial IoT: A survey. Computer Networks, 191, pp. 108004. https://doi.org/10.1016/j.comnet.2021.108004.

22. Latif S, Idrees Z, e Huma Z, and Ahmad J. Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions. Transactions on Emerging Telecommunications Technologies, 32(11), pp. 1-37. https://doi.org/10.1002/ett.4337.

23. Moustafa N, Turnbull B, and Choo KKR. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. IEEE Internet of Things Journal, 6(3), pp. 4815-4830. https://doi.org/10.1109/JIOT.2018.2871719.

24. Chio C, and Freeman D. Machine learning and security: Protecting systems with data and algorithms. " O'Reilly Media, Inc.", pp. 1-118.

## FINANCING

The authors did not receive financing for the development of this research.

## CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

## AUTHORSHIP CONTRIBUTION

*Conceptualization:* Arunkumar S.
*Data curation:* Gowtham M.S.
*Formal analysis:* Gowtham M.S.
*Research:* Revathi N.

*Methodology:* Krishnaprasath V.T.
*Drafting - original draft:* Krishnaprasath V.T.
*Writing - proofreading and editing:* Arunkumar S.

https://doi.org/10.56294/sctconf2024934