Journal of Trends in Computer Science and Smart Technology (ISSN: 2582-4104)
www.irojournals.com/tcsst/

IIoT-IDS Network using Inception CNN Model

A. Arun Kumar[1*], Radha Krishna Karne[2]

[1]Professor in CSE, MLRITM, Dundigal, Hyderabad, India
[2]Assistant professor in ECE, BITS, Narsampet, India

E-mail: *krk.wgl@gmail.com

Abstract

Modern network and Industrial Internet of Things (IIoT) technologies are quite advanced. Networks experience data breaches annually. As a result, an Intrusion Detection System is designed for enhancing the IIoT security protection under privacy laws. The Internet of Things' structural system and security performance criteria must meet high standards in an adversarial network. The network system must use a system that is very stable and has a low rate of data loss. The basic deep learning network technology is picked after analysing it with a huge number of other network configurations. Further, the network is upgraded and optimised by the Convolutional Neural Network technique. Additionally, an IIoT anti-intrusion detection system is built by combining three network technologies. The system's performance is evaluated and confirmed. The proposed model gives a better detection rate with a minimum false positive rate, and good data correctness. As a result, the proposed method can be used for securing an IIoT data privacy under the law.

Keywords: Convolutional Neural Network (CNN), Industrial Internet of Things (IIoT), Intrusion Detection System (IDS)

1. Introduction

Two of the key technologies in the digitalization revolution are the Internet of Things (IoT) and the Industrial Internet of Things (IIoT). The IoT is a network of interconnected gadgets that may exchange messages and give consumers access to data. IoT devices often feature sensors that allow them to collect data and can connect to the Internet. Even though an IoT device might be helpful on its own, they become even more effective when used in combination with other IoT devices. The IoT expands in scope as more equipment becomes able to connect to the Internet. A wide variety of gadgets are part of the IoT. The number of

DOI: https://doi.org/10.36548/jtcsst.2022.3.002
Received: 19.06.2022, received in revised form: 22.07.2022, accepted: 08.08.2022, published: 18.08.2022
© 2022 Inventive Research Organization. This is an open access article under the Creative Commons Attribution-NonCommercial International (CC BY-NC 4.0) License

connected devices is increasing every day, and anything from factory equipment to electrical substations to buildings and infrastructure can be a part of it. The IoT is used by a wide range of enterprises, including manufacturers, energy providers, local governments, and many more. With the use of IoT technology, data can be gathered automatically from many different tasks, such as the amount energy a building's lighting uses or the quantity of water that pass through a wastewater treatment plant. The data that IoT systems and devices collect can be sent to a centralised system over the Internet.

A subtype of IoT is IIoT. IoT technology utilised in industrial settings, namely in manufacturing plants, is what the phrase alludes to. The next stage of the industrial revolution, known as Industry 4.0, heavily relies on the IIoT. Smart technology, data, automation, interconnection, artificial intelligence, and other technologies and capabilities are highlighted by Industry 4.0. The management of factories and industrial organisations is being revolutionised by these technologies. Many of the same applications and advantages as IoT are possible with IIoT. Manufacturing equipment, energy systems, and infrastructure like pipelines and wiring can all use smart sensors. These sensors can assist industrial businesses in increasing their efficiency, production, employee safety, and other factors through the data they collect and the cutting-edge capabilities they provide. The IIoT improves machine-to-machine connectivity and feeds plant administrators data that helps them understand how their facility is running. Industrial businesses can keep a better eye on how much energy, water, and other resources they're using, when their machinery is working, and how much they're generating through the ongoing collection of detailed data. To maximise their operation, operators can then make manual modifications, or equipment can adjust automatically.

2. Methods

2.1 IIoT

The term "IIoT" refers to the fusion of industrial production and IoT to increase the productivity of industrial automation products. Transportation, electricity grids, industrial, and environmental monitoring all routinely employ IIoT. It benefits from reliable transmission and intelligent processing. Figure 1 shows how informationalization, remote management control, and intelligent networks are achieved by connecting sensors, controllers, machines, people, and objects through local networks or the Internet [1]. An addition to the Internet is the IoT. It is compatible with all Internet apps and encompasses the

entire Internet as well as all of its contents. However, every component of the IoT (devices, resources, communications, etc.) is customised and privatised.

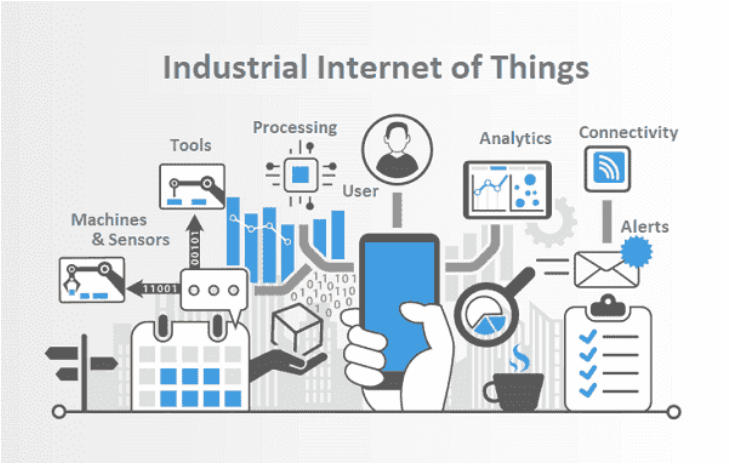

Figure 1. IIoT Control System

The language of the networked world is represented by the communication protocol in Figure 2. The industrial business competition and the lack of security design in network architecture, makes the system directly open to threat when it is connected with an internet [2]. Traditional industrial protocols have not reached their full potential in terms of security and future-proofing due to the arrival of cutting-edge concepts like the Industrial Internet.

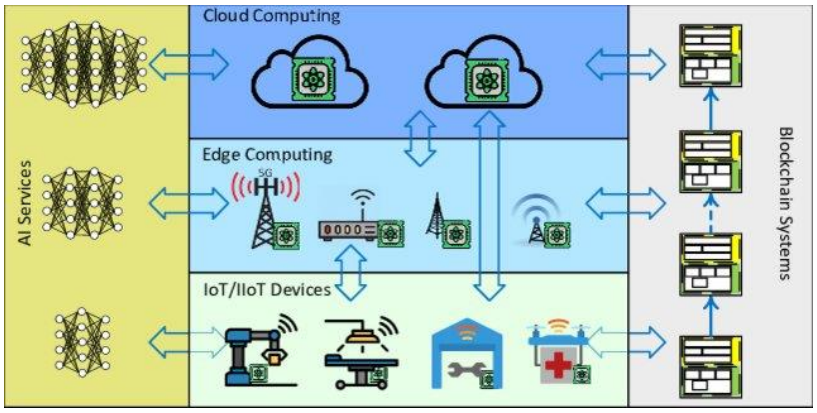

Figure 2. IIoT Network Model

The technological revolution is somewhat influencing the digital industrial revolution, which is shown in Figure 3. Industrial specialist examines their own internal technological issue, updates the same after new methodologies are established, and chooses the ones that are suitable for them. Various sectors have various application scenarios, which leads to various needs [3]. Bubble net and spiral searches are used in place of the network's

search machine to increase accuracy and cut down the execution time in order to accomplish the retrieval function's purpose.

Figure 3. IIoT application areas

The IIoT's invention stage is separated into three stages as seen in Figure 4. Cognitive innovation is step one. The understanding of the Industrial Internet has advanced steadily, moving from the connectivity of equipment through the interconnection of machines, people, and things, finally to the all-encompassing interconnectedness of all elements [4], with the complete industrial connection, and its value chain. Idea innovation is the next phase, i.e., the evolution and law. The mechanics of the Industrial Internet has to be fully understood. The Industrial Internet is a total expansion of information network methodology to a physical platform from a virtual scenario. It is not simply a production-focused counterpart of the consumer Internet. Pattern invention is the step 3. The social and economic growth of various countries is becoming increasingly entwined as the world enters a new phase of significant development, transformation, and adjustment.

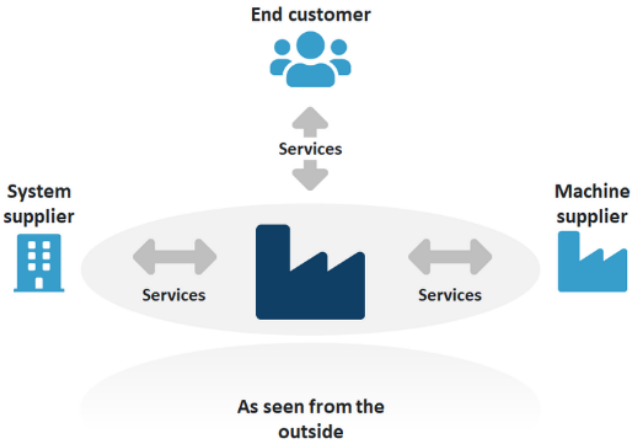

Figure 4. IIoT Stages

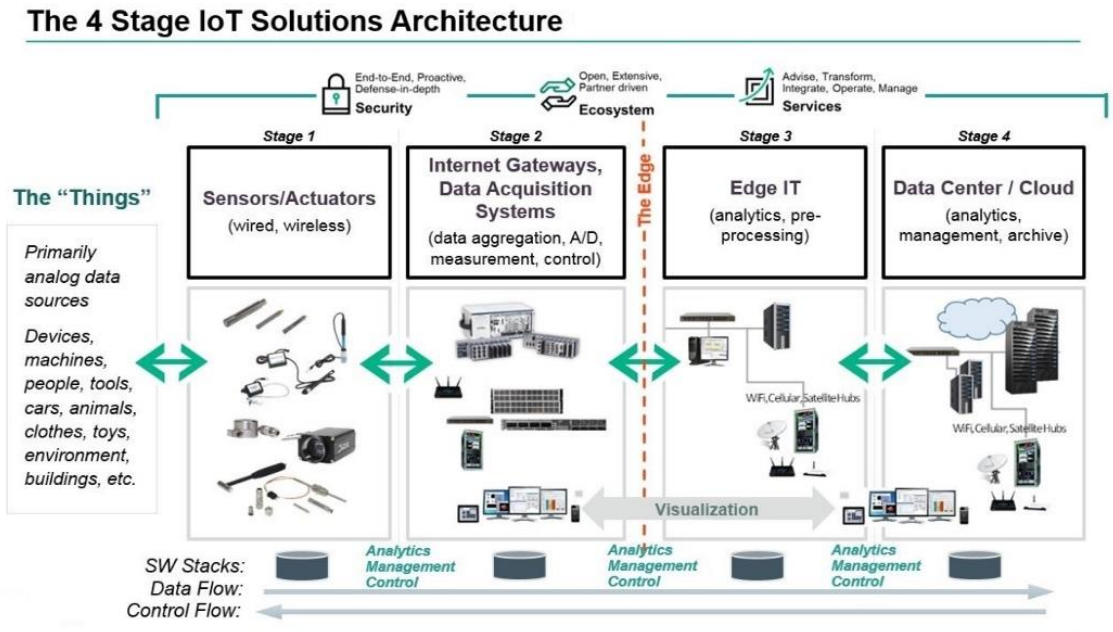

Figure 5. IIoT Key Technologies

Comprehensive sensing, information transmission, intelligent processing, and information feedback are the primary IIoT key technologies shown in Figure 5. Comprehensive perception is the process of gathering and acquiring knowledge about objects at any time and place using current information gathering and gathering strategies. Information transmission refers to the timely and secure exchange of information through Internet and communication networks. In order to better comprehend the production, environment is equipped with division making system incorporated with a control strategy. Intelligent processing requires analysing and processing the large amounts of data and information that have been acquired [5]. To optimise the production structure and complete the production plan, information feedback refers to the transfer of programme instructions, including the processed information to each production link [6].

2.2 IDS

The IDS is essentially a network security management tool. The basic idea is to gather and examine network data to extract offensive information and behaviours to ascertain whether there have been intrusions. Because assaults and intrusions cannot be totally prevented, IDS is a system that may detect them early and send valuable security notifications to security administrators [7]. Users are clear in monitoring the intrusion detection systems, as the actual harm caused by intrusion events rise.

An essential component of the architecture for network security is the intrusion detection system. The IDS can safeguard the system, machinery, and equipment by precisely assessing odd network occurrences. The firewall typically consists of processing rules, resource objects, audit records, behaviour files, and behaviour subjects. The IDS expands the firewall.

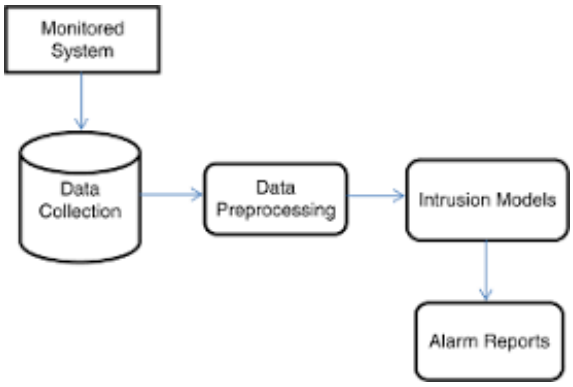

Figure 6. IDS Model

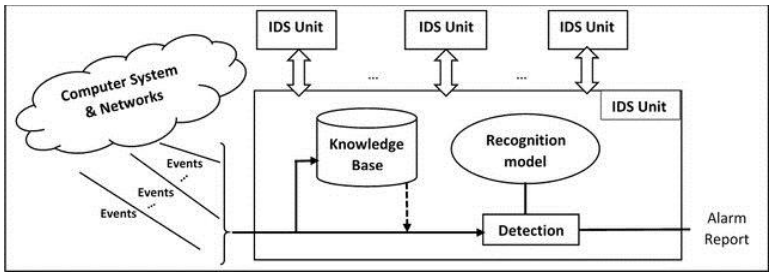

Figure 7. IDS Network Structure

The system's goal is to find abnormalities, system flaws, or application problems that could allow intrusions. The system can be separated into two categories: abnormal behaviour and misuse detection. The decisions made during the preceding step are addressed in the report and response phase. If the system concludes that an intrusion has occurred, it will take the proper countermeasures or notify management employees so that action can be taken [8]. The IDS can be split into three categories based on the classification of detection technology: hybrid detection, misuse detection, and anomaly detection. The idea behind an abnormality detection is to compare the proportion of system activities and daily behaviours of network users to the potential incursion. The base of misuse detection is the creation of a database from observed intrusion activity [9-11]. To evaluate an intrusion behaviour, an access behaviour that has occurred is contrasted with an intrusion behaviour that has been recorded

in the database. Both the false negative rate and the abuse detection rate are very high. Therefore, by following thorough optimization of the two, a hybrid detection is created.

2.3 IIoT-IDS

The Internet is constantly accessible to devices in the IIoT. As a result, IIoT security protection needs to be built. Deep learning's flexibility is utilised. The following actions are taken to detect intrusions:

1. Keep track of and evaluate system and user activity;
2. Examine system vulnerabilities and structure;
3. Spot patterns behaviour that resemble known assaults and notify the necessary parties;
4. Statistical evaluation of irregular behaviour trends;
5. Examine the reliability of crucial systems and data files; and
6. Manage operating system audit trails and look for user actions that go against security rules.

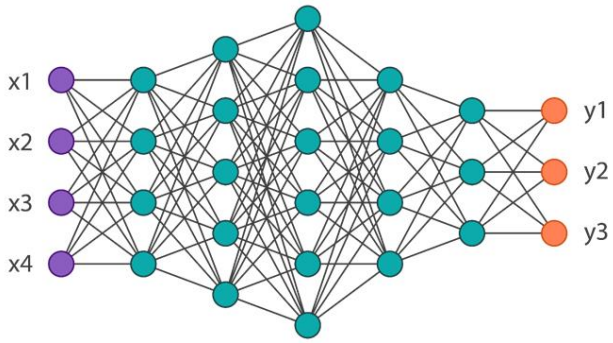

Figure 8. ANN Model

Researchers have developed the Artificial Neural Network (ANN), a processing method that was motivated by the neural impulses found in human nerves. In order to reduce network error and improve accuracy, the number of hidden layers might be raised. A 3-layer network should be prioritised while designing a neural network. It is simpler to acquire the training effect and results in less errors when the number of hidden layer nodes is increased rather than the number of hidden layers. A linear or nonlinear regression without hidden layers is a neural network model. As a result, the regression analysis employs the network model without hidden layers. It is not essential to discuss the technology in terms of neural network theory because it is so advanced. The hidden layer counts in a neural network must be carefully chosen. It significantly affects how well the present neural network model

performs and is the primary cause of "overfitting" during training. Theoretically, it is yet a universally accepted scientific method of determination. The majority of the literature suggests calculating algorithms that are designed for a high number of training samples and finding the number of hidden layer nodes under the worst case scenario. It shouldn't be used because it is difficult to meet the standard engineering practise. An input layer, a hidden layer, and an output layer make up the neural network. Considering the input network connection, data I is an m-dimensional classification sample when employing an ANN as an IDS. The input layer's neurons are then depicted by the following equation.

$$i = \{i_1, i_2, ..., i_n\}, i_i \in \{0,1\}$$

The output layer is in charge of making decisions, while the hidden layer determines if the input data constitutes an incursion. The following equation illustrates how the hidden layer receives the data from the input neuron i.

$$h = \{h_1, h_2, ..., h_n\}, h_i \in \{0,1\}$$

The following operation shows the output.

$$H = \sigma(f(x)) = \sigma(W * i_i + b_i)$$

As demonstrated in the following equation, the hidden layer forwards its outcome to formulate the output layer.

$$Y = \sigma(g(H)) = \sigma(W^T * H_i + b_i)$$

Deep learning is widely employed in many fields and is effective at handling high-latitude nonlinear issues. The multiclassification issue with anti-intrusion detection and deep learning's neural network architecture is employed in the study. The CNN Inception network and deep learning are combined to specifically handle the extremely high-energy problem caused by the neural network's parameter hierarchy.

2.4 Inception-CNN

A deep neural network with an architectural layout made up of repeated elements known as Inception modules is referred to as an inception network. The Multilayer Perceptron (MLP) is a regularised variant of the convolutional neural networks. They were created based on how the neurons in the visual cortex of animals function. The Inception network was an important milestone in the development of CNN classifiers. One of the fundamental ideas in machine learning is that, feature selection has a significant impact on

how well the model performs. The performance obtained depends greatly on the data attributes used to train the machine learning models. There are already 4 Inception networks, and the more complicated Inception-ResNet network can be created by merging Inception V4 with residual connections. The Inception network has the ability to produce dense data while sparing the network structure. The network can be configured with several channels and levels as well as a variety of convolution kernels and pooling techniques. The Inception model is expanded to enhance the nonlinear model and minimise parameter settings. The model's calculating amount and structure are both boosted and altered, the number of convolutional parameters is decreased, and the depth of the network nonlinearity is appropriately increased. More data features can be extracted by combining various channels.

Using the modified pooling method, data features can be scaled and shifted without causing any distortion, which can lighten the burden on the network. Consequently, a proposed adaptive pooling technique. In addition to a more detailed explanation of data properties, it can supply pooling weights over the dynamic components of various pooling cores. This approach can get around the maximum pooling restriction and provide more precise feature data. The flow chart of the developed Inception-CNN IIoT-IDS and its training structure model demonstrate the subsequent steps for merging the Inception detection method with the enhanced network.

Data pre-processing: The dataset's mobile network data is reviewed before usage, and the data presented here is from that dataset. After that, the data is normalised. The original data must be reduced because of its high dimensionality. Data with a stronger impact on the outcome is chosen, while no-impact data is eliminated.

Model training: To fit the CNN format, the pre-processed data is transformed into a two-dimensional representation. Extraction of rich and varied incursion behaviour features and parameter adjustment until convergence are performed.

Data output: After training, the model's performance is analyzed using the test set. Training will be stopped if it satisfies the criteria. If not, the previous steps are repeated to verify the model's correctness.

3. Result

Three models' performances are compared: a straightforward CNN, a conventional Inception framework, and an enhanced Inception-CNN framework. After the upgrade, the

Inception-CNN model is superior to the two established monitoring methods. The training set, test set and the enhanced Inception-CNN model's data correctness, both can sustain a gradually improving trend and eventually stabilise. The loss value of the data in the training set and test set is greater than one at the start of the test. The loss value eventually drops to a value close to 0 as the experiment goes on and stabilises. Additionally, the network environment is getting more and more complicated. The number of complicated devices that need to be continuously updated and patched adds to network managers' workload. Network managers' carelessness could pose serious security threats. The IDS has consequently emerged as a fresh hotspot in the security industry, gaining not only increasing attention but also starting to play a vital role in a variety of circumstances.

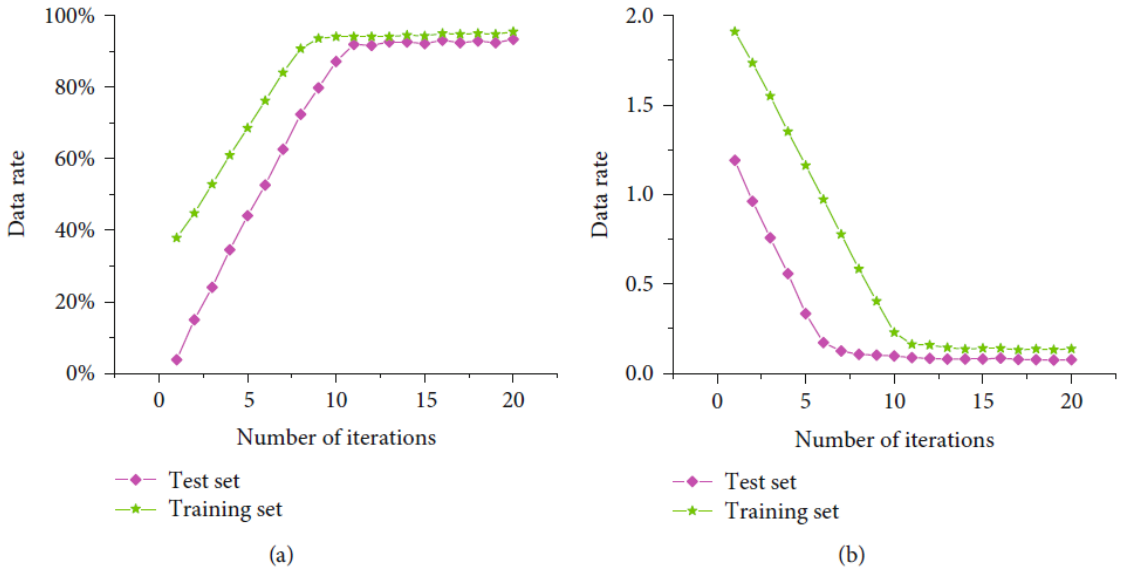

Figure 9. Performance of Inception CNN Model

The literature is mined for the requirements for security performance, starting from the IIoT security. It describes the IIoT structure system and looks at the associated technology for security protection. The inception network merged with a deep learning convolutional neural network serve as the foundation for the IIoT IDS. Actual needs are taken into account when making network improvements. IDS has many advantages, including higher accuracy, large data correctness, accurate detection, and a minimum false positive rate. For discrete data intrusion activities, this kind of technology offers a high degree of detection accuracy. The existing detection network system, however, lacks the capacity to identify larger databases. Second, in a specific complex network environment, a

variety of objective factors affect the detection performance, resulting in a decline in detection performance. The most effective unloading technique is then trained.

According to methodical experiments, the strategy outperforms other representative benchmark methods. A privacy protection model proposed by the new network technology could demonstrate how secure it is to use, how crucial privacy protection is, and how new technologies are required for privacy protection research. The IIoT's covert threats to security and personal information have grown, nevertheless. Network data breaches have become increasingly common in recent years. The goal of research has also changed to include the creation of security and anti-intrusion technologies for IIoT. Starting with the safety of the IIoT, the security performance standards are learned from the literature.

Table 1. Performance comparison of Traditional CNN with Inception CNN

Model	Accuracy	Precision	Recall	F1score
Traditional CNN	98.25	98.12	98.36	98.11
Inception CNN	75.03	73.67	75.01	73.66

The model has not been repeatedly validated in a more sophisticated, multi-interaction network context, nor has the study here been employed in large-scale industrial processes. Instead, it has only been tested in a single network environment. Modern multimodal deep learning traffic classifiers are examined for reliability and interpretability using AI-based methodologies, and their behaviour is enhanced. The report is an important resource for current network traffic trends. The effectiveness of the developed model will next be evaluated in the actual IIoT.

4. Conclusion

IIoT is becoming more prevalent in manufacturing as information technology and industrial technology advance, which offers exceptional ease for industrial control and inspection. The IIoT's covert threats to security and personal information have grown, nevertheless. The IIoT structural system has been presented in this work. AI-based methods look into reliability and modern multimodal systems' behaviour and interpretability. How deep learning traffic classifiers work has been described here. Moreover, the research looks at

the related security defence method. An IDS for IIoT has been developed using the Inception network and CNN. This method gives a good data accuracy, accurate detection rate, and a minimum false alarm rate, according to experimental results. Projects that secure the privacy of IIoT data can therefore employ this methodology. The model has not been repeatedly validated in a more sophisticated, multi-interaction network context, nor has the study here been employed in large-scale industrial processes. Instead, it has only been tested in a single network environment.

References

[1] Vaigandla, Karthik Kumar, Radha Krishna Karne, and Allanki Sanyasi Rao. "A Study on IoT Technologies, Standards and Protocols." *IBMRD's Journal of Management & Research* 10, no. 2 (2021): 7-14.

[2] Karne, RadhaKrishna, Ashok Battula, Dudimetla Prasad, Malothu Devsingh, and KarthikKumar Vaigandla. "Simulation of ACO for Shortest Path Finding Using NS2." (2021): 12866-12873.

[3] HA, Ms Anusha. "INVESTIGATION ON INTRUSION DETECTION SYSTEMS IN IOT." *EPRA International Journal of Multidisciplinary Research (IJMR)* 8, no. 7 (2022): 43-51.

[4] RadhaKrishna Karne, Dr TK. "COINV-Chances and Obstacles Interpretation to Carry new approaches in the VANET Communications." *Design Engineering* (2021): 10346-10361.

[5] Al-Janabi, Samaher, and Ayad F. Alkaim. "A nifty collaborative analysis to predicting a novel tool (DRFLLS) for missing values estimation." *Soft Computing* 24, no. 1 (2020): 555-569.

[6] Karne, RadhaKrishna, Ashok Battula, Dudimetla Prasad, Malothu Devsingh, and KarthikKumar Vaigandla. "Simulation of ACO for Shortest Path Finding Using NS2." (2021): 12866-12873.

[7] He, Sen, Wei Ren, Tianqing Zhu, and Kim-Kwang Raymond Choo. "BoSMoS: A blockchain-based status monitoring system for defending against unauthorized software updating in industrial Internet of Things." *IEEE Internet of Things Journal* 7, no. 2 (2019): 948-959.

[8] RadhaKrishna Karne, Dr TK. "Review On Vanet Architecture And Applications." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12, no. 4 (2021): 1745-1749.

[9] Saleem, Tausifa, and Mohammad Chishti. "Assessing the efficacy of logistic regression, multilayer perceptron, and convolutional neural network for handwritten digit recognition." *International Journal of Computing and Digital Systems* 9, no. 2 (2020): 299-308.

[10] Balakrishnan, Nagaraj, Arunkumar Rajendran, Danilo Pelusi, and Vijayakumar Ponnusamy. "Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things." *Internet of things* 14 (2021): 100112.

[11] Karne, RadhaKrishna, and T. K. Sreeja. "ROUTING PROTOCOLS IN VEHICULAR ADHOC NETWORKS (VANETs)." *International Journal of Early Childhood* 14, no. 03: 2022.