**Malware detection-based edge computing in Industrial IoT using Drift aware Residual Encoder-Decoder CNN**

**Abstract**

The malicious practices pose a significant threat to individuals and organizations, which disrupt the whole system, cause harm to the network, and steal data through different kinds of cyberattacks. As malware threats continue to evolve, securing edge networks has some limitations in their distributed nature and resource limitations. These malware attacks potentially cause loss of finance, data breaches, theft identification, and reputational damage to the environment. In order to reduce the malware threats, focus on security software, adopt a zero-trust security model, and increase the need for advanced and modern accurate malware classification and detection techniques. This research designs a method for classifying the malware threat using a hybrid multi-metric residual encoder-decoder CNN model. Accordingly, the proposed method consists of various heterogeneous devices that are connected to an edge network, and these heterogeneous devices are used to capture the data and this data is transferred to pre-processing and missing data imputation mechanism. In the Data pre-processing phase, the data are cleaned, transformed, and organized the raw data into a suitable form for further analysis, whereas, the missing data imputation method estimates and replaces the missed values of data in the edge network by proper biasing for the complex data analysis. The processed data are fed into a hybrid multi-metric drift aware residual encoder-decoder CNN model, which is composed of hybrid drift and hybrid Attention module. These hybrid models detect and adapt to drifts to ensure their accuracy and reliability when changing the training data. Also, the residual encoder-decoder CNN will be used in preserving the spatial information and reducing the vanishing gradient problem in the model. The variations in the multi-metrics are aware of the training data and send the selected information to the model. Here the model combines with the test data and updates the classified threats and if there are any variations shown in the output phase, then the drift begins to update and train the model with new features. Thus, the process continues and produces the classified threat as an output. The implementation of the proposed method will be done in the PYTHON tool using the CICIDS 2017 Dataset [1], N-BaIoT Dataset [2], and UNSW-NB15 Dataset [3]. The efficiency of the model will be analyzed by using different metrics like accuracy, TPR, FPR, and ROC. Figure 1 depicts the proposed methodology.

Data Aggregation layer from edge layer

Data pre-processing and missing data imputation

Hybrid multi metric drift aware residual encoder-decoder CNN

Model

Heterogeneous devices

D1

D2

D3

D4

Classified Threat

Hybrid Drift

Hybrid Attention

Train Data

No

Test Data

Update model’s weight

**Figure 1**. Schematic representation of the proposed method

**References**

[1] CICIDS 2017 Dataset “<https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset>”, accessed on June 2025.

[2] UNSW-NB15 Dataset “<https://ieee-dataport.org/documents/n-baiot>”, accessed on June 2025.

[3] UNSW-NB15 Dataset “<https://www.kaggle.com/datasets/dhoogla/unswnb15>”, accessed on June 2025.