Enhanced Cyber Attack Detection Process for Internet of Health Things (IoHT) Devices Using Deep Neural Network

- ☑ ~~**Ecu Data set**~~
- ☑ ~~**IoHT**~~
- ☑ ~~**Deep neural network**~~
- ☐ **Federated learning**

The primary innovations and contributions of this paper are as follows:

- **Detection of various types of attacks by applying deep learning approach rather than detection of specific type of attacks in IoHT environment.**
- **The proposed method uses a new dataset ECU-IoHT in the domain of health care**
- **The proposed system achieves higher detection accuracy by analyzing an enormous amount of data (ECU-IoHT dataset consist of 111,207 numbers of samples).**

The paper begins with an introduction to the Internet of Health Things (IoHT) and emphasizes the need to protect these devices from vulnerabilities due to their small and heterogeneous nature. It presents a deep neural network-based cyber-attack detection system that leverages artificial intelligence to identify cyber-attacks using the latest ECU-IoHT dataset. The proposed system achieves an accuracy of 99.85%.

- **Introduction**

- **The paper talked about IoT: Internet of Things (IoT) is an evolving paradigm that facilitates communication between sensors and electronic devices over the Internet, and IoHt: Internet of Health Things (IoHT) is essentially an IoT-based solution that permits the connection between a patient and health care amenities and their applications, such as electrocardiography,electroencephalogram..etc.**

- **IoT in healthcare uses wireless communication, posing security risks like wireless sensor network violations and cyber-attacks like Denial-of-Service attacks, network sniffing, and medical record theft in IoHT environments, categorization of Cyber-attacks: Denial-of-Service (DoS), logical bomb, Sniffer, Trojan horse, Virus, Worm, Send spam, and Botnet. DoS attacks prevent internet access, logical bombs use malicious programs, and Sniffer overhears data transmission.**

- **The paper discusses the ECU-IoHT dataset used in the study and highlights the associated safety risks. Datasets related to cyber-attacks in the medical field are typically not publicly available due to the sensitivity of the data, as exposure could potentially harm patients and even lead to fatal outcomes.**

- **The paper then discussed why DNN is chosen :Researchers have discovered intrusion detection systems (IDS) to prevent network attacks, but they struggle to identify new attacks and increase detection accuracy. To address this, researchers are using artificial intelligence, machine learning, and deep learning approaches. Deep learning, with its deep architecture, has proven effective in various domains like network security, natural language processing, computer vision, cancer detection, speech recognition, and robotics.**
- **The attack was detected are ARP Spoofing, DoS attacks, Nmap Port Scan and Smurf attacks**

- **Literature Survey:**
  from the studies, some of the issues identified are:
  (i) anomaly detection using statistical methods needs significant amount of repetitions for training the model; in addition, the threshold used to detect anomalies may not suitable for real time scenario
  (ii) cluster-based methods lead to time consumption and are inappropriate for anomaly detection
  (iii) lack of openly accessible datasets that reflects cyber assaults in the Internet of Medical Things

- **Proposed System**

1. **Anomaly Detection: Detection of anomaly is an essential cyber safety analysis process for detecting unusual information from a dataset. The proposed model considers four types of attacks such as ARP Spoofing, DoS attacks, Nmap PortScan and Smurf attacks.The paper then continues talking about the attacks.**

2. **Deep Neural Network:belongs to the family of supervised techniques for training the model through multiple layers. The structure of DNN includes input layer, multiple hidden layers and an output layer. Consider X = {x1, x2, ... , xn} is the input vector with n = 5 features ((type, source packets, destination packets, type of protocol, length))and Y = {y1, y2, ... , yn} is the output vector consisting the probability values in the range of [0,1] and values add to 1 to classify normal (no attack) and abnormal (ARP Spoofing, DoS attack, Nmap PortScan and Smurf attack) attacks. In the experimentation, only numerical features are considered, whereas the categorical features are transformed into numerical features using one-hot coding. The model is built with input layer, which entails five neurons, followed by two dense layers (each with eight neurons) and output layer with softmax activation function to categorize into normal or abnormal attacks (ARP Spoofing, DoS attack, Nmap attack and Smurf attack).**

3. **Methodology:**
   Now for the model methodology : the system consists of two phases for detecting attacks .
   1- data preprocessing: the ECU IoHT dataset is used for analyzing various cyber‑attacks; (1)five features are extracted from this dataset and one‑hot encoding is used for encoding categorical features; (2) the dataset is labeled as Normal or attack(Dos,..etc), (3) the data set split into training 80%and testing 20%data sets.
   2-DNN based attack detection:(4) the DNN is trained on the training dataset by choosing these labels as target features using multiclass classification, and it provides a trained model; (5) the trained DNN model is tested by using testing dataset for predicting normal or other types of attacks.
   - **Another detailed Description of Dataset**

4. **Result and Discussion:**
   The proposed system's performance is evaluated by using Accuracy, Precision, Recall, F1-Score, True Positive Rate and False Positive Rate parameters.

- **Environmental Setup**

To implement and evaluate the proposed approach on the ECU-IoHT dataset, the ex- periment is conducted on the DELL laptop installed with Windows 10 OS, 16 GB RAM with Intel Core I5-10210U processor. Spyder Python (version 3.8) is used as an implementation tool with some libraries such as matplotlib (version 3.3.2), Numpy (version 1.19.2), Pandas (1.1.3), Scikit-learn (version 0.23.2), Keras (version 2.6.0) and Tensor flow (version 2.6.0).

- **The paper talked about the data set again.**
- **The results are discussed in detail.**

5. **Conclusions**