Algethami2024deep.pdf

- □ Federated learning
- ☑ ~~Ecu-IHoT Dataset~~

Key Points

- This paper proposes a **hybrid deep learning-based intrusion detection system** using **Artificial Neural Networks (ANN)**, **Bidirectional Long Short-Term Memory (BLSTM)**, and **Gated Recurrent Unit (GRU)** architectures to address critical cybersecurity threats in IoHT (Internet of Health Things). The model was tested using the **Electronic Control Unit (ECU-IoHT) dataset**.

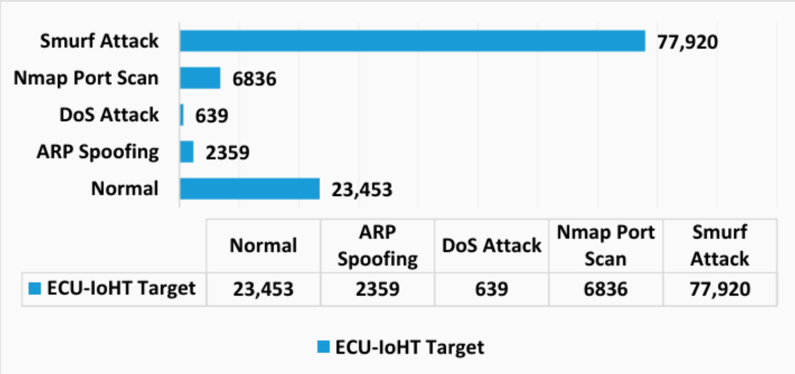
- **Introduction**: Brief introduction of IoT (Internet of Things) and IoHT, emphasizing the growing need for **machine learning (ML)** and **deep learning (DL)** to enhance cybersecurity.
- **Previous Studies**: The study starts with a thorough review of the existing literature, which offers a theoretical analysis of diverse intrusion detection approaches focused on deep learning methodologies.
    - Paper26(27) talked about a deep neural network-based cyber-attack detection system developed using artificial intelligence on the ECU-IoHT dataset to detect cyber-attacks in the Internet of Health Things ecosystem(vijayakumar2023enhanced.pdf).

    - Paper 27(28) talked about a deep neural network in federated learning (DNN-FL) to detect security-threatening anomalies in IoHT data ((our main paper mosaiyebzadeh2023intrusion.pdf)).

- **Dataset**:The study then talked about the data set used , The novel ECU-IoHTdataset, known for reflecting various cyber-attacks in the medical field(, which includes both normal network activity and cyber-attacks in the healthcare domain), is chosen for experimentation.

- The paper discusses the dataset in detail including the equipment used for collecting the data, the seven key network data features, and 4 attacks classification .

- ECU-IoHT dataset comprising a total of 111,207 samples, as presented.



	Normal	ARP Spoofing	DoS Attack	Nmap Port Scan	Smurf Attack
■ ECU-IoHT Target	23,453	2359	639	6836	77,920

- **Model**: The model used in this paper is The ANN component that efficiently processes complex patterns inherent in IoHT data. The BLSTM layer captures bidirectional dependencies, while the GRU layer excels in handling long-term sequential features.

- **Performance Metrics**: Explaining how to calculate the performance metrics (Accuracy , Recall , Rrecision , F1-Score , Specificity , Mean , Error Rate.
  where:
  True positives (TP) are the instances correctly classified as attacks. True negatives (TN) are the instances correctly classified as normal.
  False positives (FP) are the instances incorrectly classified as attacks. False negatives (FN) are the instances incorrectly classified as normal.

These performance metrics are essential in evaluating the system's ability to detect cyber-attacks and assess their effectiveness in the IoHT environment. High accuracy, recall, precision, specificity, error rate, weighted average results, and F1-Score values indicate that the system can efficiently identify and classify attacks while minimizing false detections

- **Results**:
  While the results in the paper show very high performance, it's important to critically evaluate these findings. In practice, 100% accuracy in cybersecurity is unlikely, and the paper should acknowledge the limitations of real-world applications. Further testing on more diverse datasets and more transparency in the methodology would help assess the robustness of the model.

- Dissection
- Conclusion