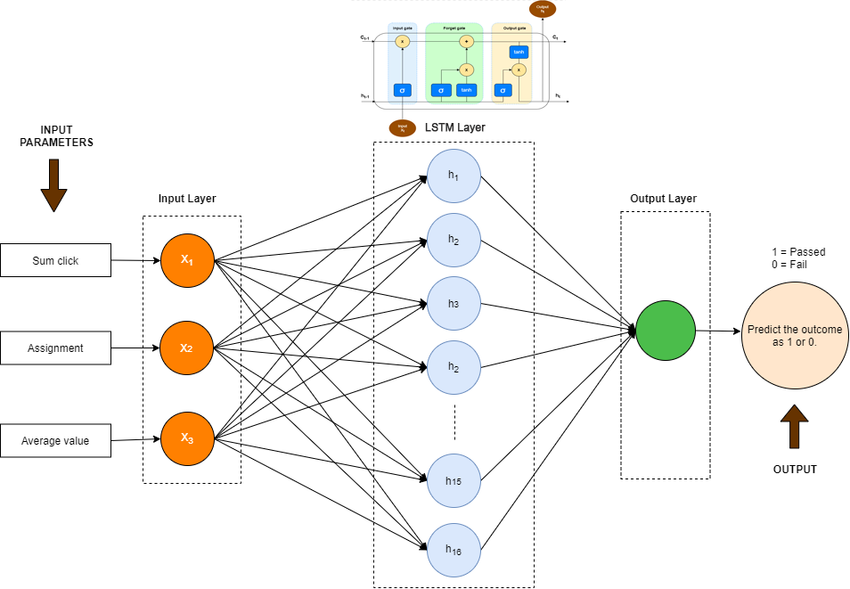
**LSTM Model Research for Intrusion Detection**

**Why LSTM:**

* LSTM (Long Short-Term Memory) is a type of Recurrent Neural Network (RNN) specialized for **sequence data**.
* Network traffic behaves sequentially over time — attacks develop as patterns (e.g., repeated failed logins, DDoS bursts).
* LSTM can **remember long-term dependencies**, making it ideal for detecting such evolving threats.

**Advantages of LSTM**

* **Captures Temporal Behavior:** Understands time-based attack trends that static models (like Random Forest) miss.
* **Avoids Vanishing Gradient:** Uses gates (input, forget, output) to control memory flow and retain key information.
* **High Accuracy:** Proven to reach 95–99% detection accuracy on datasets like CIC-IDS2017.
* **Explainable:** Attention-based LSTM can show which time steps contributed most to an alert.
* **Lightweight & Real-Time:** Faster inference compared to large Transformers — suitable for deployment.

**Architecture of LSTM Model:**

**LSTM Architecture Overview**

Input Layer → LSTM Layers (2) → Dense Layer → Sigmoid/Softmax Output

* **Input:** Sequential flow features (duration, packet rate, bytes, flags, etc.)
* **Hidden Layers:** 2 Bi-directional LSTM layers (128 units each, dropout 0.2)
* **Output:**
  + Binary: Normal (0) / Attack (1)
  + Multiclass: DDoS, Port Scan, Brute Force, etc.

**Training Configuration**

* **Dataset:** CIC-IDS2017 (contains normal + 15 attack types)
* **Data Split:** 70% train, 15% validation, 15% test (time-based split preferred)
* **Loss Function:** Binary Cross-Entropy / Categorical Cross-Entropy
* **Optimizer:** Adam or AdamW
* **Batch Size:** 64–128
* **Epochs:** 30–50
* **Metrics:** Accuracy, Precision, Recall, F1-Score, ROC-AUC