**Summary**

This paper talks about a new firewall scheme called Enhanced Intrusion Detection and Classification (EIDC) system for secure cloud computing environment. EIDC detects and classifies the received traffic packets using a new combination technique called most frequent decision where the nodes’ past decisions are combined with the current decision of the machine learning algorithm to estimate the final attack category classification. This strategy increases the learning performance and the system accuracy.

EIDC combines the performance of supervised learning and past information about the network users. Basically, by taking the history of each node into account, the proposed scheme improves the estimation of the node reliability when making the final packet classification.

Each node can be identified and differentiated by a set of features that reflect the characteristics of trans- mitted data packets (for example IP destination, transmission

protocol).

We assume that each node keeps the same status for an enough period of time that allows the firewall to detect it. In particular, this strategy is applied to protect the network

from any unknown node that keeps trying to inject malicious packets in the network.

**Overall FrameWork**

1. **Learning Phase - In the first step, a learning phase is performed to train the machine learning algorithm and create the learning model which will be used to make the first classification for any received packet.**
2. **Decision History Storing - The second step includes decision history storing where EICD scheme stores in a separate database all the previous decisions made for each node in the network.**
3. **The final step where the final classification decision is made namely, combined decision phase.**

For each received packet from any node in the network, EICD combines the decision of

the machine learning model with the saved past information (nodes attack types classification decision histories) and the most frequent decision will be taken (.i.e. for a received packet in time t, the decision is made based on all the previous

decisions from instant 0 to t).

**Learning Phase**

In the machine training, an input data that includes packets for normal and abnormal behaviors is needed. This process focuses on modeling the input features for each node to an output class. The learning algorithm tries to find a function f(x) of the input features that best predicts the output class.

At the end of this step, the created model should be able to classify any received packet.

**Decision History Storing**

The created model generates a new decision classification and the system adds it to the database. The saved decisions will be updated so that each node has a behaviors history.

**Combined Decision Phase**

Step 1: Determine node using the set of features.

Step 2: Access to the decision history database and extract Di of the node.

Step 3: Combine Di with the current decision.

Step 4: Compute the most frequent decision and select it as the best decision.

**Conclusion**

EIDC improves the detection and classification of malicious users using a novel combination technique that exploits the decision histories as well as current decisions.