Network Intrusion Detection System using Neural Networks, aided by Blockchain

Group members:

1. Ananya Dutta - 1805011
2. Arismita Banerjee - 1805021
3. Arkaprabha Samanta - 1805106
4. Sayantani Bala - 1805245
5. Aisika Roy - 1805366

Core Idea:

Network Intrusion Detection System, aided by Neural Networks, with security enhanced using blockchain.

Problem statement description:

Nowadays, network is one of the essential parts of life, and lots of primary activities are performed by using the network. Also, network security plays an important role in the administrator and monitors the operation of the system. The world security context is changing more than ever. Military interest has shifted from the conventional means of warfare to that of cyber warfare. The most potent nations have entire armies that are watching the international cyberspace for anomalies. And these forces are ready to intervene for keeping peace at home or for an enemy nation. The international interest in exploit development has risen significantly. In this ever-changing world of computer technology and rapidly evolving cyber threats, attackers and defenders are in a constant loop of cat-and-mouse. On the defender's side, a defense-in-depth strategy must be added to their security layer to effectively detect advanced persistent cyber threats, where Intrusion Detection System (IDS) is a key element. The network intrusion detection system (NIDS) is a crucial module to detect and defend against the malicious traffics before the system is affected. This system can extract the information from the network system and quickly indicate the reaction which provides real-time protection for the protected system. However, detecting malicious traffics is very complicating because of their large quantity and variants. Also, the accuracy of detection and execution time are the challenges of some detection methods. Hence, we are aiming to use an IDS platform based on neural network, to detect DoS attack, web attacks, brute-force attacks over the SSH and FTP protocol, etc. Also, as the cyber security is a major issue that is to be addressed, so the security of the neural network model also plays a crucial role, as a small change in the neural network model can affect the model's output to a large extent. Hence, the neural network model is thought to be securely set up in a blockchain network for further security purpose, thus making the system more robust, along with having high precision.

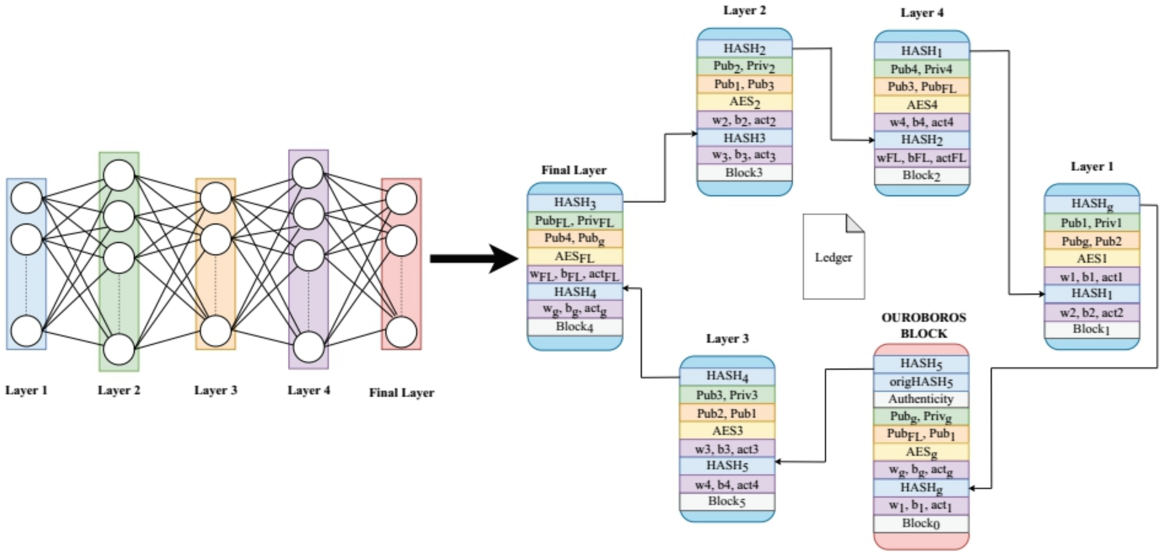
Project specific workflow:

BLOCKCHAIN IN NEURAL NETWORK:

Main security issue that is faced by the neural network is that it is not tamper resistant. One can make a change in one of the layers of the model. This will result in a wrong prediction output of the model, thus drastically reducing its efficiency, and posing a threat to the authenticity of the result. The security of the neural network can be enhanced by blockchain in various ways:

1. To secure the data: here, the data is to be secured by using blockchain, to provide a layer of anonymity and tamper resistance to the data used.

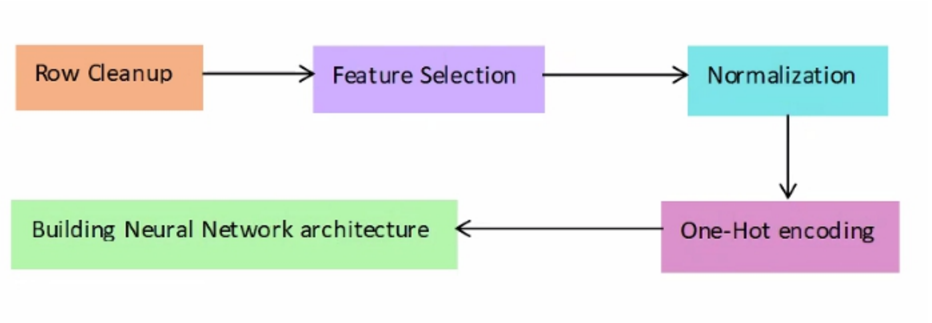
2. Secure the neural network model: implement each layer of the neural network model in a block of a blockchain- the deep ring model



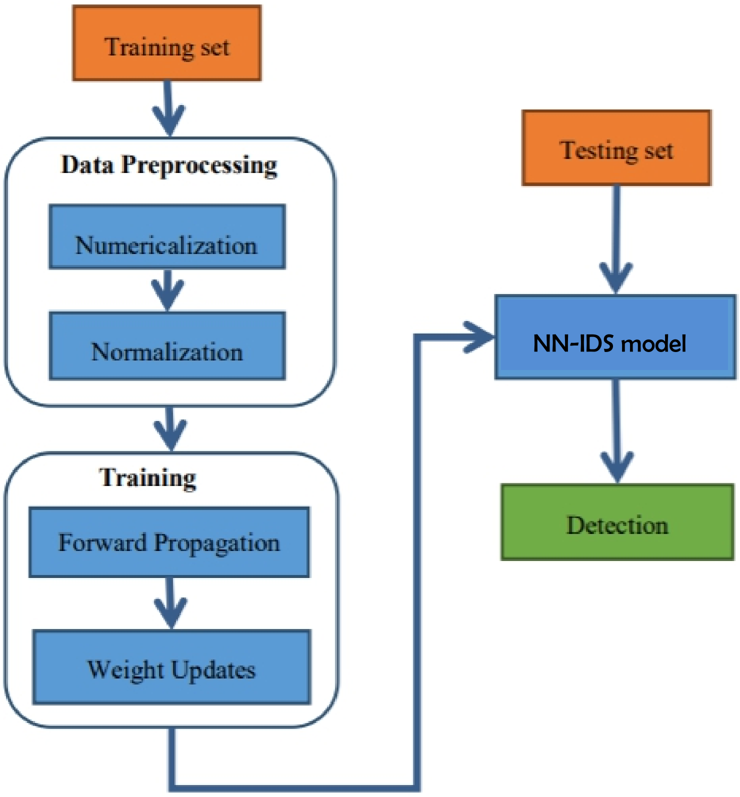
3. Decentralize the neural network model, thus distributing the computational overhead.

THE NEURAL NETWORK MODEL:

Here, we will build a few Neural Network models, with different architecture, for example, having different number of hidden layers, activation functions and optimization. Each of these models will be evaluated against the test data and then the optimal model would be chosen from them. The basic steps of preprocessing the data that are common for building the models are given below:



The basic workflow of the models can be summarized in a flowchart, that contains the necessary steps:



Market Demand:

With the growing need for distributing the IDS workload among various devices, security hazards has continued to persist in various organizations. Absence of a strong security system integrated in the network can lead to significant loss of imperative information. Unmonitored networks can further lead to intrusion through various malicious attacks on the system, due to which the organizations can run into various losses. As the need for protecting and detecting malware attacks on the system surfaces, demand for the intrusion prevention & detection system is expected to remain high in various organizations. The intrusion detection system / intrusion prevention system (IDS / IPS) market is estimated to hike to USD 8 billion by 2025, according to a 2019 Global Market Insights, Inc. report. The market growth is attributed to factors including the growing number of IT data breaches and security threats, rising demand for enterprise mobility, and stringent regulations established by government to safeguard consume.